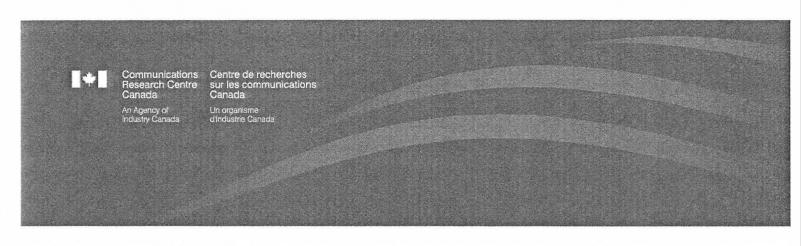
(A-2018-00073) - Page: 1



# **Technical Study on Privacy in Wireless Networks**

August 25, 2014

Contribuors:

Phil Vigneron, Siva Palaninathan, Jacob Gurnick, François

Lefebvre, Li Li, Andre Brandao, Colin Brown, Pascal Charest,

Jacob Slobodov (CRC)

and

Frederic Nolin (DPB)

Lead VP:

Alex Vukovic

This document is the result of a CRC Direct Client Support project executed for the CRC Research Advisory Board. The document's intent is to investigate the impact on privacy from the use of mobile telecommunications and Wi-Fi services. Technical results are presented, and technical actions for further support to the Department are recommended.

**Communications Research Centre Proprietary** 





(A-2018-00073) - Page: 2



# **Executive summary**

In the February 2014 Research Advisory Board (RAB) meeting at the Communications Research Centre (CRC), the research topic of wireless privacy in Canada was proposed and approved for a short-term investigation. Concerns over privacy for wireless services arise from the evolution of wireless technology combined with the omnipresence of telecom and Wi-Fi infrastructure. In this context, widespread wireless usage enables a real threat that intrusions and security breaches could compromise the privacy of Canadians. This report contains results and findings of technical investigations, and provides recommendations for Industry Canada.

In order to provide mobility, devices transmit system information that is required for proper functioning of the wireless and wired network and applications. Some system information, often referred to as *metadata*, indicates device identity. When metadata is collected from wireless devices over an extended period of time and is corroborated with known physical access location and time, usage patterns emerge that reveal information on the characteristics and preferences of the user. When metadata collected from one source is merged or *fused* with other sources, a clearer picture is revealed on the behaviour and traits of the device owner. Over weeks and months, the fused information can, ultimately, be used to identify the user of the device and glean personal information. As consumers migrate towards electronic wallets and e-commerce, there is a concern that privacy breaches over wireless infrastructure may slow down or even inhibit the adoption of these new applications.

The aspects of privacy under study by CRC concern the collection of wireless metadata that demonstrate patterns of activity and are used in fusion and processing to assemble personal information. Also studied is the assessment of the protection level of users' communications. These studies provide the Department's Spectrum, Information Technologies and Telecommunications (SITT) sector with valuable information, while adding credible research sources to policy and partnership development. The scientific approach used was the identification of potential issues, documentation of issues, and demonstration of the ease in which current inexpensive technology can be deployed to invade privacy. Many topics addressed in this work merit a thorough R&D investigation within a longer-term project.

The following questions, concerning the state of wireless privacy today in Canada, have been addressed within the study:

Question 1: What is the level of privacy protection for wireless service users in Canada? How does it compare to other nations? This study was initiated in response to disturbing news stories about wireless privacy in Canada, and concerns about the level of protection inherent in the radio protocols. Experimentation with inexpensive equipment was conducted to assess how someone with few resources and modest education could take advantage of inexpensive radio equipment and free software from the Internet. In this context it has been found to be easy to obtain unique device identifiers that can be used to breach privacy. Based on initial measurements on telecom service conducted around Ottawa, Canada's wireless privacy is comparable with the US and behind Western Europe.

Question 2: Where are the weaknesses for access to private information within the established wireless services in Canada? Can users play a role in securing their own device information? There are weaknesses in Wi-Fi and telecom technologies that allow unique identifiers of mobile devices to be surreptitiously taken using inexpensive hardware and free software from the Internet. There are options for service providers and users to secure their information, such as proxy identifiers. These are not widely used due to the effort required by users.

Question 3: What are the potential scenarios for the interception of signals for common wireless technologies in Canada? Users with minimal technical expertise can use inexpensive hardware and software tools and methods described on the Internet to capture the unique device identifiers of mobile devices while remaining unseen and undetected. This can be done from outside a building, to a pedestrian, or to a passing vehicle under certain conditions. These identifiers, combined with location and time information, can be sold to companies with expertise in data and identity fusion, and analytics.

Question 4: How can the collection of information and metadata from wireless protocols compromise Canadians' privacy? Information and metadata collected from wireless devices can be used in data fusion where single measurements, of little privacy concern on their own, are combined to create a meaningful picture over time. This processing reveals profiles of people's habits, preferences, travels and sometimes identities. Inexpensive and easy-to-use technology is disruptive by enabling automatic collection of metadata from thousands of people in urban environments.

There are possible actions of a technical nature that can address wireless privacy, and can be summarized as:

- 1) Engage service providers for discussions on privacy in wireless networks in Canada. The department can obtain information on privacy protections in relation to peers (i.e., "to complete the map" for Canada).
- 2) Partner with industry to increase the level of wireless privacy in Canada. Propose an action plan to establish best practices of factory settings for equipment and consumer devices retailed in Canada through engineering and certification, regulation, or other policy options, and identify how telecom and Wi-Fi standards can be configured within infrastructure equipment to maximize wireless privacy.
- 3) Establish parameters of privacy metrics with industry players, other government departments, and other countries.
- 4) Work with industry to steer international standards towards enabling greater protection of privacy in wireless networks.
- 5) Ensure CRC will remain available for consultation on any technological possibilities regarding privacy in the wireless domain.

In conclusion, there is no single "smoking gun" enabler that, if solved technologically, would deliver total privacy to wireless users. Rather, addressing the problem requires an ecosystem of solutions developed by regulators, industry and R&D organizations that, when taken together, will deliver an enhanced level of privacy protections.

## Résumé

À l'occasion de la réunion de février 2014 du Conseil consultatif de la recherche (CCR) du Centre de recherches sur les communications Canada (CRC), les membres ont proposé et approuvé la protection de la vie privée sur les réseaux sans fil comme sujet de recherche à court terme. Les progrès de la technologie sans fil ainsi que l'omniprésence de l'infrastructure des réseaux de télécommunications et Wi-Fi soulèvent des préoccupations à cet égard. Dans ce contexte, l'utilisation généralisée de la technologie sans fil constitue une véritable menace en raison des intrusions et des atteintes à la sécurité pouvant compromettre la protection de la vie privée de la population canadienne. Le rapport qui suit contient les résultats et les conclusions des études techniques et formule des recommandations à Industrie Canada.

Pour permettre la mobilité, les appareils transmettent de l'information sur le système requise pour assurer le bon fonctionnement des réseaux et des applications sans fil et filaires. Certaines informations sur le système, couramment appelées *métadonnées*, font état de l'identité de l'appareil. Lorsque les métadonnées provenant d'appareils sans fil sont recueillies sur une longue période et sont corroborées par les données spatiotemporelles connues relatives à l'accès physique, des tendances d'utilisation ressortent et révèlent des renseignements sur les caractéristiques et les préférences de l'utilisateur. Quand on regroupe ou *fusionne* les métadonnées recueillies auprès d'une source avec celles provenant d'autres sources, on obtient un portrait plus clair du comportement et des particularités du propriétaire de l'appareil. Au fil des semaines et des mois, les renseignements fusionnés peuvent, en définitive, servir à identifier l'utilisateur et à glaner des renseignements personnels. En cette époque où les consommateurs optent pour les portefeuilles électroniques et le commerce électronique, on craint que les atteintes à la vie privée sur l'infrastructure d'accès sans fil risquent de freiner voire même d'empêcher l'adoption de ces nouvelles applications.

L'étude du CRC portait sur les aspects de la protection de la vie privée ayant trait à la collecte de métadonnées sur les réseaux sans fil dévoilant des types d'activités habituelles et servant à la fusion et au traitement de données en vue d'assembler des renseignements personnels. Elle visait également à évaluer le degré de protection des communications des utilisateurs. Les résultats de cette étude fournissent de précieux renseignements au Secteur du spectre, des technologies de l'information et des télécommunications (STIT) du Ministère et représentent d'autres sources crédibles de recherche en vue de l'élaboration de politiques et de la formation de partenariats. La méthode scientifique utilisée consistait à cerner les éventuels enjeux et à les documenter ainsi qu'à démontrer à quel point il est facile de déployer des technologies peu coûteuses qui existent à l'heure actuelle pour porter atteinte à la vie privée. De nombreux sujets abordés dans ce rapport méritent des travaux de R-D approfondis dans le cadre d'un projet à plus long terme.

Les questions suivantes, ayant trait à l'état actuel de la protection de la vie privée sur les réseaux sans fil au Canada, sont abordées dans le cadre de cette étude :

Question 1: Quel est le niveau de protection de la vie privée des utilisateurs de services sans fil au Canada? Comment se compare-t-il à celui des autres pays? Cette étude a été entreprise en réponse aux nouvelles troublantes dans les médias au sujet de la protection de la vie privée sur les réseaux sans fil au Canada et en raison des préoccupations soulevées par le niveau de protection inhérent aux protocoles radio. Des expériences à l'aide de matériel bon marché ont été menées pour évaluer comment une personne ayant peu de ressources et un niveau de scolarité modeste pourrait tirer parti de matériel radio peu coûteux et de logiciels libres offerts dans Internet. À cet égard, on a découvert qu'il est facile d'obtenir l'identifiant unique d'un appareil et

de s'en servir pour porter atteinte à la vie privée. Selon les mesures initiales sur les services de télécommunications effectuées à Ottawa et les environs, le niveau de protection de la vie privée au Canada est comparable à celui des États-Unis et inférieur au niveau de protection en Europe de l'Ouest.

Question 2: En quoi consistent les faiblesses des services sans fil établis au Canada en matière d'accès aux renseignements privés? L'utilisateur peut-il jouer un rôle pour protéger les renseignements de son propre appareil? Les technologies Wi-Fi et de télécommunications comportent des faiblesses en permettant de s'emparer sournoisement de l'identificateur unique des appareils mobiles à l'aide de matériel peu coûteux et de logiciels libres offerts dans Internet. Diverses options sont à la portée des fournisseurs de services et des utilisateurs pour protéger leurs renseignements privés, notamment les identificateurs mandataires, mais on n'y a pas largement recours en raison de l'effort demandé à l'utilisateur.

Question 3: Quels sont les scénarios possibles d'interception des signaux propres aux technologies sans fil couramment utilisées au Canada? Un utilisateur possédant un minimum de savoir faire technique peut se servir d'outils matériels et logiciels bon marché et profiter de méthodes expliquées dans Internet pour s'emparer de l'identificateur unique d'appareils mobiles sans être vu ni détecté. Il peut parvenir à cette fin à l'extérieur d'un immeuble ou viser un piéton ou même un véhicule en déplacement, dans certaines conditions. Cet identificateur unique, accompagné des données spatiotemporelles, peut être vendu à des entreprises possédant un savoir faire dans l'analyse et la fusion de données et d'identités.

Question 4: Comment la collecte de renseignements et de métadonnées provenant de protocoles sans fil peut-elle compromettre la protection de la vie privée de la population canadienne? Les renseignements et les métadonnées soutirés des appareils sans fil peuvent servir à la fusion de données; une seule mesure, peu problématique en soi pour la protection de la vie privée, si elle s'ajoute à d'autres mesures, permet d'obtenir un portrait significatif au fil du temps. Ce traitement de l'information dresse le profil des habitudes, des préférences, des déplacements et même parfois de l'identité des gens. La technologie bon marché et facile à utiliser devient perturbatrice quand elle permet la collecte automatique de métadonnées provenant de milliers de personnes en milieu urbain.

Il existe des mesures de nature technique à utiliser pour contribuer à assurer la protection de la vie privée et que pourrait prendre à cette fin le gouvernement. En voici un aperçu :

- 1) Inviter les fournisseurs de services à prendre part à des discussions sur la protection de la vie privée dans les réseaux de communication sans fil au Canada. Le Ministère pourrait obtenir de l'information sur leurs mesures de protection de la vie privée par rapport à celles des autres pays (c.-à-d. pour « apporter la touche finale à la carte » canadienne).
- 2) Entrer en partenariat avec l'industrie pour accroître le degré de protection de la vie privée dans les réseaux sans fil au Canada. Dresser un plan d'action, entre autres mettre en œuvre des pratiques exemplaires quant aux réglages en usine du matériel et des appareils grand public vendus au détail au Canada au moyen de l'ingénierie et de la certification, de la réglementation ou d'autres options stratégiques, et déterminer les moyens à prendre en vue de configurer les normes de télécommunications et du Wi-Fi du matériel d'infrastructure pour protéger le plus possible la vie privée dans les réseaux sans fil.

- 3) Établir les paramètres des mesures visant la protection de la vie privée avec les intervenants de l'industrie, d'autres ministères gouvernementaux et d'autres pays.
- 4) Collaborer avec l'industrie pour orienter les normes internationales en vue d'assurer une meilleure protection de la vie privée dans les réseaux sans fil.
- 5) Assurer la disponibilité du CRC aux consultations sur toute possibilité technologique relative à la protection de la vie privée dans le domaine du sans-fil.

En conclusion, il n'existe aucun facteur déclenchant flagrant et unique, dont la résolution, à l'aide de moyens techniques, offrirait une protection complète de la vie privée aux utilisateurs de services sans fil. La résolution du problème exige plutôt un écosystème de solutions mises au point par les organismes de réglementation, l'industrie et les instituts de R-D qui, de concert, permettront d'obtenir un meilleur niveau de protection de la vie privée.

# **Table of Contents**

List of Figures	10
List of Tables	10
List of Acronyms	11
1. Introduction	12
1.1 Role of Metadata	12
1.2 Background	
1.2.1 Privacy versus Security in Wireless Networks	
1.3 Privacy Legislation under Responsibility of Industry Canada	
1.4 Report Contents	
2.0 Problems Studied and Addressed	16
3.0 Telecom Equipment and Systems	18
3.1 Background	18
3.2 Demonstration with GSM Systems	18
3.3 Options Available for Industry Canada to Reinforce Telecom Service Privacy	19
3.4 Measurement of Base Station Privacy Settings	
3.4.1 Options for Industry Canada to Assess Wireless Privacy of Telecom Infrastructure.	
4.0 Unlicensed Wi-Fi Equipment Using 802.11 Standards	
4.1 Background	
4.2 Privacy issues in Wi-Fi	
4.3 Test Results Obtained at CRC Campus	
4.4 Options Available for Industry Canada to Reinforce Wi-Fi Privacy	
5.0 Fusion – Enablers of Smart Services in Connected Environments	
5.1 Options to Manage Fusion and Analytics Effectiveness	29
6.0 Summary of Findings	30
6.1 Technical Options for Action on Wireless Privacy	
6.2 Personal Scenarios	33
References	34
Appendix A: Technical Information about Telecom System Protocols and Revealing Unique	
Identifier	
A-1 Identifiers Used in the LTE System	
A-2 Use of Metadata in Network	
A-3 Mechanisms in Telecom Protocols Whereby IMSI is Revealed	
A-4 Passive Scenario: Use of LTE Receiver	
A-5 Active Scenario: Use of Base Station to Draw Out Mobile Device Identifier	
A-6 Test Configuration for GSM IMSI Testing	
A-7 Demonstration Results for GSM Testing	
Appendix B: Equipment for Independent Measurement of Base Station Privacy Settings	44

Appendix C: Wi-Fi Protocol Elements Impacting Privacy, and Results	49
C-1 Unique Identifiers for Wi-Fi	
C-2 Wi-Fi Association	
C-3 Field testing	
C-3-1 Test Hardware Platform	51
C-3-2 Test Scenarios	
C-3-4 Interpretation of Results	54

# **List of Figures**

Figure 1: OpenBTS GSM/2G base station with inexpensive radio hardware (in anechoic chamber at CRC
to avoid interference with deployed telecom services).
Figure 2: Wi-Fi test measurement locations around Shirleys Bay campus of Industry Canada, Ottawa25
Figure 3: GSM Attach Procedure [19]
Figure 4: Segment of LTE-attach procedure, IMSI or GUTI are transmitted unencrypted [20]39
Figure 5: Segment of LTE-attach procedure where temporary address is designated [20]39
Figure 6: GSM/2G base station hardware, showing size perspective
Figure 7: Selection of captured metadata using a proprietary tool from base station towers near CRC, for
GSM-2G, indicating ciphering algorithm A5/1
Figure 8: Selection of metadata categories using a proprietary tool from base station towers near CRC,
for LTE-4G showing status of some privacy protectors
Figure 9: Selection of captured metadata using a proprietary tool from base station towers near CRC, for
UMTS-3G showing status of some privacy protectors
Figure 10: Association phase of Wi-Fi connection between mobile device and Wi-Fi access point [21]49
Figure 11: Scenario whereby a low-cost radio device can collect Wi-Fi metadata without knowledge of
the users
Figure 12: Wi-Fi hardware "Router" RB433 + Wistron CM9
Figure 13: Scenario where Wi-Fi metadata is collected over a geographic region as source material for
metadata fusion
List of Tables
Table 1: Options of hardware and software tools for privacy investigations, reflecting capabilities
currently available at CRC21
Table 2: Field trial results of Wi-Fi measurements at CRC targeting MAC addresses of mobile devices.
Reported are numbers of devices captured
Table 3: Mobile devices making IMSI identifiers available over the air without connecting to service42
Table 4: Status of ciphering element of privacy protections on Rogers LTE base stations within radio
range of CRC48
Table 5: Snapshot of Wi-Fi monitoring results, captured using a \$140 commercial hardware platform
(MAC addresses have been detected, but are hidden herein for privacy)
Table 6: One entry from Wi-Fi MAC detection data log from June 20, 2014, at Shirleys Bay (see third
column, Table 6), Test 2, 10-second duration (MAC address were detected, but are hidden to protect
privacy)54

# **List of Acronyms**

2G	Second Generation Cellular Standard
3G	Third Generation Cellular Standard

3GPP Third Generation Partnership Project (Standards Group)

4G Fourth Generation Cellular Standard AES Advanced Encryption Standard

CID Cell Identifier
DRB Data Radio Bearer
E-911 Emergency-911
GHz GigaHertz

GPS Global Positioning System

GSM Global System for Mobile Communications
GUTI Globally Unique Temporary Identity

IEEE Institute of Electrical and Electronics Engineers

IMSI International Mobile Subscriber Identity
LTE Long Term Evolution (4G Standard)

MAC Media Access Control

MHz MegaHertz ms milliseconds

RFID Radio Frequency Identification
SIM Subscriber Identity Module
SRB Signalling Radio Bearer
SSID Service Set Identifier

UMTS Universal Mobile Telecommunications System

USB Universal Serial Bus

USRP Universal Software Radio Peripheral

VoLTE Voice over LTE

WPA Wi-Fi Protected Access
WEP Wired Equivalent Privacy

Wi-Fi Wireless Fidelity

WLAN Wireless Local Area Network

# 1. Introduction

In the February 2014 Research Advisory Board (RAB) meeting of the Communications Research Centre (CRC), the topic of wireless privacy in Canada was proposed and approved by the RAB for a short-term investigation.

The evolution of technology and mobility of wireless devices, along with the omnipresence of telecom infrastructure and Wi-Fi connections, are increasing opportunities for users to be connected from anywhere at anytime. Unfortunately, such ubiquitous connectivity and widespread usage of devices are opening the door to potential intrusions or security breaches that could compromise the privacy of everyday users.

As many people use devices for mobile access on a daily basis, they are sensitive to how their personal information is used. Their mobile devices are significant gateways to mobile services, social networks and applications that are increasingly important to them. While Canadians understand that their private information is needed for their applications to work, they also expect that it will be fairly treated, and used only as required by networks and applications.

Modern wireless networks and protocols are complex, and the network needs to use some personal information, such as unique-device identifiers, to deliver useful applications and services to the user. This information may also be collected and stored for further purposes beyond those originally intended by the user. For example, the information may be shared with other applications and services that network operators anticipate may be used by the client.

Recently, there have been indications that the personal information used by wireless devices and services is not being used in line with expectations of users in Canada, where even if users take some steps to protect their privacy (eg. disabling "cookies") the technology firms then follow up with more sophisticated approaches to achieve their goals [1], [2], [3]. This is an old and familiar issue in the "wired" Internet community, where there have been long-time concerns about how security protects privacy. Although Canadian laws such as the Privacy Act, the Personal Information Protection and Electronic Documents Act (PIPEDA), and the Federal Anti-Spam Legislation address privacy, ongoing technological innovation in wireless systems must continue to be considered in the evolution of regulatory measures.

Investigations into the protection of wireless privacy at CRC aim to provide Industry Canada's Spectrum, Information Technologies and Telecommunications (SITT) sector with technical background, while adding credible research sources to policy and partnership development for SITT.

#### 1.1 Role of Metadata

In order to provide mobility, devices transmit system information that is required for proper functioning of the wireless and wired network and applications. Some system

information, often referred to as *metadata*, indicates device identity. When metadata is collected from wireless devices over an extended period of time and is corroborated with known physical access location and time, usage patterns emerge that reveal information on the characteristics and preferences of the user. When metadata collected from one source is merged or *fused* with other sources (including application cookies and Internet surfing), a clearer picture is revealed on the behaviour and traits of the device owner. Over months and years, the fused information can, ultimately, be used to identify the user of the device and glean personal information. The technological aspects of privacy under investigation by CRC concern the collection of metadata over wireless access links, and how these small tokens of data, which contain no personal information, can be obtained, fused and processed to assemble personal information about a user.

# 1.2 Background

The Federal Government's Digital Canada 150 [4] policy indicates a priority on investigation of privacy as it pertains to mobile online activities:

"...We will take action so that the communications networks and devices that connect Canadians will be secure from threats, protecting the privacy of Canadian families, businesses and governments..."

Newspaper stories and press releases address how mobile devices can be configured to improve privacy [1], [2], [3], including how the technological evolution will counteract peoples' changing use habits by tracking without using cookies, for example [3].

Some specific concerns regarding wireless privacy that are raised within the website of the Office of the Privacy Commissioner of Canada [5] and in the sections pertaining to PIPEDA are:

- Location tracking using built-in Global position systems (GPS), radio-frequency identification (RFID) and other tiny wireless devices can keep tabs on your every move;
- People engaged in social networking when accessing the Internet from mobile devices may fail to apply the privacy settings in the devices as well as the applications, compromising personal information;
- High-speed communications and data management let companies outsource business activities abroad. This sends personal information around the globe and beyond the control of Canadian policies.

# 1.2.1 Privacy versus Security in Wireless Networks

It is common to see issues of privacy discussed at the same time as those of security. The Direct Client Support work conducted by CRC addresses wireless access privacy and aims to find synergy with work underway at SITT on the topic of security.

According to the Privacy Act of Canada [5], "... personal information is defined as information about an identifiable individual that is recorded in any form including... any identifying number, symbol or other particular assigned to the individual...". Concerns about privacy of wireless systems are focused on the protection of personal information.

# 1.3 Privacy Legislation under Responsibility of Industry Canada

This research project provides a better understanding of potential security breaches in wireless technologies. This would help a number of strategies and initiatives currently underway either under Industry Canada's mandate or under the responsibility of partner departments that are involved in cyber security.

Digital Canada 150 [4] includes a pillar on protecting Canadians, with the objectives of protecting the privacy of Canadians and preparing them for online threats. The aim is to increase the level of confidence of Canadians in online transactions. Industry Canada is also supporting the efforts of Public Safety Canada in delivering its cyber strategy, including a pillar of the Digital Canada 150 on Protecting Canadians online, which reports:

"We passed Canada's world-leading anti-spam law, which comes into force July 1, 2014, to protect Canadians from malicious online attacks."

Wireless technology is an important gateway to the Internet and to applications for personal and business use. Legislation aims to keep up with concerns of wireless privacy, but as technological innovations quickly change, the Department needs engineering facts and investigations to support further regulatory evolution.

Industry Canada is involved in several pieces of legislation addressing privacy concerns:

- The Personal Information Protection and Electronic Documents Act (PIPEDA) oversight by Office of Privacy Commissioner of Canada;
- The Privacy Act oversight by Office of Privacy Commissioner of Canada;
- Federal Anti-Spam Legislation oversight by Industry Canada (SITT and Office of Consumer Affairs.

# 1.4 Report Contents

The scope of investigation into wireless privacy is explained in Section 2 of this report. Section 3 describes telecom equipment and systems, and provides results of technical investigations that show the role that wireless telecom access schemes play in revealing private information. This section also describes tools and early results of assessing wireless privacy in telecom networks in Canada and how this allows us to develop comparative results with other countries. Section 4 contains results showing wireless privacy concerns for unlicensed Wi-Fi

(A-2018-00073) - Page: 15

# TECHNICAL STUDY ON PRIVACY IN WIRELESS NETWORKS

(802.11) systems. In Section 5 we discuss the critical role of data analytics and fusion in converting wireless device information into private information. Finally, in Section 6 we summarize findings and propose actions. Appendices contain the in-depth technical information on measurements and field tests reported in Section 3 and Section 4.

# 2.0 Problems Studied and Addressed

The breadth of investigations into wireless privacy is reflected in the following questions probing major concerns:

Question 1: What is the level of privacy protection for wireless service users in Canada? How does it compare to other nations?

Question 2: Where are the weaknesses for access to private information within the established wireless services in Canada? Can users play a role in securing their own device information?

Question 3: What are the potential scenarios for the interception of signals for common wireless technologies in Canada?

Question 4: How can the collection of information and metadata from wireless protocols compromise Canadians' privacy?

Question 1 has been addressed in two ways. First, technical questions have been prepared for major service providers in Canada pertaining to how their infrastructure protects customer privacy. The questions have been sent to colleagues at the Digital Policy Branch for refinement. Second, CRC is developing the capabilities to allow Industry Canada, in partnership with service providers, to measure and assess the privacy protections of service-provider equipment.

Investigations about how Wi-Fi and telecom standard technologies can be used to maximize privacy have been conducted in order to answer Question 2. The role of backwards compatibility will be shown to be a weakness in wireless privacy. Communications protocols have been analyzed to identify the phases of operation where metadata is revealed.

Regarding Question 3, the feasibility of interception has become achievable for the average hobbyist or small organization due to the advent of inexpensive base station hardware and freely available source code implementation of commercial protocols such as LTE, GSM, Wi-Fi and others. This investigation has demonstrated metadata interception for GSM and Wi-Fi. CRC also has the capability to capture LTE metadata using professional tools which analyze the wireless communication packets between a slightly modified phone and a base station. Additionally, it is possible to inexpensively pose as a legitimate base station, to more actively interact with telecom customers in pursuit of private information.

To address Question 4, we observed that disparate sources of metadata gathered from the connection phases of telecom signals and Wi-Fi signals [9], may have limited value on their own. When processed and combined, however, this information can reveal a significant profile

of the user as well as their routine personal and business activities. Experimentation has shown the ease of accumulating metadata using inexpensive equipment.

Finally, it is useful to consider a few personal scenarios in which privacy concerns play a role. Investigations, including field measurements and experimental results, were made with these scenarios in mind:

- An organization wishes to track the whereabouts and habits of a group of people (e.g., key decision makers in a corporate or government organization). They can use inexpensive equipment in the public space to do this, and require little technological expertise beyond an undergraduate of computer science or engineering.
- Someone wishes to learn about a specific person (e.g., a CEO, celebrity, etc.), and deploys inexpensive equipment in the neighborhood where they live to collect details that can be combined with other information to reveal his/her activities.
- An organization wishes to track thousands of people in an urban area, and has some resources to deploy radio receiver devices throughout the city. They assess their eating, shopping and other habits, and how often they venture into the area. They analyze this data after six months, combine it with other information, and sell it to marketing firms for significant revenue given the accuracy of the profiles on each person.

The topics of this study have helped to answer the questions posed at the beginning of this chapter.

# 3.0 Telecom Equipment and Systems

# 3.1 Background

To address the possibility of privacy exposure in wireless communications, current generations of telecom standards have improved privacy protections over legacy systems. LTE (4G), for example, has improved protection measures in user authentication and data encryption compared with previous generations. When deployed properly, the ease of eavesdropping on application and network metadata is significantly reduced in the latest systems.

However, commercial equipment uses backwards compatibility to maximize coverage in regions where the newest systems are not deployed. Furthermore, all voice traffic in Canada is still transported through older-generation protocols. A direct payload of voice traffic within the LTE protocol (VoLTE) will be deployed progressively. The weaker privacy protections of previous-generation systems present a major privacy weakness, essentially acting as a continually open back-door, even into devices using the most modern and robust services.

Some of the metadata used in telecom systems is described in Appendix A. Metadata that is transmitted over the air contains the unique device identifier (IMSI) and temporary device identifiers (GUTI), where both IMSI and GUTI are defined in Appendix A. Other metadata is generated and used within the fixed infrastructure to support placing and routing calls, Internet surfing, and running applications. Metadata is required for wireless networks to operate, and is integral to the design and interoperability of the communications protocols.

# 3.2 Demonstration with GSM Systems

In the past, the average person would not have access to the internal workings of commercial wireless protocols that hold machine identifying information, IP addresses, locations, sites accessed, etc. These internal data and messaging configurations would be embedded within the chip that drives the mobile device and within the expensive base station infrastructure. The advent of free GSM and LTE software codes (see [6], [7], [8]) and inexpensive radio equipment now allow greater access to these types of metadata information. Free software for the newer protocols will be in less mature form than that of older protocols, but over time, hobbyists bring free software to remarkable levels of completeness. Investigative tools such as so-called IMSI catchers were extremely expensive and thus only available to governments, law enforcement and highly specialized security organizations. Today there are free and open source software tools for GSM and LTE base stations (see [6], [7], [8]) that allow low-cost base stations to be run on radio equipment costing less than \$1000 (e.g., National Instruments USRP radios). In Figure 1, for example, we see a fully functional GSM base station that is capable of accepting mobile devices. This allows the base station to capture device identification codes (e.g. IMSI codes) and service provider names, and to send out unexpected text messages that appear to arrive from any phone number. With these simple tools, smartphones of passers-by can be probed and in some cases, further manipulated into revealing personal information. Questions to address include the ease and depth of these third-party

telecom service interactions, and how wireless protocol designs may be modified or reconfigured to guard against such interactions.



Figure 1: OpenBTS GSM/2G base station with inexpensive radio hardware (in anechoic chamber at CRC to avoid interference with deployed telecom services).

Legacy communications systems such as GSM (part of the 2G telecom technologies) have less stringent protections on both metadata and message content. During communications, the metadata (including identifying words and unique identifiers) are completely unprotected. Backwards compatibility of mobile devices means that most devices will interact with GSM base stations and respond with IMSI metadata, even though some may not be subscribed to GSM service.

Demonstration results showing how metadata is detected using a low cost GSM base station, with free open source software, are shown in Appendix A.

# 3.3 Options Available for Industry Canada to Reinforce Telecom Service Privacy

Actions to better understand the extent of any privacy concerns stemming from technological sources within telecom systems in Canada can be taken, and efforts to address these privacy concerns are possible. Specific options for the Department to pursue are:

• Work in partnership with service providers to ensure that telecom infrastructure equipment deployed in Canada makes full use of the available security protections in all standards to improve the protection of privacy for users. These protections go beyond

basic encryption to settings for use of temporary IDs, duration between reset of temporary IDs, and other measures (see discussion, Appendix A).

- As service providers contemplate off-loading traffic onto unlicensed bands such as those
  used by Wi-Fi, there is concern that metadata detectability of Wi-Fi becomes an added
  weakness of telecom services. In response, the Department and industry can work
  together to establish an approach for Wi-Fi offloading that does not diminish customer
  privacy.
- Obtain technical knowledge on how mobile devices retailed in Canada can be configured
  to maximize security protections that are offered in the standards, thereby enabling use of
  the most effective protection offered by base stations. Note that this may be problematic
  for low-cost handsets, where engineering and testing of all aspects of standard
  conformance could be inferior to the quality control conducted on high-end handsets. It
  will likely be impossible to implement this measure on existing handsets.
- Ensure that mobile devices operate only in legitimate and licensed bands for their jurisdiction and service provider, yet allow them to continue to roam reliably. Although the hardware and chipsets are common to all markets for some devices, it might be possible to disable operation in out-of-jurisdiction bands through software configuration.
- Assess the effectiveness of improving privacy of wireless networks by limiting the
  retention period for metadata. This may apply to data collected by the service provider or
  by the application, via the service provider. This would be done in a manner to not
  interfere with lawful interception.
- Recognizing the weakness of legacy protocols in privacy protection, develop an approach to limit backward compatibility of telecom systems. This might include retiring legacy systems sooner, and/or ensuring that mobile devices retailed in Canada have a means to easily deactivate use of legacy systems under conditions set by users (i.e., in retail environments). Note that in many current handsets, legacy systems will still reveal unique identifiers even though legacy service is not provided. This is possibly due to the need to support E-911 services.

# 3.4 Measurement of Base Station Privacy Settings

For an assessment to be made about security and privacy protections in commercial networks, technology is needed to capture the relevant metadata. This information needs to be obtained and recorded at many cell sites using equipment of all service providers to facilitate comparison. This data can be used to compute metrics that measure privacy, which can then be used as a basis for comparison of privacy between the different service providers and in the different regions of Canada. Some information about metrics used for the GSM audit reported in [9] is known, but metrics for other systems will depend on specific features of the protocols and

have yet to be developed. Once the department has assessed the security and privacy protections of the currently fielded systems, this information can aid industry and the Department in determining whether such protections are sufficient.

Appendix B contains more technical information about the use of tools to measure metadata and therefore enable assessment of wireless privacy. Acquired results are also shown in Appendix B.

# 3.4.1 Options for Industry Canada to Assess Wireless Privacy of Telecom Infrastructure

In Table 1, the tools available for the Department to investigate privacy are listed, with approximate costs. Tools using inexpensive hardware and open source software will likely require technical support expertise within the Department, whereas commercially available tools usually come with external support. In either case, a person with expertise to evaluate and verify correct operation of the software (eg. undergraduate level) will be required to properly use the software and understand the results.

Table 1: Options of hardware and software tools for privacy investigations, reflecting

capabilities currently available at CRC.

Tool for Inexpensive Radio	Software Source and Cost	Hardware and Cost	Comments	
GSM Open Source	Free	USRP ~\$1K	Full access to metadata, limited support	
LTE Open Source	Free	USRP~\$1K	Full access to metadata, limited support	
Amarisoft LTE Commercial- Object software	~\$4.5K	USRP ~\$1K	Limited access to metadata, support	
GSM Map Project- Metadata Analysis, Object software [9]	Free	Mobile Phone \$400	No direct access to metadata, privacy assessed via metrics	
Proprietary Metadata Analysis Tool GSM, LTE, IS-95, 1xRTT	~\$20K	Use regular mobile phone via USB ~\$400	Full access to metadata, wide range of standards	

The assessment of the best approach to develop a technical capacity to measure privacy should be based on whether a small-scale deployable capability is desired, or whether a permanent nationally installed capacity is required. Then the price and flexibility tradeoff can be made between in-house development (giving flexibility on how metadata is reported and metrics are evaluated), versus off-the-shelf procurement.

(A-2018-00073) - Page: 22

# TECHNICAL STUDY ON PRIVACY IN WIRELESS NETWORKS

The LTE standard includes options for the "AES" crypto, and the older "SNOW 3G" crypto. Initial privacy audit measurements have shown, in Appendix B, Table 4 that of the seven LTE base stations within radio range of CRC, one uses the older crypto SNOW 3G and six use the latest crypto AES. Extensive measurements are needed to assess this element of privacy provided by base stations in other regions, and of the other service providers.

# 4.0 Unlicensed Wi-Fi Equipment Using 802.11 Standards

# 4.1 Background

Wi-Fi is a short-range wireless access technology which operates in the 2.4 GHz and 5 GHz unlicensed spectrum, but it is also under consideration in various parts of the world for other bands. Its range depends on a number of factors, but is generally less than 50 metres indoors and a few hundred metres outdoors. These ranges can be increased when using special hardware and antennas. Its use outside of licensed spectrum and its relatively simple operation have led to low-cost and highly integrated solutions, with quick adoption in all sorts of devices ranging from smartphones to TVs and cars. However, this technology has some deficiencies in terms of protecting the privacy of the people who own the devices.

Technical information about MAC addresses, the Wi-Fi protocol association process, and some measurement results for MAC addresses, are given in Appendix C. Metadata used by the Wi-Fi system includes the device's MAC address, which is transmitted over the air.

# 4.2 Privacy issues in Wi-Fi

Wi-Fi enabled devices and access points share a common wireless channel and communicate using a messaging scheme defined in the IEEE 802.11 standard. The messaging scheme includes management, control and data frames. The purpose of management frames is to establish a connection between the access point and devices, and maintain the connection. The management frames include beacon and probe-request frames. Beacon frames are transmitted periodically by the access points to announce the presence of a wireless network, whereas probe requests are transmitted by Wi-Fi enabled devices to request information from either a specific access point or all access points in the vicinity. Beacon frames contain the information about the wireless network, a unique identifier of the access point (MAC address) and the name of the wireless network (SSID). MAC and SSID are defined in Appendix C. Probe requests contain the unique identifier of the device (MAC address) and may also contain the name of previously accessed networks, depending on the chip manufacturer and the operating system of the device.

The Wi-Fi protocol currently uses a robust encryption and authentication mechanism to protect the user data in the data frames, but the mechanism is not applied to protect the metadata in the management and control frames. As a result, the management and control frames are not encrypted and metadata is transmitted in clear text. This can expose the unique identifier of the mobile device to any Wi-Fi capable receiver, which can then be tracked over time and location. Inexpensive Wi-Fi enabled devices exist and can be converted into a *sniffing* system to capture metadata in the Wi-Fi management and control frames, and identify the devices. In some configurations of mobile-device Wi-Fi, information about previous network connections is emitted by the smartphone or tablet while searching for a new connection (e.g., "...previously connected at Tim Hortons Wi-Fi, YOW Wi-Fi, ...").

Tracking of mobile devices using MAC addresses within a certain area (for example a shopping district) has become an activity that generates intense public interest by way of newspaper stories [10], and businesses are emerging where this location and identifier information is gathered, processed and sold for marketing and customer profiling [10]. Repeated measurements of MAC addresses within an urban area yield preferences for shopping, and information about how often an individual returns to the same business establishments. When merchants fuse this location information with purchase information, they can develop customer profiles that have added value over the individual MAC addresses. It would be possible to create associations of buying patterns between businesses using analytics that demonstrate, for example, how customers of Starbucks often visit Apple stores. Emerging services such as Google "Nearby" and Apple "Continuity" aim to create ecosystems of devices that are aware of the location and activities of the users to enable seamless transitions from smartphone to laptop, to tablet [11], [12] and beyond. These capabilities, which are intended to provide users with better service and enable productivity, are delivered at the expense of the network knowing the location, activities and context of users activities. The underlying technological enabler for these new capabilities is tracking and identification of mobile devices through their Wi-Fi and telecom service modems. Results shown in Appendix C contain a selection of laptops and mobile devices in which CRC has performed passive Wi-Fi identifier detection.

# 4.3 Test Results Obtained at CRC Campus

The measurement locations are indicated on the map of the Shirleys Bay campus, in the west of Ottawa. Indoor measurements were conducted in a ground floor office of Building 2A. Outdoor measurements, numbered Test 1 to Test 7, were made at increasing distances away from Building 2, with locations shown in the aerial photo in Figure 2.



Figure 2: Wi-Fi test measurement locations around Shirleys Bay campus of Industry Canada, Ottawa.

Measurement results are shown in Table 2, where we see the numbers of devices captured at each test location for the various time durations. For example, at test location 1, a receiver captured MAC addresses of 30 different Wi-Fi routers and 7 different mobile phones during a 5-second test. At test location 4, a 60-second test yielded 11 routers and 10 mobile phones. The GPS location of the interceptor equipment is also recorded to support future analytics and fusion. Notice that as the test equipment was located at increasing distances from the office building, the number of devices in radio range was reduced. The shorter duration tests also identified fewer MAC addresses than the longer tests.

Table 2: Field trial results of Wi-Fi measurements at CRC targeting MAC addresses of mobile devices. Reported are numbers of devices captured.

	5 Sec.	10 Sec.	20 Sec.	60 Sec.	GPS Coordinates
Test 1	30 (# fixed routers detected)	34	36	N/A	45.346566, -75.884054
	7 (# mobile devices detected)	10	27	N/A	
Test 2	18	20	21	N/A	45.346905,
	7	13	23	N/A	-75.886728
Test 3	6	7	8	10	45.347689,
	4	6	6	29	-75.889413
Test 4	9	9	10	11	45.348835,
	2	2	1	10	-75.891055

TECHNICAL	STUDY ON	PRIVACY IN WIREL	ESS NETWORKS
LECHNICAL	וט זעטוכ.	PRIVACT IN WIREL	ESS NE I WURNS

Test 5	7	7	7	8	45.349491,
	0	2	3	4	-75.894713
Test 6	1	2	2	2	45.349552,
	0	0	0	0	-75.89864
Test 7	1	1 1	1	2	45.350909,
	0	0	0	1 1 1	-75.901151
Indoor	32	38	43	47	45.346226,
	7	9	22	42	-75.884685

As noted from the test results, the number of detected devices decreases as test locations are further from the building, and increases with test-duration time. Relating these results to the vehicle scenario, it is possible to assume that a moving vehicle will be in radio range for a shorter period of time, resulting in fewer captured MAC addresses. However, as this table shows, it is still possible to obtain some MAC addresses within 5 seconds.

Appendix C contains details of the field testing of the collection of Wi-Fi metadata, and a description of how the metadata is interpreted and used to compromise privacy.

# 4.4 Options Available for Industry Canada to Reinforce Wi-Fi Privacy

A weakness in Wi-Fi is the use of unencrypted MAC addresses. The same MAC, if detected by an eavesdropper at two different locations and at different times, discloses travel information of the mobile device. It could also be used to identify home and work locations and thus, the owner of the device if the eavesdropper is able to assess when the device stops moving for long periods of time (for example, overnight).

Technical solutions for protecting Wi-Fi parameters exist and have appeared in academic literature dating back to early 2000 ([13] through [17]), which have in common methods to hide unique identifiers from the on-air transmissions. The problem is that commercial standards do not mandate use of these solutions today because of the complexity to implement and test these features, and how the configuration required by the user might become more comlpex. Product developers likely prioritize efforts on features demanded by customers such as higher data rates instead of privacy. Recent progress by Apple to implement MAC randomization in iOS8 [18], which hides the true device identifier while on air, is positive and will be part of the solution to address wireless privacy. These types of solutions are not widely adopted, however, due to the need to modify commodity chipsets in some cases.

CRC has technical expertise to design and implement software or hardware solutions that are able to protect the MAC and SSID parameters, and improve the privacy of Wi-Fi devices. However, implementing such solutions in Wi-Fi devices would require changes to Wi-Fi industry standards. Nevertheless, CRC could work in partnership with industry and academia to raise awareness of the technical aspects of privacy issues and support industry participation in the development of new standards by technology demonstration.

Some specific technical options for addressing Wi-Fi privacy are:

- Document how tracking of MAC addresses works, so people may use their mobile
  devices with caution, including disabling Wi-Fi in scenarios where privacy concern is
  greatest. This will be balanced by users' desire for convenience and low-cost service.
- Enable use of a temporary MAC, or a proxy MAC. This would sever the relationship between MAC and the device as long as the proxy changes fairly regularly. There would be a need to address the association phase, prior to assigning the proxy.
- Ensure retail products sold in Canada have settings whereby past hotspots visited are not broadcast while searching for connection.
- Document how products can use the sufficiently powerful encryption that lies within the 802.11 standard family.
- Create an app for the public that gives users, in real time, a sense of what wireless access
  metadata is being transmitted within the processing capability of the device, and with
  what level of protection. This app could also allow users to control the way hotspots are
  searched.
- Obtain the technical information that would be required to create a "do not track" register
  in a manner that can be adopted by the emerging "mobile location analytics" industry.
  Such an approach has been initiated in the U.S. by the Future of Privacy Forum
  (<a href="http://smartstoreprivacy.org/">http://smartstoreprivacy.org/</a>).

# 5.0 Fusion – Enablers of Smart Services in Connected Environments

The capabilities arising from broad wireless deployment and the emergence of sufficient processing to support intelligent apps enable services that provide automated content-based personal assistants. Google's upcoming "Nearby" [11] and Apple's "Continuity" [12] services may be early versions of a type of service utilizing "sensed" environmental parameters, a person's historical data to identify a user's needs in order to improve productivity. It opens a new set of interactions between a person, nearby people, places and things.

Typical examples include parking reminders, proper time management, bill payment reminders and similar services that have already been released. Other optional services, such as "remind me when I'm with this person" or "report game scores silently if I'm stuck in a meeting" are coming, and the useful ones will operate with minimal human intervention. What recent history teaches us is that the game-changing app of this type will be impossible to predict, and will revolutionize perceptions of mobile connectivity (eg. consider how smartphone GPS has become prevalent, and was not perceived to be a need by many prior to availability of this navigation feature).

Applications that provide such productivity enhancements will require support by hardware and wireless communications in the mobile device. For example, when activated, Google's upcoming Nearby service will periodically turn on the Wi-Fi, Bluetooth and audio microphone without user involvement to study the environment, and identify other devices, contacts, people and objects in the vicinity. The service also reads user's configuration data, reports location with history, and determines behaviour and action history to establish the next recommended steps to achieve its tasks.

The privacy concern arises from the wireless location tracking and sensed interactions with other people or machines. The promulgation of this tracking data by the service provider or the applications (e.g., Google), and possibly beyond the application, will determine privacy. Metadata that is not, on its own, markedly private in nature may become more personal as fusion is used to map this information to the user.

The technological enabler of personal productivity applications is effective data analytics and data fusion, bringing together disparate information from as many independent sources as possible to create a very personal record of activities. Eventually, electronic records with sufficient detail to reveal personal identity will be available to customers of the analytic and fusion process (e.g., the street address where the mobile device rests during the night is highly likely to lead to the home address and family name).

The question is then, at what point during the fusion operation does the generation of an increasingly personal profile of the mobile-device owner become sufficiently personal that it is protected under the Privacy Act. Is the fusion and analytic process sufficiently regulated at the present time, in light of the anticipated effectiveness of this post-processing? The question is also

(A-2018-00073) - Page: 29

# TECHNICAL STUDY ON PRIVACY IN WIRELESS NETWORKS

about protecting these new sources of personal information that have been derived from wireless devices.

# 5.1 Options to Manage Fusion and Analytics Effectiveness

An approach to reduce the viability of data analytics and fusion is to weaken the connection between the unique identifiers: the IMSI for telecom service and MAC for Wi-Fi. This means that temporary IDs such as the GUTI in LTE would be used and reassigned often, while proxy MAC address would be used for Wi-Fi. This would require technological developments to standards and products. While these steps would reduce efforts to track devices, it could still be possible to track users and their habits by other means such as through the applications listed above. These apps use wireless access metadata, but rely more on application metadata that they collect, store and fuse. This reinforces the question posed above regarding how to protect and regulate these new sources of information.

# 6.0 Summary of Findings

There are clearly bases for concern about wireless privacy driven by the emergence of inexpensive and highly capable radio units, and of freely available software implementations of communications protocols on the Internet. Investigations in this project allow us to address this topic by way of considering basic questions pertaining to wireless privacy.

# Question 1: What is the level of privacy protection for wireless service users in Canada? How does it compare to other nations?

This study was initiated in response to disturbing news stories about how the privacy of wireless devices is actively overcome in pursuit of tracking movement and shopping patterns, and how companies, including in Canada, are innovating in this area [10]. In addition, systems are under development that make use of proximity information, in essence using the location, tracking and history of smart devices to devise useful services for customers [11], [12]. These developments are possible due to the low levels of privacy protection inherent in the radio protocols. Experimentation with inexpensive equipment was conducted to assess how someone with few resources and modest education could take advantage of accessible radio equipment and free software from the Internet. In this context it has been found to be easy to breach privacy by obtaining unique device identifiers from smartphone and tablet devices used by people in personal and business scenarios.

Based on initial measurements on telecom service conducted around Ottawa and analyzed by the GSM Map Project [9], Canada's wireless privacy is comparable with the US and behind Western Europe. More testing will reveal the state of privacy over the full geography of Canada. CRC can provide technical support to Industry Canada for the development of privacy metrics for wireless telecom services that can be applied to Canada and to other nations to establish international comparisons.

# Question 2: Where are the weaknesses for potential access to private information within the established wireless services in Canada? Can users play a role in securing their own device information?

There are weaknesses in Wi-Fi and Telecom technologies that allow unique identifiers of mobile devices to be surreptitiously taken using economical hardware and free software from the Internet. The feasibility of doing this has been demonstrated by CRC using the aforementioned hardware and software, and has been reported within this study. All devices tested, including corporate devices, were shown to provide unique identifiers to equipment that fits in a backpack. This technology can be setup and used by hobbyists, or by someone with a few years of university or college training. Service providers themselves have ready access to unique identification codes of their customers' mobile devices (Wi-Fi and telecom), and to those of customers of other service providers who query their networks searching for access.

At the point of identification, the interceptor or the service provider can stamp these identifier codes with additional metadata information such as local time and location. Without decrypting private communications, this information can be made available to data analytics and fusion companies as source material for their processing. The processing techniques are devised to cross reference data sources and allow the device identifier data to be associated with the person holding the device. There are options for service providers and users to secure their information, such as proxy identifiers that mask the unique identifier. The use of these techniques required specialized technical expertise to install and configure and therefore they are not widely used.

# Question 3: What are the potential scenarios for the interception of signals for common wireless technologies in Canada?

Users with minimal technical expertise can use inexpensive hardware and software tools and methods described on the Internet to capture the unique device identifiers of mobile devices while remaining unseen and undetected. This can be done from outside a building, to a pedestrian, or to a passing vehicle under certain conditions. These identifiers, combined with location and time information, can be sold to companies with expertise in data and identity fusion, and analytics.

The technical "recipes" to do this can be found quite easily on the Internet, and the technical expertise for Wi-Fi and GSM/2G interception is estimated to be equivalent to that of an undergraduate student. As free software implementations become available for later standards such as LTE, the expertise for manipulating these systems is also becoming widely known and described on the Internet. The concern is that once the methodologies are known, they can be easily copied and replicated by anyone. Given the rapidly increasing availability of interception tools, disruptive scenarios can be envisioned. It then becomes feasible to blanket an urban area to track the location and activities of masses of people with low-cost communications reception hardware.

# Question 4: How can the collection of information and metadata from wireless protocols compromise Canadians' privacy?

Information and metadata collected from wireless devices can be used in data fusion where single measurements, of little privacy concern on their own, are combined to create a meaningful picture over time. This processing reveals profiles of people's habits, preferences, travels and sometimes identities. Inexpensive and easy-to-use technology is disruptive by enabling automatic collection of metadata from thousands of people in urban environments.

Investigations using equipment of the class available to third-party interceptors can show the extent of metadata collection by organizations. Some telecom and widely deployed Wi-Fi standards have been assessed. It has been demonstrated that it is possible to detect unique identification codes without the target fully connecting to any service, or taking any cooperative action. Backwards compatibility of mobile devices, in place to maximize reliability of wireless service, is shown to be a privacy weakness since legacy systems contain the weakest privacy protections.

# 6.1 Technical Options for Action on Wireless Privacy

Possible actions of a technical nature by government to address wireless privacy include:

- 1) Engage service providers for discussions on privacy in wireless networks in Canada. The department can obtain information on privacy protections in relation to peers (i.e., "to complete the map" for Canada) using test software developed and/or integrated by CRC with inexpensive hardware (which is therefore ideal for widely fielded equipment) or using professional test equipment (having greater cost per unit).
- 2) Partner with industry to increase the level of wireless privacy in Canada. Develop an action plan to, for example, establish best practices of factory settings for equipment and consumer devices retailed in Canada through engineering and certification, regulation, or other policy options, and identify how telecom and Wi-Fi standards can be configured within infrastructure equipment to maximize wireless privacy. This may include advice on the impact that technical settings can have on wireless privacy in retailed mobile devices.
- 3) Establish parameters of privacy metrics with industry players, other government departments, and other countries. Note that metrics measuring wireless privacy for the major telecom standards are not universally accepted, nor accepted for comparison purposes. This can be done with the support of CRC and industry expertise, and with other nations who have similar concerns.
- 4) Work with industry to steer international standards towards enabling greater protection of privacy in wireless networks.
- 5) CRC will remain available for consultation on any technological possibilities regarding privacy in the wireless domain.

At the request of the CRC Research Advisory Board, CRC can provide some technical expertise required towards these activities. CRC can also aid in the selection of protocol test tools and analysis tools for procurement that would be used in investigation of these topics.

### 6.2 Personal Scenarios

Finally, regarding the personal scenarios introduced in Section 2, the technologies that have been evaluated and tested are part of the overall story on privacy, whereby metadata can be obtained from people as a result of their use of wireless services, and the metadata is the fuel for data analytics and data fusion. Methods to obtain the metadata vary, and depend on the wireless services used as well as on the scenarios.

One hypothetical example has a person in an urban setting, shopping, stopping for coffee, and shopping some more. Based solely on metadata collected from any Wi-Fi and mobile telecom device, results of this short study demonstrate the feasibility of compiling a record of businesses visited. By using analysis of long records of measured metadata taken in the shopping area, a record of how often various businesses are frequented is obtained for many customers. Another source of information of the same activities is a transaction record for Air-Miles (or other such loyalty program), where a transaction made at that same location and time can be data-mined. As these two records are fused together, the previously anonymous metadata, time and location is uniquely mapped to personal identity, amount purchased, and other information known by Air-Miles, for example. This is how anonymous metadata, retrieved from the wireless link, is transformed into personal information by analysis and fusion. It is likely that if customers of loyalty cards were aware of what could be done with their loyalty data, they would not "tick" the box allowing use of their shopping data, leading to the observation that public awareness should be part of any actions to strengthen wireless privacy.

In conclusion, there is no single "smoking gun" enabler that, if solved technologically, would deliver total privacy to wireless users. Rather, addressing the problem requires an ecosystem of solutions developed by regulators, industry, and R&D organizations that, when taken together, will deliver a desired level of privacy protections.

# References

- [1] Site Aims to Help Users Opt Out of Smartphone Tracking <a href="http://blogs.wsj.com/digits/2014/02/18/site-aims-to-help-users-opt-out-of-smartphone-tracking/?mod=WSJ">http://blogs.wsj.com/digits/2014/02/18/site-aims-to-help-users-opt-out-of-smartphone-tracking/?mod=WSJ</a> hpp sections tech
- [2] FTC Staff Report Recommends Ways to Improve Mobile Privacy Disclosures <a href="http://www.ftc.gov/news-events/press-releases/2013/02/ftc-staff-report-recommends-ways-improve-mobile-privacy">http://www.ftc.gov/news-events/press-releases/2013/02/ftc-staff-report-recommends-ways-improve-mobile-privacy</a>
- [3] How You Might Be Tracked for Ads in a Post-Cookie World <a href="http://blogs.wsj.com/digits/2014/01/28/the-ad-industry-envisions-a-world-after-web-cookies/">http://blogs.wsj.com/digits/2014/01/28/the-ad-industry-envisions-a-world-after-web-cookies/</a> and <a href="http://www.iab.net/media/file/IABPostCookieWhitepaper.pdf">http://www.iab.net/media/file/IABPostCookieWhitepaper.pdf</a>
- [4] Government of Canada, "Digital Canada 150", <a href="http://www.ic.gc.ca/eic/site/028.nsf/eng/h">http://www.ic.gc.ca/eic/site/028.nsf/eng/h</a> 00569.html, 4 April 2014.
- [5] Office of the Privacy Commissioner of Canada <a href="www.priv.gc.ca">www.priv.gc.ca</a>, <a href="https://www.priv.gc.ca/resource/topic-sujet/owp-pvplrsf/index\_e.asp">https://www.priv.gc.ca/leg\_c/interpretations\_02\_e.asp</a>.
- [6] Open Source GSM base station software OpenBTS.org
- [7] Open Source LTE base station software <a href="http://sourceforge.net/projects/openIte/">http://sourceforge.net/projects/openIte/</a>
- [8] Open source base station portals myriadrf.org bellard.org
- [9] "GSM security country report: Canada", GSM map project, Security Research Labs Berlin, June 2014, map: <a href="https://www.gsmmap.org">www.gsmmap.org</a> .
- [10] Wi-Fi tracking and analytics  $\frac{http://getturnstyle.com,}{http://www.theguardian.com/technology/datablog/2014/jan/10/how-tracking-customers-in-store-will-soon-be-the-norm}, <math display="block">\frac{http://www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?pagewanted=all&r=0$
- [11] Context Awareness Google "Nearby" <a href="http://gizmodo.com/report-google-nearby-to-bring-android-next-level-conte-1587541353">http://gizmodo.com/report-google-nearby-to-bring-android-next-level-conte-1587541353</a>
- [12] Context Awareness Apple "Continuity" <a href="https://www.apple.com/ios/ios8/continuity/">https://www.apple.com/ios/ios8/continuity/</a>

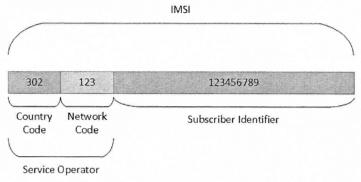
- [13] M. Gruteser and D. Grunwald, "Enhancing location privacy in wireless LAN through disposable interface identifiers: A quantitative analysis", in *Proc. of ACM WMASH*, Sept.2003.
- [14] T. Jiang, H. J. Wang, and Y.-C. Hu, "Location privacy in wireless networks", in Proc. of MobiSys 07, June 2007.
- [15] J. Lindquist, T. Aura, G. Danezis, T. Koponen and A. Myllyniemi, "Privacy-Preserving 802.11 Access-Point Discovery (full version)", Microsoft Research Technical Report, MSR-TR-2009-7, January 2009.
- [16] <a href="http://appleinsider.com/articles/14/06/09/mac-address-randomization-joins-apples-heap-of-ios-8-privacy-improvements">http://appleinsider.com/articles/14/06/09/mac-address-randomization-joins-apples-heap-of-ios-8-privacy-improvements</a>
- [17] https://datatracker.ietf.org/doc/rfc4941/
- [18] http://www.engadget.com/2014/06/09/ios-8-wifi-privacy/
- [19] J. Gurnick, SITT- CRC SME on LTE.
- [20] "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); General Packet Radio Service (GPRS); Service description; Stage 2," ETSI TS 123 060 V11.9.0 (2014-03), p.81.
- [21] General packet radio service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access, ETSI TS 123.401 v11.9.0 (2014-03), p.85.
- [22] UMTS metadata monitoring source code <a href="http://umtsmon.sourceforge.net/index.shtml">http://umtsmon.sourceforge.net/index.shtml</a>
- [23] Cisco Systems, "Architecture for Mobile Data Offload over Wi-Fi Access Networks", Cisco Public Information, 2012, pgs 1-23.

# Appendix A: Technical Information about Telecom System Protocols and Revealing Unique Identifier

# A-1 Identifiers Used in the LTE System

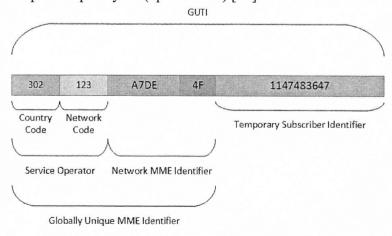
The IMSI is a unique identifier that resides in the SIM card of the mobile device and within the subscriber repository within the telecom network. When attaching to a new network, the IMSI is transmitted to the base station with no privacy protections. The IMSI is used by the network to authenticate the new user.

IMSI: International Mobile Subscriber Identity (64 bits) [19]



In the LTE architecture, users are subsequently given a temporary ID, referred to as the GUTI, to use as a privacy enhancing replacement for the IMSI. All further attachment procedures are attempted with the new GUTI. While the GUTI is a unique identifier to the mobile device, the flexibility of the system to provide new GUTI addresses to devices can obscure the unique relationship between the GUTI and the user as long as the GUTI is periodically re-assigned.

GUTI: Globally Unique Temporary ID (up to 80 bits) [19]



### A-2 Use of Metadata in Network

It is inevitable that not all network and communication control information can be easily encrypted for protection given the mobile and ad hoc nature of commercial systems. A commonly targeted piece of metadata is the unique ID of the device or user, known as the IMSI (International Mobile Subscriber Identity) that is sent by the smartphone to the base station to establish communications. The IMSI, when recorded, can be monitored to derive where and when devices are located. In LTE, a temporary ID (GUTI- Globally Unique Temporary ID) is used after the initial attachment process and privacy is enhanced when the temporary ID is reset periodically to erase traces tying the GUTI to a mobile device.

Definition and specifics on the generation and use of IMSI and GUTI are made in the LTE telecom standards. Implementation choices in commercial base station equipment govern how often GUTIs are reset, and the level of security protection that is offered by encryption. Base station equipment manufacturers and service providers have complete latitude in how aggressively they protect privacy by selecting the options used within the standard. For example, if the GUTI is rarely reset it becomes a de-facto permanent ID for the mobile device and can be tracked. Alternatively, if encryption is not used then every time a temporary ID is reset, the "old" and "new" values are easily detected and cross-referenced with the IMSI by listening to the protocol exchanges on the air.

The possible strategies by which communications protocols can be used to detect metadata will depend on how many of the protection options are in use on both the base station equipment and the mobile device. While it is clear that privacy protections have been improved in the newer standards, these features are all optional and may not be implemented or configured for use in actual deployments.

By conducting independent measurements and analysis of fielded base station equipment (i.e., measurements not requiring cooperation of the service providers), the actual protections that are in place can be identified. Then the state of wireless privacy protections in any region can be assessed.

### A-3 Mechanisms in Telecom Protocols Whereby IMSI is Revealed

Whenever a mobile device joins a wireless service provider network, the IMSI is sent to inform the network of the request to "attach." The service provider then uses this unique ID to verify that the mobile device belongs to a customer prior to completing the attach procedure. Following the attach procedure, the encryption is initiated, completely protecting all further wireless communications. The weakness is in the initial attach phase of the protocol where the IMSI is sent in unencrypted form. It may be possible for someone to take advantage of this weakness using a passive LTE receiver or an active rogue base station (i.e., one that uses transmit and receive).

### A-4 Passive Scenario: Use of LTE Receiver

The attach procedures for a GSM and LTE network are shown in Figure 3 and Figure 4 respectively. In both cases, the IMSI is sent unencrypted during the "attach request" in order to authenticate the user. Since this is sent unencrypted, it may be possible to obtain this information using a passive LTE receiver.

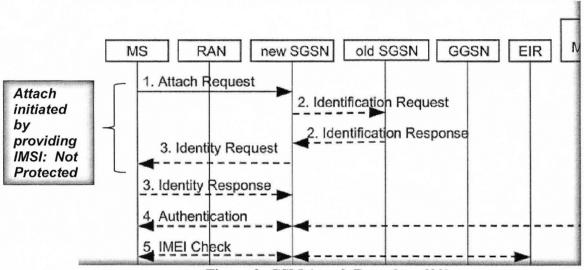


Figure 3: GSM Attach Procedure [20].

Commercial LTE receivers are available but are generally extremely expensive and cost prohibitive for most. Nevertheless, the revolution in inexpensive commercial radio equipment and software-defined waveforms now allow someone to build their own LTE receiver, for the purpose of intercepting the IMSI, using open source LTE software and programmable radio devices such as the USRP mentioned earlier. This would certainly not be an easy feat and would require some tweaks to both the software and radio platform for the device to synchronize and receive data from nearby cell towers. Once the process is completed, however, it could then be readily copied and replicated at low cost. Such units could then be widely deployed to cover any geographical area, to passively obtain metadata information.

In this scenario, the LTE receiver would be located near a legitimate base station to monitor the back-and-forth protocol exchange. By simply listening to publicly transmitted signals, the receiver would then capture the IMSI, which is transmitted without encryption. Since no RF transmissions are made in the process of collecting the IMSI, it would be very difficult to detect, and would likely be seen as a low-risk activity since it involves no unauthorized use of licensed spectrum. There is then the possibility that this approach is deployed widely in an urban environment, targeting a specific type of user, such as regular shoppers.

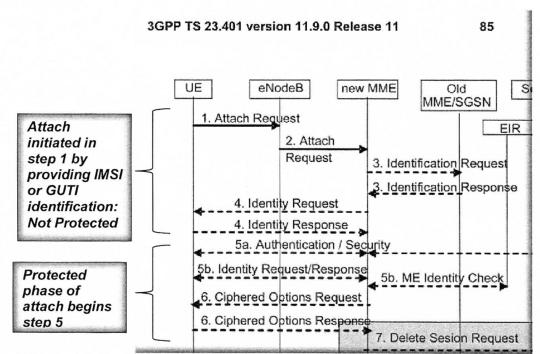


Figure 4: Segment of LTE-attach procedure, IMSI or GUTI are transmitted unencrypted [21].

As seen in Figure 5, the content of communications after the attachment phase is protected, in principle, by encryption. However, it is still not clear if this protection is universally applied. In cases where security protections are not applied, the use of temporary identifiers for mobile devices becomes ineffective. Figure 4 shows how a temporary ID is assigned, in steps 17 through 21. When messaging is not protected by encryption, the temporary ID can simply be cross-referenced with the IMSI by message analysis. For this reason it is imperative for privacy that the encryption protections provided in the LTE standard are verified to be active in deployed base stations.

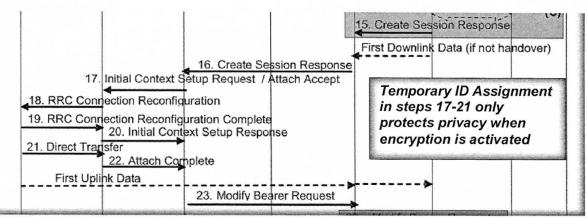


Figure 5: Segment of LTE-attach procedure where temporary address is designated [21].

### A-5 Active Scenario: Use of Base Station to Draw Out Mobile Device Identifier

Instead of using an LTE receiver to passively obtain the IMSI, an active eavesdropper might be eager to accumulate information and therefore will pose as a legitimate base station using open source LTE code and programmable radios, taking advantage of the mobile device's conformity to the protocol to "draw out" the IMSI at will. In this scenario, the licensed spectrum is used in an unauthorized manner. This process can be achieved within a few seconds, however, making this unauthorized transmission difficult to detect.

Since country codes and network codes are publically available, the rogue station could be configured to mimic a known service operator's network. It may then broadcast a seemingly valid LTE reference signal into the open in the hope that mobile devices might be drawn to connect to it. Since LTE uses mutual authentication, these devices will ultimately not be able to complete the connection process. However, since the mutual authentication occurs after the IMSI is sent out, the rogue station would be able to obtain the IMSI, as well as other parameters related to the propagation conditions of the receive signal.

In order to bypass the mutual authentication, the rogue base station could also be configured as a GSM base station. Most devices support backwards compatibility and may be drawn to connect to a legacy system, particularly if no other signal is available. For instance, this could be installed in an indoor mall or office area where network providers generally have low signal.

The active scenario involves unauthorized use of licensed spectrum, and would be viewed as a risky activity if used often because of the detectability of the rogue base station by the service provider. It is therefore likely that this approach would be used in pursuit of specific "valuable" targets (for example a CEO), and this activity would not be deployed in a widespread manner.

It may be possible to minimize the risk of detection by using spectrum in the bands where commercial mobile phones are active, but not actually licensed in Canada. Most phones today support multiple bands including some that are not typically used in Canada. In fact the 3GPP specifications list a number of valid GSM, UMTS, and LTE bands, not all of which are applicable to Canada. As a result, it may be possible for the rogue station to operate very effectively in international bands, away from frequencies used by Canadian carriers.

Tests done at CRC and described below in Section A-7 follow this above approach, where an international GSM frequency was used in a controlled laboratory environment. As is evident in Table 1, most phones were still able to connect to this network. Furthermore, experimental results based on test conducted at CRC have also shown that even when a service provider of a

particular system does not offer the GSM service, their mobile devices will react to metadata collection probes using the GSM system.

### A-6 Test Configuration for GSM IMSI Testing

The device used is Range Networks Development Kit, which includes:

- Modified USRP;
- Laptop;
- OpenBTS free source code for GSM [9];
- Antenna.

The test equipment is described at http://www.rangenetworks.com/#!professional-development-kit/cuy3

The antenna used is provided by National https://www.ettus.com/product/details/VERT900, https://www.ettus.com/product/details/VERT2450

Base Station downlink frequency is 900.4 MHz.

Base Station Configuration Settings: Primarily "Default", with specific values

Control.LUR.OpenRegistration,.\*

GSM.MS.Power.Max,29

GSM.Radio.Band,900

GSM.Radio.C0,52

GSM.Radio.PowerManager.MaxAttenDB,70

GSM.Radio.PowerManager.MinAttenDB,50

GSM.Radio.RxGain,56

GSM.Radio.RSSITarget,-57

MNC = 01

MCC = 001

GSM 04.08, param RACH, field AC, byte 3, bit 3 set to 1 (Emergency call not supported).

### A-7 Demonstration Results for GSM Testing

Tests were conducted at CRC to assess how many, from a pool of currently used mobile devices, would connect to a base station that was specifically configured to not advertise itself as a known Canadian or international network operator.

The open source GSM/2G base station was configured as follows:

- GSM/2G development network;
- 911 service not provided;
- Using a frequency not commercially available in North America;
- Low transmit power.

By using frequencies not used for service in Canada but still supported in most mobile devices sold in Canada, the test aimed to show how readily mobile devices will initiate a connection, even with a base station that is unknown when this base station provides the only available signal in the area. Despite this very cautious approach, all mobile devices tested provided their IMSI unique identifiers over the air to the test base station.

Table 3 contains the complete list of the tested devices along with their respective service provider information. This was accomplished without users having to press any keys or buttons on the mobile devices to select the base station. All of the information in the service provider and IMSI columns were obtained without the knowledge of the test subjects (CRC employees who graciously volunteered their mobile devices for testing), although the IMSI numbers and service provider indicators were not included in Table 3 for privacy reasons. The system frequency used by the base station is not one used by any of the service providers in the list, yet connection attempts were made. The devices continually scan for base stations, irrespective of whether the owner's service provider makes use of the GSM/2G bearer.

Some of the service provider codes obtained in the tests were for carriers that do not offer GSM service, yet the devices still connected to the GSM station and revealed their IMSI. In Table 3, the HTC One and iPhone 4 initially revealed their IMSIs. The test was then repeated after the owners of the mobile devices disabled 2G support on their phones. The IMSI was not revealed after this configuration change. This shows that it is possible to improve user privacy by disabling support for legacy telecom systems since backwards compatibility of modern mobile devices offers a "back door" to the enhanced privacy protections that have been built into the newer standards like LTE. However, disabling the backwards compatibility may harm mobile connectivity in some areas.

Table 3: Mobile devices making IMSI identifiers available over the air without connecting to service.

IMSI Provided
Yes

In the photo in Figure 6, the size of this GSM/2G base station hardware height relative to the diameter of a Twoonie coin is shown. This hardware was used for the tests reported in Table 3. Given its small size, it is possible to place it into a small container such as a backpack, for deployment at a location where a potential specific target is found. Note that the outer case contains unused space. It is possible to further minimize the size of this hardware.

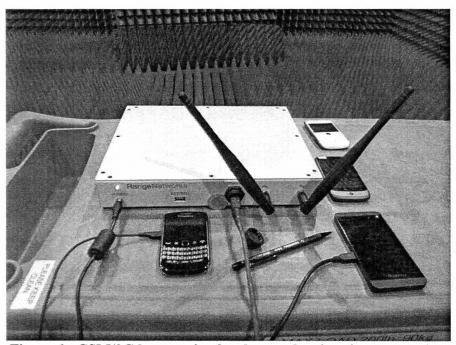


Figure 6: GSM/2G base station hardware, showing size perspective.

The hardware used for the current testing at CRC (Figure 1 and Figure 6) is a GSM/2G base station. The identical hardware and form factor can also operate as an open source LTE base station using software for an LTE system [7], although the open source LTE software is not yet as well tested and mature as the GSM/2G software. Such a software-defined system could indeed attract mobile devices using several telecom service standards as a way to gain knowledge of the IMSI, and different specific strategies will likely prove more effective against specific mobile devices.

It should be noted that this test was performed in a controlled laboratory environment where the rogue base station provided the only available signal in an enclosed area. In normal circumstances, it is known that devices prefer to connect to their own wireless service provider even if other better signals are available. As such, it is unlikely that this scenario will work when other signals from legitimate service providers are available. Nevertheless, it is possible to place the base station in an area known to have extremely poor signal reception such as inside office areas or certain malls. Without other strong signals, mobile devices will be drawn to connect to it.

# Appendix B: Equipment for Independent Measurement of Base Station Privacy Settings

Service providers engineer cell sites according to their business priorities. Some of the settings and configurations of the base station equipment used for servicing their customers are set based on default values, while others are chosen for specific reasons. Mobile devices need to know these settings to communicate, and so the values of the relevant settings are provided to the mobile device in the form of metadata exchanged during the initial call-attachment procedure. These metadata impact the privacy of users as they dictate the encryption settings, and when a temporary ID is reset. An investigation into how telecom base stations are configured, and how the wireless access metadata sent by these base stations impact the privacy of users, would benefit the Department.

CRC has portable tools that have the capability to access metadata for the major commercial wireless systems, including GSM(2G), UMTS(3G), LTE(4G) and others. Appendix B features graphics (Figures 7, 8 and 9) that show typical screenshots of a commercially available proprietary metadata analysis tool that extracts metadata from regular mobile phones via a USB cable. The metadata is presented in a graphical user interface format, where the fields are populated with data received by the mobile device subscribing to the wireless service provider. A single proprietary tool may not be the most efficient means to measure base station metrics nationally since hundreds of systems may be required for a persistent monitoring capability. For a deployed monitoring capability, the use of inexpensive radio equipment and software-defined base station technology would bring affordability and flexibility to the measurement tools; it would be feasible to widely deploy them to Industry Canada offices across the country. Investigations into the viability of this are still underway. Open source software implementation of the LTE standard is available [7] and could be a good basis for developing such a system. Source code for 3G metadata monitoring is available (see [22]), although this has not been evaluated by CRC to date.

The metrics that are used to assess privacy are ones that CRC would create based on the understanding of the technical issues of privacy. For GSM, the metrics used in the GSM map project are available (see [9]), and are appropriate for the legacy GSM service. Metrics for 3G and 4G would be different, and would be based on technical aspects of the newer standards. Initial findings on privacy in Canada of GSM are reported on the GSM Map and in a short report [9], however they are based on a very small set of measurements contributed by CRC to date on Rogers base stations around Shirleys Bay. Results of the limited privacy audit of GSM indicate that Canada lags France, Germany, Norway and Italy and is comparable to USA, Russia, Spain and India. Although comparative assessments of this sort that are made by international working groups are useful to understand Canada's wireless privacy, they are based on metrics that are not customized for Canada, and results are not broken down into regions of the country.

In Figure 7 the metadata is reported using a proprietary tool for GSM, where the A5/1 protection is shown to be enabled for the service. The full assessment of privacy is made from several such settings, and from analysis of the metadata over time. Figure 8 and Figure 9 show the metadata display format for LTE, and for the UMTS 3G system, respectively.

Cell Selection Parame	ters	Control Channel Descri	ption	Channel	Config	
Cell Reselect Hysteresis	6	IMSI Attach-Detach Allowed	Yes	Dedicated Channels		1
Maximum TX Power Level	5	Blocks Reserved Access Grant	0	Discontinuous TX Indicator		0
Minimum RX Signal Level	3	Physical Channels Supporting CCCH	1	Power Level		5
Power Offset	0	CCCH/SDCCH Channel Combination	Not Combined	Starting Time		
Power Offset Valid	Not Valid	Flag	NOC COMDINED	Ciphering Flag	Start (	Ciphering
lew Establishment Cause Indicator	1	Paging Messages MultiFrames	5	Ciphering Algorithm	A	5/1
Additional Reselect Parameter	SysInfo 16/17	T3212 Timeout	40	Parameter	After	Before
Indicator	Not Supported			Mode	Speech	Signalling Only
Cell Reselect Parameter Indicator	1	RACH Control Parame		Mode	Version3	Signaling Only
Cell Bar Qualify	0	Maximum ReTX	2	Channel Type	Half Rate	
Cell Reselection Offset	2	ReTX Interval	50		Traffic	
Temporary Offset	0	Reestablishment Allowed	Allowed	Subchannel Number	1	
Penalty Time	0 dB	Cell Bar Access	Cell Is Not	Timeslot Number	1	-
		Access Control Class	Barred 0	Training Sequence Code	3	-
Cell Information		Access Control Class	. 0	Hopping Flag	Yes	7.4
Base Channel Number	45191	Paging Parameter		Mobile Allocation Index Offset	0	•
Base Station Identity Code	1	Paging Multiframes	0	Hopping Sequence Number	29	-
Cell ID	0	Paging Platin aries	8	Frequency Count	3	
LAI - Cell	2308	Paging Data Valid	1	GPRS Inc		
Cell Selection Priority	236877644678	All Paging Blocks	No	RA Color	icators	
NCC Permitted	20	Paging Mode	Normal Paging		Crans	ted On BCCH
NCC Permitted	0	CCCH Group	0	Sl13 Position	2112 F0C9	tea on scon
E-80.6		Paging Group	8	AHR Info	emation	
Cell Options  Power Control Indicator	Not Set	Power Average Frequency	12	DL AMR		pplicable
Discontinuous TX	Not Set	- Onci Avelege i requerey		UL AMR		0 kbps
Radio Link Timeout	48			LERK	0.7	o voha

Figure 7: Selection of captured metadata using a proprietary tool from base station towers near CRC, for GSM-2G, indicating ciphering algorithm A5/1.

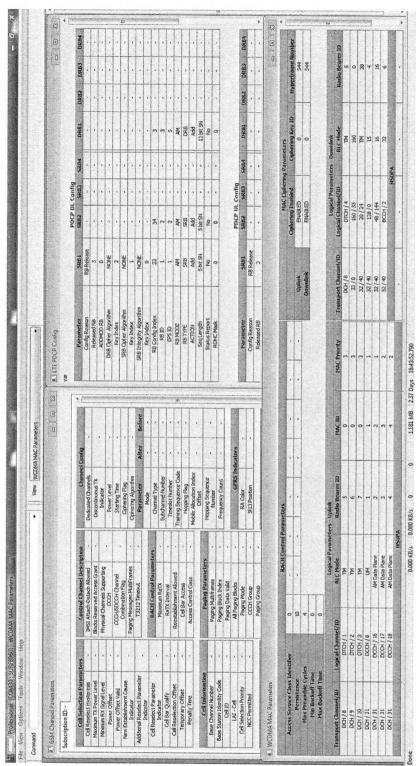


Figure 8: Selection of metadata categories using a proprietary tool from base station towers near CRC, for LTE-4G showing status of some privacy protectors.

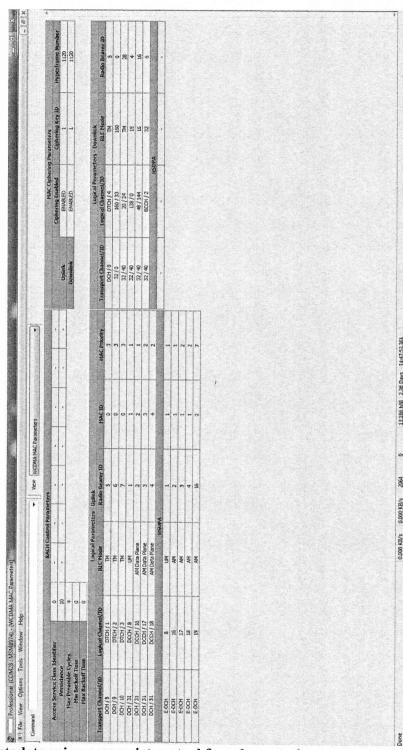


Figure 9: Selection of captured metadata using a proprietary tool from base station towers near CRC, for UMTS-3G showing status of some privacy protectors.

In Table 4 we see measurements taken in the vicinity of the Shirleys Bay campus at, west of Ottawa, for LTE service. Results are collected using the proprietary metadata detection tool and reported using the GUI format shown in Figure 8, where the various elements of privacy protection related to the downlink channel for the DRB Cipher, the SRB cipher and the SRB Integrity are shown. Interestingly, there are two different protection algorithms seen. The base station with CID 12801 uses the older SNOW 3G algorithm, while the rest of the base stations use the latest AES algorithm.

These results show that a larger privacy audit campaign is needed to explore what algorithms are deployed in different regions around Ottawa, and ultimately other locations. The audit of base stations for other service providers is also needed to quantify the prevalence of the older privacy protection algorithm SNOW 3G.

Table 4: Status of ciphering element of privacy protections on LTE base stations within radio range of CRC.

LTE Base	TE Base Ciphering		E Base Ciphering Algorithm		Received	Comments	
Station ID (CID)	DRB	SRB	Integrity	Power			
13268738	AES	AES	AES	-93dBm	Office 2B		
12801	SNOW 3G	SNOW 3G	AES	-85dBm	Outside power plant		
18182	AES	AES	AES	-91dBm	CRC Guard house		
8966	AES	AES	AES	-93dBm	Railway bridge Carling Ave.		
10132	AES	AES	AES	-63dBm	Bourke's on Carling		
19718	AES	AES	AES	-93dBm	Carling at Rifle Rd.		
18945	AES	AES	AES	-93dBm	Rifle Rd. near river		

### Appendix C: Wi-Fi Protocol Elements Impacting Privacy, and Results

### C-1 Unique Identifiers for Wi-Fi

The MAC address is a permanent hardware identifier that is associated with a network device. MAC addresses are 12-digit hexadecimal numbers. The format of the MAC is commonly presented as pairs of digits separated by colons, e.g., MM:MM:MM:SS:SS:SS, where the "MM:MM:MM" prefixes are associated with equipment manufacturers and the "SS:SS:SS" suffixes identify devices from each manufacturer.

The purpose of the MAC address is to act as an address for communications between network devices. When connecting to a wireless access point, the 802.11 protocol exchanges the MAC address over the air.

The access point also uses an SSID (Service Set Identifier) to identify the network access point, and is commonly referred to as the Network Name. The SSID is a string up to 32 bytes.

### C-2 Wi-Fi Association

When first establishing communications between a mobile device and a Wi-Fi service point (i.e., "association"), the question of privacy depends on the messaging that establishes the connection.

In the most basic configuration, the association phase is not encrypted, and is thus subject to eavesdropping by Wi-Fi capable receivers. The usual association process flow is shown in Figure 10.

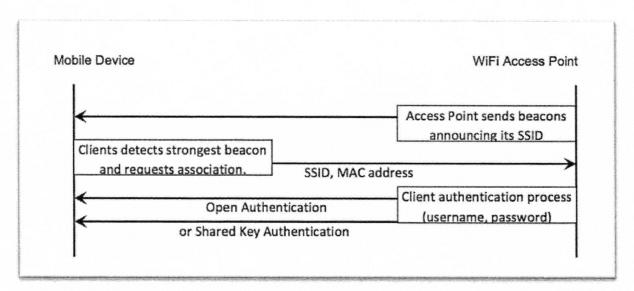


Figure 10: Association phase of Wi-Fi connection between mobile device and Wi-Fi access point [23].

There are two methods for client authentication of data payload: a) the Open Authentication which is not encrypted and b) the Shared Key Authentication with three encryption options (WEP, WPA WPA2) [23]. Currently, most commercial systems employ WPA2 for the shared key authentication, which has proven to be reasonably good in protecting users against eavesdropping of the data payload. Nevertheless, mobile users still disclose SSIDs and MAC addresses over the air, unencrypted, during association.

### C-3 Field testing

Initial field experiments conducted at CRC, in which MAC addresses were detected using a very portable and affordable (~ \$140) Wi-Fi measurement system and free open source Wi-Fi detection software available from the Internet, demonstrate the low level of investment and expertise required to obtain the MAC addresses of nearby Wi-Fi communications. The Wi-Fi testing hardware acts as a passive listener and records traces of metadata of all Wi-Fi devices within radio range, including fixed routers and mobile phones and tablets. The measurement scenario is depicted in Figure 11. No energy is transmitted, only received and recorded, making devices such as this very difficult to detect and control. In Figure 11 we see the mobile user, identified by their MAC address, on the mobile phone communicating with the Wi-Fi access point. Their radio signal propagates in all directions, and reaches the measurement device that records the metadata of the connections.

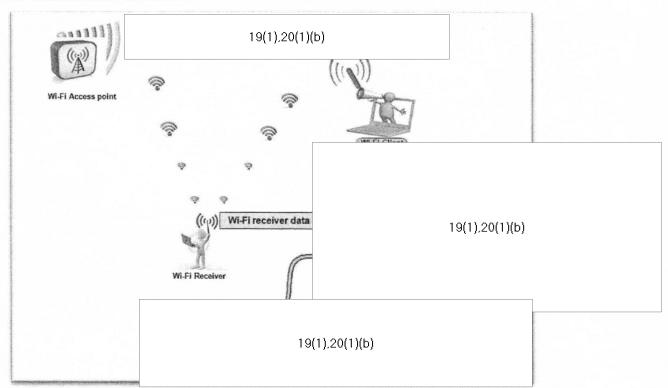


Figure 11: Scenario whereby a low-cost radio device can collect Wi-Fi metadata without knowledge of the users.

### C-3-1 Test Hardware Platform

As shown in Figure 12, the test platform comprises a main board (hardware "Router" RB433 + Wistron CM9), a Wi-Fi radio card and an antenna. Software used by the platform is open source and is hosted and controlled via a laptop. In principle, the controller could be any computing device, such as an android phone, and could be remotely controlled via a customized application.

The software running in the test platform, a modified version of the open source Wi-Fi software "Aircrack," configures the Wi-Fi radio in monitor mode and collects Wi-Fi packets off the air. The procedure was repeated for all of the 11 Wi-Fi channels in the 2.4 GHz frequency band. Each channel was scanned for 500 ms in the test. Each test was repeated for 5, 10, 20 and 60-second durations.

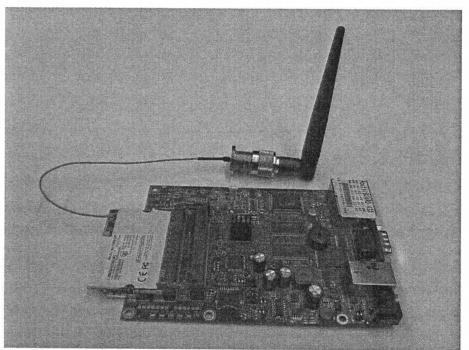


Figure 12: Wi-Fi hardware "Router" RB433 + Wistron CM9.

### C-3-2 Test Scenarios

Testing scenarios were chosen to replicate different ways that Wi-Fi equipment might be used in pursuit of metadata measurement activities. The four scenarios were:

- Measuring from a fixed location inside a CRC office building;
- Measuring from a fixed location outside a CRC office building with windows;
- Measuring from various distances away from a CRC office building; and
- Measuring targeted vehicles driving past the receiver.

During outdoor measurements, four different locations at increasing distances away from the CRC office building (Building 2) were selected to show the impact of distance. In all tests, the receiver was only active for specific time durations (5 sec., 10 sec., 20 sec. and 60 sec.).

It should be noted that these tests do not accurately emulate the last scenario where a targeted vehicle drives by the Wi-Fi receiver. However, results show that metadata information can be captured, even during small windows of time. It is therefore feasible that this method may be used to capture Wi-Fi information from passing cars, especially if the eavesdropper carefully plans the deployment.

In Table 5, detailed results showing metadata from a single test of Wi-Fi MAC measurement are shown. These were obtained at test location 2, and the receiver was active for a 10 sec. time duration.

Table 5: Snapshot of Wi-Fi monitoring results, captured using a \$140 commercial hardware platform (MAC addresses have been detected, but are hidden herein for

19(1),20(1)(b)

### C-3-4 Interpretation of Results

Raw measured results for Test 2, with a 10-second capture time, are shown in Table 6, which is taken from the larger set of results in Table 5 to facilitate interpretation. The columns show MAC address, manufacturer, time stamp, received power, number of packets, BSSID (which indicates whether the mobile device is connected, or has merely been captured without connecting), and the history of previously used hotspots if this information is provided by the device. For example, the person possessing the device captured in the third column of Table 5 (extracted and highlighted in Table 6, below) carries an ASUS tablet, has travelled to Washington, flying through Dulles and Reagan airports, stayed at the Marriott, and was previously connected at the Ottawa airport (YOW). This information can be used to hypothesize that the person has business at a certain location, and by accumulating a record of the individual's trips over time, a history of travelling to a particular city might indicate traits about the person's business, favourite places to stay and social activities. The person detected in the tenth column in Table 5 apparently spends time at the Ashton Pub, west of Ottawa. Based on the context of the measurements, and in particular based on time and location, (i.e., the Shirleys Bay campus), it can be assumed that most of the people detected in these tests are security-cleared public servants who have scientific or other government responsibilities. This type of context information is crucial to aiding the data analytics and fusion, post processing. Because of the personal nature of the data, the actual MAC addresses have been removed from Table 5 and Table 6.

Table 6: One entry from Wi-Fi MAC detection data log from June 20, 2014, at Shirleys Bay (see third column, Table 5), Test 2, 10-second duration (MAC address were detected, but are hidden to protect privacy).

MAC	Manuf.	Last Time	Power	Packets	BSSID	Probed ESSIDs
XX:XX:XX: XX:XX:XX	ASUSTek	2014-05-20 10:06:31	-84	27	not associated	<ul> <li>opl-bpo1</li> <li>Marriott_Guest</li> <li>Wingate</li> <li>WashingtonDulles Wi-Fi</li> <li>NG-50G</li> <li>YOW Free Wi-Fi</li> <li>' ReaganNational Wi-Fi</li> <li>iNet</li> <li>Courtyard_GUEST</li> <li>attWi-Fi</li> </ul>

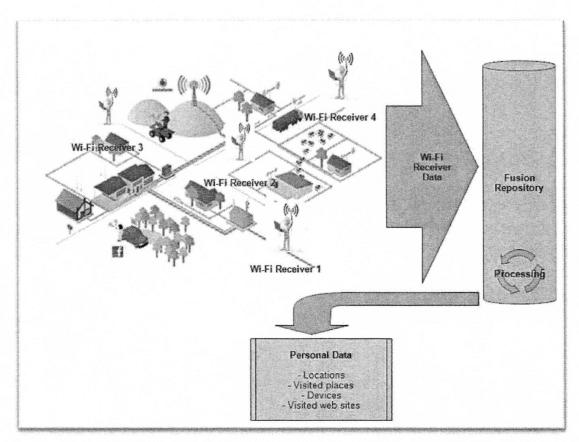


Figure 13: Scenario where Wi-Fi metadata is collected over a geographic region as source material for metadata fusion.

Measurements of this type can be conducted by a person carrying a backpack (containing the equipment in Figure 12) parked outside the House of Commons, any corporate HQ, or other financial trading institution on Bay Street; indeed, it is likely already done.

Figure 13 shows a depiction of how measured results of such tests can be conducted within a particular geographic area, and the metadata collected becomes the source material for metadata analytics and fusion. Vast amounts of data collected over location and time can be realistically post-processed using modern computational resources.

### TECHNICAL STUDY ON PRIVACY IN WIRELESS NETWORKS

**End of Document** 

### TECHNICAL STUDY ON PRIVACY IN WIRELESS NETWORKS

### **Document Control**

### Approver(s)/Reviewer(s)

Person	Representing	
Alex Vukovic	VPNS	VP

### Consultants

Person	Dept Representing		
N/A			

### **Release History**

Date	Version	Editor	Comment
3 July 2014	0.1	P. Vigneron	Draft
11 July 2014	0.2	P. Vigneron	Edits from Lisa Burke incorporated
20 July 2014	1.1	P. Vigneron	Leave results in main body, technical material to Appendices
25 Aug 2014	3.0	P. Vigneron	Final

File Name:

Privacy Project Aug 25 2014 - V3.0.docx CRC-REP-2014-009

Document #:

Version: Status:

3.0 Final

HARRIS CORPORATION

600 Maryland Avenue, S.W. Suite 850E Washington, D.C. 20024 phone 1-202-729-3700 fax 1-202-729-3735

www.hamis.com

April 28, 2011

Marlene H. Dortch, Secretary Federal Communications Commission Office of the Secretary 445 12<sup>th</sup> Street, S.W. Washington, D.C. 20554

Re: Final Request for Confidentiality of Harris Corporation for FCC ID No. NK73092523 (FCC Correspondence Number 39487)

Dear Ms. Dortch:

Harris Corporation ("Harris") submits this revised, post grant request for confidentiality. Public disclosure of certain materials included in the above referenced equipment authorization application could reasonably put public safety officials at risk, jeopardize the integrity and value of investigative techniques and procedures, reveal Harris trade secrets due to the nature of the equipment, and harm Harris' competitive interests. Harris respectfully requests, pursuant to 47 C.F.R. § 0.457(g), 47 C.F.R. § 0.457(d), and 47 C.F.R. § 0.459, that certain documents be held as confidential and withheld from public inspection or be superseded in the Commission's equipment authorization system by subsequently filed versions. Exhibit A, Exhibit B, and Exhibit C provides listings of Harris' requested treatment of exhibits, cover letters and correspondence.

- Exhibit A- Harris respectfully requests that these documents be treated as confidential and withheld from public inspection.
- <u>Exhibit B-</u> Harris respectfully requests that these documents be superseded in the Commission's equipment authorization system because the materials have been subsequently replaced with a revised version.
- <u>Exhibit C</u>- The following documents may be made publicly available without any restrictions.

### 1. Confidentiality Compliance with 47 C.F.R. § 0.457(g)

Section 0.457(g)(5) and (6) of the Commission's rules—pursuant to 5 U.S.C. § 552(b)(7)(E) and (F)—provides confidentiality if the production of records would either "disclose law enforcement investigative techniques or procedures," or "endanger the life or physical safety of public law enforcement." The product FCC ID No. NK73092523 is intended for use by federal, state, and local public safety entities. The nature of the product make it necessary for the descriptions provided in the equipment authorization application and supporting documents/exhibits— including technical information regarding the performance parameters, design and operation of the technology, and information regarding the identity of the entities proposing to use the product—be withheld from public disclosure and treated as

confidential under Section 0.457(g) of the Commission's rules. A complete list of documents that Harris respectfully requests be treated as confidential and withheld from public inspection is provided in Exhibit A.

To further support Harris' request for confidentiality and to underscore the need for confidentiality, Harris requests that the Commission condition its equipment authorization application as stated below:

### Requested Equipment Authorization Conditions:

(1) The marketing and sale of these devices shall be limited to federal/state/local public safety and law enforcement officials only; and

(2) State and local law enforcement agencies must advance coordinate with the FBI the acquisition and use of the equipment authorized under this authorization.

These conditions are respectfully requested to ensure that the product associated with FCC ID No. NK73092523 is limited to its intended use, operated only by federal, state, and local public safety officials, and to prevent and address concerns regarding the proliferation of the equipment to unauthorized users.

Providing confidential treatment of the materials included with the equipment authorization application identified as FCC ID No. NK73092523 would be in compliance with Section 0.457(g) of the Commission's rules—specifically 47 C.F.R. § 0.457(g)(5) and (6). It is crucial to the protection of public safety officials that all materials identified in Exhibit A be treated as confidential and withheld from public inspection.

### 2. Confidentiality Compliance with 47 C.F.R. § 0.457(d).

Likewise, Section 0.457(d) of the Commission's rules provides that trade secrets may not be routinely made available for public inspection. Harris competes with a number of companies that are developing and marketing similar public safety devices. Harris is careful in protecting proprietary aspects of its equipment design and manufacturing processes due to the sensitive nature of the product. The information for which confidential treatment is sought has been kept confidential from public disclosure by Harris and has not been made available to third parties without the execution of non-disclosure agreements.

Disclosure of the technical information disclosed in the attached documents to competitors could compromise Harris' ability to develop and protect this technology as other companies could reverse engineer products using the information provided as part of the equipment authorization application. Moreover, disclosure of technical content would relinquish valuable proprietary information about the technologies Harris has developed and its manufacturing processes. Disclosure would also offer competitors additional unwarranted insight into the state of Harris' product development, thereby allowing competitors an advantage that would otherwise be unavailable to Harris. Therefore, in furtherance of Section 0.457(d) of the Commission's rules, Harris respectfully requests that all materials identified in Exhibit A be treated as confidential and withheld from public inspection.

### 3. Confidentiality Compliance with 47 C.F.R. § 0.459(b).

Pursuant to Section 0.459(b)(1-9) of the Commission's rules, Harris provides the following information in support of its request for confidentiality:

- (1) The information disclosed in the attached equipment authorization application includes highly confidential and proprietary technical information about the equipment design and operating characteristics. Harris respectfully request that the attached equipment authorization application, in its entirety, and all supporting materials identified in Exhibit A be withheld from public inspection.
- (2) The Commission proceeding by which the information is submitted is identified as— FCC ID No. NK73092523.
- (3) Disclosure of the technical information disclosed in the application to competitors could compromise Harris' ability to sell and continue to develop the product line. Public disclosure of the information in the attached documents would provide other companies the opportunity could reverse engineer the communications technology.
- (4) There are many competitors that produce similar public safety equipment. Thus, any disclosure of Harris technical information regarding this product would relinquish valuable proprietary information about the how the technology was developed and the manufacturing process. Disclosure would also offer competitors additional unwarranted insight into the state of Harris' product development, thereby allowing competitors an advantage that would otherwise be unavailable to Harris.
- (5) Disclosure would result in substantial competitive harm to Harris. Disclosure would offer competitors insight into Harris' product development process and provide competitors a competitive advantage in the market.
- (6) Harris is careful in protecting proprietary aspects of its equipment design and manufacturing processes. The information for which confidential treatment is sought has been kept confidential from public disclosure by Harris throughout development. It has only been made available to third parties pursuant to non-disclosure agreements.
- (7) None of the technical information included in the attached equipment authorization application has been made available to the public. Information revealed to third parties was made pursuant to non-disclosure agreements.
- (8) Harris requests that this information be withheld from public disclosure until and unless Harris notifies the Commission that such information may be publicly released. This equipment is designed for use by authorized users only and may be used for more than a decade in some cases. Moreover the equipment will be used by federal, state, and local public safety officials, thus, it is important that its design and operational details not be made available to unauthorized persons who might attempt to use knowledge of such details to compromise the applications for which the equipment will be employed.

(9) Confidential treatment of the information contained in the attached equipment authorization application allows Harris to provide a full technical description of the equipment. However, refusal to treat such documents as confidential would result in submission of insufficient information on which the Commission could base its decision and delay deployment of these new and improved public safety devices.

For the foregoing reasons, Harris respectfully requests that the Commission treat the attached equipment authorization application and supporting materials as confidential and withhold them from public inspection. If Harris' request for confidentiality is found to be incomplete, Harris respectfully requests the Commission notify Harris of any deficiencies and provide Harris reasonable time to provide additional information. Should Harris' request for confidentially be denied, Harris respectfully requests that the Commission return all materials to which confidentiality cannot be provided.

Respectfully submitted,

/s/

Tania W. Hanna, Esq.
Vice President, Legislative Affairs and Public Policy
Harris Corporation
600 Maryland Avenue, S.W.
Suite 850E
Washington, D.C. 20024

E-mail: <u>thanna@harris.com</u> Phone: (202) 729-3712

Evan S. Morris, Esq. Counsel, Government Relations Harris Corporation 600 Maryland Avenue, S.W. Suite 850E Washington, D.C. 20024

Email: evan.morris@harris.com

Phone: (202) 729-3702

From:

Brien, Jean-Claude: DGEPS-DGGPN (NCR-RCN)

To: Cc:

Date:

Chau, Peter: DGEPS-DGGPN: Duquay, Daniel: DGEPS-DGGPN

Proulx, Martin: DGEPS-DGGPN; Hafez, Reema: DGEPS-DGGPN; Nixon, Jason: DGEPS-DGGPN; Proulx, Stephane: DGEPS-DGGPN

G&M/ IMSI catchers/ Today 5m

Subject:

RE: Follow-up: Media Call: September-02-14 5:20:57 PM

Attachments:

Harris final request for confidentiality for ID # NK73092523.pdf

19(1)

Peter, Daniel

As we just finished our conversation on the ISMI catcher issue, Jason and I looked in more in details on the FCC certification of some of the Harris Corp products that could fit the description. One of them is FCC ID NK73092523. Harris requested confidentiality of disclosure of certain materials under section 47 § 0.457 'Records not routinely available for public inspection'. They also asked for equipment authorization conditions to be set upon their product, as you may read in para 1. of the attached documents where the marketing and/or sale of the devices is restricted to federal/state/local PS and law enforcement entities. Obviously, we were not able to see any images and/or figures that would tell us it is the Stingray devices but, it is easy to deduce it may be. In any case, and in a nutshell, Harris has their device certified in the US but has conditions attached to so it can be sold only to Law enforcement/ PS users.

We will dig further on some other manufacturers and will try to cross reference in our REL. We do not have such a clear process in our Act and regulations. It would be on a case-by-case.

Hope this help

JC

From: Chau, Peter: DGEPS-DGGPN Sent: September-02-14 4:06 PM

To: Duguay, Daniel: DGEPS-DGGPN; Brien, Jean-Claude: DGEPS-DGGPN (NCR-RCN)

Cc: Proulx, Martin: DGEPS-DGGPN; Hafez, Reema: DGEPS-DGGPN

Subject: RE: Follow-up: Media Call: G&M/ IMSI catchers/ Today 5m 19(1)

I will be there.

From: Duguay, Daniel: DGEPS-DGGPN

Sent: September-02-14 3:58 PM

To: Brien, Jean-Claude: DGEPS-DGGPN (NCR-RCN); Chau, Peter: DGEPS-DGGPN

Cc: Proulx, Martin: DGEPS-DGGPN; Hafez, Reema: DGEPS-DGGPN

Subject: FW: Follow-up: Media Call: G&M/ IMSI catchers/ Today 5m 19(1)

For our 16h15 discussion today.

d

**Daniel Duguay** 

613.990.4820

daniel.duguav@ic.gc.ca

From: Hill, Peter: DGSO-DGOGS Sent: September-02-14 3:45 PM

To: Gillis, Kelly: STTT-STTT; Duguay, Daniel: DGEPS-DGGPN; Bérubé, Jean Luc: CRC (NCR-RCN);

Pereira, Rachel: SITT-STIT (NCR-RCN)

19(1) G&M/ IMSI catchers/ Today 5m Subject: Fw: Follow-up: Media Call:

We're getting this one on multiple fronts. Some more info below.

From: Cepella, Rob: DGSO-DGOGS

Sent: Tuesday, September 02, 2014 03:42 PM

To: Corbin, Marc: DGSO-DGOGS

Cc: Rathler, Gilles: DGSO-DGOGS; Hill, Peter: DGSO-DGOGS; Fleming, Philip: DGSO-DGOGS G&M/ IMSI catchers/ Today 5m

Subject: FW: Follow-up: Media Call: 19(1)

Marc - for your consideration:

### **FOLLOW-UP REQUEST:**

- 1. So the company that develops an IMSI catcher must first obtain technical acceptance from Industry Canada. And then an operator must gain a license from Industry Canada authorizing its use?
- 2. What department or agency would deal with the unauthorized use of such a device in Canada, ie. an IMSI catcher that is used without a license and/or technical acceptance from industry Canada?
- 3. In addition, the reporter would like to know what role, if any, the CRTC plays in this process.

### SUGGESTED RESPONSE:

As previously mentioned, legal use of radio equipment in Canada requires, as appropriate, technical acceptance be obtained from Industry Canada. This does not mean that Industry Canada would authorize the use of these sorts of devices by issuing a licence.

Industry Canada is responsible for enforcing the Radiocommunication Act and therefore would deal with unauthorized use of radio equipment in Canada. We suggest that you contact the CRTC directly regarding any role that it might play.

From: Rathier, Gilles: DGSO-DGOGS Sent: September-02-14 2:36 PM To: Cepella, Rob: DGSO-DGOGS Cc: Corbin, Marc: DGSO-DGOGS

Subject: FW: Follow-up: Media Call: G&M/ IMSI catchers/ Today 5m 19(1)

Rob – 2 follow up question on this media call.

				- 1	-	-1-
$\mathbf{H}$	pre	e is	a	CI	га	r

We've told the reporter to contact PS and RCMP on the subject on unauthorised use but 19(1)

19(1) has one main follow-up question below. In addition, he'd like to know what role, if any, the CRTC plays in this process.

Industry Canada is responsible for the enforcement of the Radiocommunication Act.

### **FOLLOW-UP REQUEST:**

- 1. So the company that develops an IMSI catcher must first obtain technical acceptance from Industry Canada. And then an operator must gain a license from Industry Canada authorizing its use?
- 2. What department or agency would deal with the unauthorized use of such a device in Canada, ie. an IMSI catcher that is used without a license and/or technical acceptance from industry Canada? **ANSWER:**

As previously mentioned, Legal use of radio equipment in Canada requires that technical acceptance be obtained from Industry Canada that it meets the applicable RSS. This does not mean that Industry Canada would permit such devices from entering Canada or authorized for it for use, however.

Again, Industry Canada is responsible for enforcing the Radiocommunication Act and therefore would be dealing with illegal use of radio equipment in Canada.

From: Fleming, Philip: DGSO-DGOGS
Sent: September-02-14 2:26 PM
To: Sloan, Glen: CMB-DGCM
Cc: Rathier, Gilles: DGSO-DGOGS
Subject: RE: Follow-up: Media Call: 19(1) G&M/ I

G&M/ IMSI catchers/ Today 5m

Yes. Please contact Gilles Rathier. pF

**From:** Sloan, Glen: CMB-DGCM **Sent:** September-02-14 11:22 AM **To:** Fleming, Philip: DGSO-DGOGS

Subject: FW: Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m

Hi Philip, I'm trying to find out who can respond to a couple of follow-up questions on a recent media call on "Stingrays."

Did you help James with this last week	?	
Thanks, Glen		
From: Sloan, Glen: CMB-DGCM Sent: September-02-14 2:20 PM To: Fancy, Lynne: DGSO-DGOGS Subject: FW: Follow-up: Media Call:	19(1)	G&M/ IMSI catchers/ Today 5m
Hi Lynne,		
	ion for you	– dìd you help him with this "Stingray" media call
last week?		
Trying to find out who can respond to	the two foll	ow-ups below.
Thanks, Glen		
From: CMB-Media Relations Sent: September-02-14 12:09 PM To: CMB-ASG-SITT; CMB-ASG-Strategic Cc: CMB-Media Relations; Vignola, Lucie Subject: Follow-up: Media Call:	: CMB-DGC	
Hi folks!		
		on the subject on unauthorised use but 19(1) addition, he'd like to know what role, if any, the
Thanks, Stéfanie		
REPORTER: 19(1) Globe and	d Mail,	19(1)
<b>DEADLINE:</b> Today, Sept 2, 5pm		

### **FOLLOW-UP REQUEST:**

- 1. So the company that develops an IMSI catcher must first obtain technical acceptance from Industry Canada. And then an operator must gain a license from Industry Canada authorizing its use?
- 2. What department or agency would deal with the unauthorized use of such a device in Canada, ie.

an IMSI catcher that is used with	hout a license and/or	technical accept	ance from indust	ry Canada?

19(1)

IMSI catchers—sometimes referred to colloquially as Stingrays—for The Globe and Mail and was wondering if Industry Canada has any knowledge of their use in Canada.

Stingrays are devices that masquerade as legitimate cellular base stations or cellular towers by piggy-backing onto a telecommunication provider's network, allowing law enforcement agencies to covertly collect and monitor identifying information about mobile devices in the immediate area. This all happens unbeknownst to the target(s) and others in the area. There are reports of their use in the U.S., but none that I can find in Canada. Stingray is manufactured by the Florida headquartered Harris Corporation.

Any information you can provide by the end of the week on how and where Stingrays are used in Canada—if at all—would be much appreciated.

### **RESPONSE:**

In order for a IMSI catcher to be legally used in Canada it would have to be required to be certified under a Radio Standards Specification (RSS) - namely, RSS 132, RSS 133 or RSS 139 - and would also require a radio station licence.

### **FOLLOW-UP REQUEST - RESPONSE PROVIDED AUGUST 28:**

**INITIAL REQUEST - RESPONSE PROVIDED AUGUST 22:** 

When you say used legally, do you mean that the company manufacturing the equipment would need to certify the IMSI catcher under an RSS, and the operator would require a radio station license?

Also, what about illegal operation? Is there any way, at present, to detect the unauthorized use of IMSI catchers? ie. this Newsweek story from June suggests foreign intelligence services could use such devices to spy on Americans in the U.S., and I can't imagine they would acquire a radio station license were they to do the same here. If you can suggest any other department government department that might be worth contacting on this particular question, I'd appreciate it.

### **RESPONSE:**

Legal use of radio equipment in Canada requires that technical acceptance be obtained from Industry Canada that it meets the applicable RSS. This does not mean it is authorized for use, however. With the exception of equipment exempt from this requirement, a licence from Industry Canada authorizing the use of this station or device must be obtained by an operator before it may be used.

From: To:	Brien, Jean-Claude: DGEPS-DGGPN (NCR-RCN) Nixon, Jason: DGEPS-DGGPN; Desmarais, Nicolas: DGEPS-DGGPN; Proulx, Stephane: DGEPS-DGGPN; Duguay, Daniel: DGEPS-DGGPN; Proulx, Martin: DGEPS-DGGPN
Subject: Date:	Re: Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m September-03-14 12:01:37 PM
Merci	
lean-Claude	Brien from/du Blackberry
	ecteur CEB/BHS
DGEPS/DGG	
SITT/STIT	
	nada/Industrie Canada
<b>Envoyé</b> : W À: Brien, Je Stephane: D	Jason: DGEPS-DGGPN lednesday, September 03, 2014 11:57 AM an-Claude: DGEPS-DGGPN (NCR-RCN); Desmarais, Nicolas: DGEPS-DGGPN; Proulx, GEPS-DGGPN; Duguay, Daniel: DGEPS-DGGPN; Proulx, Martin: DGEPS-DGGPN Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m
Hi JC,	
searched fo	or both Harris and DRT and could not locate any of these types devices in the REL.
lason	
Sent: Septe To: Nixon, J DGGPN; Dug	, Jean-Claude: DGEPS-DGGPN (NCR-RCN) mber-03-14 11:36 AM ason: DGEPS-DGGPN; Desmarais, Nicolas: DGEPS-DGGPN; Proulx, Stephane: DGEPS- guay, Daniel: DGEPS-DGGPN; Proulx, Martin: DGEPS-DGGPN e: Follow-up: Media Call 19(1) / G&M/ IMSI catchers/ Today 5m
lason, merc	
Can you cor	firm that we have not any in our REL, as you told me this morning.
IC	
	Rican from/du Blackhara
	Brien from/du Blackberry
DIRECTOR, DIF DGEPS/DGG	recteur CEB/BHS
SITT/STIT	ITIN
	nada/Industrie Canada
nuusti y Cdi	iada/industrie Cariada
<b>Envoyé</b> : W <b>À</b> : Brien, Je Stephane: D	Jason: DGEPS-DGGPN lednesday, September 03, 2014 09:42 AM an-Claude: DGEPS-DGGPN (NCR-RCN); Desmarais, Nicolas: DGEPS-DGGPN; Proulx, GEPS-DGGPN
objet : RE:	Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m
HI IC	

I have looked through the Harris devices the I had found and there were 4 approved by the FCC (NK73092523, NK73100176, NK73186795 and NK73166210). They were all directly certified by the FCC and all of the documentation was held confidential except for the test reports, which have been scrubbed and do not contain any information to identify the device as a Stingray. I searched the REL for Harris device certified to RSS-132, RSS-133 and RSS-139 and there were no matches.

I did find another possible manufacturer of these types of devices, Digital Receiver Technology, Inc. (DRT) but they are not listed in the REL at all. 20(1)(c) are some of their devices). Products are not listed on their website and they are now owned by Boeing and the Boeing press release states it is specifically to enhance their presence in the intelligence market.
I read some articles on these devices and they seem indicate the FBI and US military can use Jammers and communications blockers. I am not sure if CISI and DND have the same exemption here. There seemed to also be an initiative to allow local law enforcement in the US to use these devices for things like blocking contraband cellphones in prisons. One article seemed to tie DRT to an NSA metadata data leak.
Regards, Jason Nixon
From: Brien, Jean-Claude: DGEPS-DGGPN (NCR-RCN) Sent: September-03-14 8:21 AM To: Desmarais, Nicolas: DGEPS-DGGPN; Proulx, Stephane: DGEPS-DGGPN; Nixon, Jason: DGEPS-DGGPN Subject: Re: Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m
Merci Nicolas. En passant, 20(1)(b).21(1)(b)
Jean-Claude Brien from/du Blackberry
Director, Directeur CEB/BHS DGEPS/DGGPN SITT/STIT Industry Canada/Industrie Canada
De : Desmarais, Nicolas: DGEPS-DGGPN
Envoyé: Wednesday, September 03, 2014 08:19 AM À: Brien, Jean-Claude: DGEPS-DGGPN (NCR-RCN); Proulx, Stephane: DGEPS-DGGPN; Nixon, Jason:
Objet: RE: Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m
Even though we (IC) would deal with the unauthorized use of such device, 21(1)(b),21(1)(a) 21(1)(a),21(1)(b). They are performing a MITM (Man in the Middle) attack so there wouldn't be any interference issues and they are virtually invisible for the base station and the customer's cellphone. The only countermeasure I could find is specialized phones that can recognize the digital fingerprint of specific models of IMSI catcher. Also, an Android app to detect IMSI catcher is possibly in development.

From: Brien, Jean-Claude: DGEPS-DGGPN (NCR-RCN) Sent: September-02-14 4:12 PM
To: Desmarais, Nicolas: DGEPS-DGGPN; Proulx, Stephane: DGEPS-DGGPN; Nixon, Jason: DGEPS-
DGGPN Subject: RE: Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m
Jason :
This all happens unbeknownst to the target(s) and others in the area. There are reports of their
in the U.S., but none that I can find in Canada. Stingray is manufactured by the Florida
headquartered Harris Corporation.
From: Brien, Jean-Claude: DGEPS-DGGPN (NCR-RCN) Sent: September-02-14 4:03 PM
To: Desmarais, Nicolas: DGEPS-DGGPN; Proulx, Stephane: DGEPS-DGGPN; Nixon, Jason: DGEPS-DGGPN
Subject: FW: Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m
You know anything about theses ISMI catcher or 'Stingray'?
From: Duguay, Daniel: DGEPS-DGGPN Sent: September-02-14 3:55 PM To: Brien, Jean-Claude: DGEPS-DGGPN (NCR-RCN); Chau, Peter: DGEPS-DGGPN Cor Hafor, Reaman DCEPS-DGGPN, Proving DCEPS-DGGPN
Cc: Hafez, Reema: DGEPS-DGGPN; Proulx. Martin: DGEPS-DGGPN  Subject: Fw: Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m
Jean-Claude/Peter,
We have a request to provide briefing on this for tomorrow morning. Can I kindly request a 16:19 call/meeting.
Peter - my office for 16:15; Jean-Claude - will dial you in.
Need to confirm a few points prior to tomorrow.
Reema - please join us as well.
Dan
Ths msge thmb typd fm my Bkbry
From: Hill, Peter: DGSO-DGOGS Sent: Tuesday, September 02, 2014 03:45 PM Eastern Standard Time To: Gillis, Kelly: SITT-STIT; Duguay, Daniel: DGEPS-DGGPN; Bérubé, Jean Luc: CRC (NCR-RCN); Pereira, Rachel: SITT-STIT (NCR-RCN)
Subject: Fw: Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m
We're getting this one on multiple fronts. Some more info below.
From: Cepella, Rob: DGSO-DGOGS

Sent: Tuesday, September 02, 2014 03:42 PM

To: Corbin, Marc: DGSO-DGOGS

Cc: Rathier, Gilles: DGSO-DGOGS; Hill, Peter: DGSO-DGOGS; Fleming, Philip: DGSO-DGOGS

Subject: FW: Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m

Marc - for your consideration:

### **FOLLOW-UP REQUEST:**

- 1. So the company that develops an IMSI catcher must first obtain technical acceptance from Industry Canada. And then an operator must gain a license from Industry Canada authorizing its use?
- 2. What department or agency would deal with the unauthorized use of such a device in Canada, ie. an IMSI catcher that is used without a license and/or technical acceptance from industry Canada?
- 3. In addition, the reporter would like to know what role, if any, the CRTC plays in this process.

### SUGGESTED RESPONSE:

As previously mentioned, legal use of radio equipment in Canada requires, as appropriate, technical acceptance be obtained from Industry Canada. This does not mean that Industry Canada would authorize the use of these sorts of devices by issuing a licence.

Industry Canada is responsible for enforcing the Radiocommunication Act and therefore would deal with unauthorized use of radio equipment in Canada. We suggest that you contact the CRTC directly regarding any role that it might play.

From: Rathier, Gilles: DGSO-DGOGS Sent: September-02-14 2:36 PM To: Cepella, Rob: DGSO-DGOGS Cc: Corbin, Marc: DGSO-DGOGS Subject: FW: Follow-up: Media Call:			
	19(1)	G&M/ IMSI catchers/ Today 5m	
Rob – 2 follow up question on this med	dia call.		
Here is a start			
•••••		•••••	
We've told the reporter to contact PS	and RCMP o	on the subject on unauthorised use but	19(1)
	n below. In	addition, he'd like to know what role, if ar	ny, the
CRTC plays in this process.			

Industry Canada is responsible for the enforcement of the Radiocommunication Act.

### **FOLLOW-UP REQUEST:**

To: Fancy, Lynne: DGSO-DGOGS

- 1. So the company that develops an IMSI catcher must first obtain technical acceptance from Industry Canada. And then an operator must gain a license from Industry Canada authorizing its use?
- 2. What department or agency would deal with the unauthorized use of such a device in Canada, ie. an IMSI catcher that is used without a license and/or technical acceptance from industry Canada?

  ANSWER:

As previously mentioned, Legal use of radio equipment in Canada requires that technical acceptance be obtained from Industry Canada that it meets the applicable RSS. This does not mean that Industry Canada would permit such devices from entering Canada or authorized for it for use, however.

Again, Industry Canada is responsible for enforcing the Radiocommunication Act and therefore would be dealing with illegal use of radio equipment in Canada.

From: Fleming, Philip: DGSO-DGOGS Sent: September-02-14 2:26 PM To: Sloan, Glen: CMB-DGCM		
Cc: Rathier, Gilles: DGSO-DGOGS Subject: RE: Follow-up: Media Call:	19(1)	G&M/ IMSI catchers/ Today 5m
Yes. Please contact Gilles Rathier. p	οF	
From: Sloan, Glen: CMB-DGCM Sent: September-02-14 11:22 AM Ter Floring Philip DCSO DCSCS		
<b>To:</b> Fleming, Philip: DGSO-DGOGS <b>Subject:</b> FW: Follow-up: Media Call:	19(1)	G&M/ IMSI catchers/ Today 5m
Hi Philip, I'm trying to find out who car media call on "Stingrays."	respond t	to a couple of follow-up questions on a recent
Did you help James with this last week	?	
Thanks,		
Glen		
From: Sloan, Glen: CMB-DGCM Sent: September-02-14 2:20 PM		

Subject: FW: Follow-u	ıp: Media Call: 19(1)	G&M/ IMSI catchers/ Today 5m
Hi Lynne,		
19(1)	so I have a question for yo	ou – did you help him with this "Stingray" media call
last week?		
Trying to find out who	can respond to the two f	ollow-ups below.
Thanks,		
Glen		
	4 12:09 PM MB-ASG-Strategic Policy (M ns; Vignola, Lucie: CMB-DO	
Hi folks!		
	llow-up question below.	on the subject on unauthorised use but 19(1) in addition, he'd like to know what role, if any, the
REPORTER: 19(1)	, Globe and Mail,	19(1)
TOPIC: IMSI catchers DEADLINE: Today, Sep	ot 2. 5pm	
FOLLOW-UP REQUES		
		er must first obtain technical acceptance from in a license from Industry Canada authorizing its
		the unauthorized use of such a device in Canada, ie. nd/or technical acceptance from industry Canada?
INITIAL REQUEST – RE	SPONSE PROVIDED AUG	UST 22 :
INITIAL REQUEST – RE		UST 22 : nes referred to colloquially as Stingrays—for The

(A-2018-00073) - Page: 73

Stingrays are devices that masquerade as legitimate cellular base stations or cellular towers by piggy-backing onto a telecommunication provider's network, allowing law enforcement agencies to covertly collect and monitor identifying information about mobile devices in the immediate area. This all happens unbeknownst to the target(s) and others in the area. There are reports of their use in the U.S., but none that I can find in Canada. Stingray is manufactured by the Florida headquartered Harris Corporation.

Any information you can provide by the end of the week on how and where Stingrays are used in Canada—if at all—would be much appreciated.

#### **RESPONSE:**

In order for a IMSI catcher to be legally used in Canada it would have to be required to be certified under a Radio Standards Specification (RSS) - namely, RSS 132, RSS 133 or RSS 139 - and would also require a radio station licence.

#### **FOLLOW-UP REQUEST - RESPONSE PROVIDED AUGUST 28:**

When you say used legally, do you mean that the company manufacturing the equipment would need to certify the IMSI catcher under an RSS, and the operator would require a radio station license?

Also, what about illegal operation? Is there any way, at present, to detect the unauthorized use of IMSI catchers? ie. this Newsweek story from June suggests foreign intelligence services could use such devices to spy on Americans in the U.S., and I can't imagine they would acquire a radio station license were they to do the same here. If you can suggest any other department government department that might be worth contacting on this particular question, I'd appreciate it.

#### **RESPONSE:**

Legal use of radio equipment in Canada requires that technical acceptance be obtained from Industry Canada that it meets the applicable RSS. This does not mean it is authorized for use, however. With the exception of equipment exempt from this requirement, a licence from Industry Canada authorizing the use of this station or device must be obtained by an operator before it may be used.

From:

Brien, Jean-Claude: DGEPS-DGGPN (NCR-RCN)

To:

Duguay, Daniel: DGEPS-DGGPN; Chau, Peter: DGEPS-DGGPN

Cc:

Jackson, Margot: DGEPS-DGGPN

Subject:

Re: Fw: Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m

Date: September-03-14 2:48:56 PM

Merci daniel, apres notre breve discussion sur cette premiere ebauche, voici une autre proposition pour le second paragraphe ( ou tout le texte).

However, in the case of an ISMI catcher, the above process would not be applicable as it is a device intended to be used by specialized law enforcement/ pucblic safety agencies. The onus would be on these users to approach industry Canada for a special authorization.

Jean-Claude Brien from/du Blackberry Director, Directeur CEB/BHS DGEPS/DGGPN SITT/STIT Industry Canada/Industrie Canada

**De**: Brien, Jean-Claude: DGEPS-DGGPN (NCR-RCN) **Envoyé**: Wednesday, September 03, 2014 02:28 PM

À: Duguay, Daniel: DGEPS-DGGPN; Chau, Peter: DGEPS-DGGPN

Cc : Jackson, Margot: DGEPS-DGGPN

Objet: Re: Fw: Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m

Daniel, having read the previous response, here is my take on how to provide the gentleman with a more factual response:

From a different perspective, any radio apparatus to be sold and/or offer to users on the Canadian market must first meet the prescribed technical requirements set forth in the applicable standards published by Industry Canada (the Radio Specification Standards or RSS). The grant of a technical acceptance does not result in the grant of an authorization to use the apparatus. Consequently, the user, once it acquired the apparatus duly certified, must seek a license to operate/ use it unless specifically exempted by the regulations.

In the case of an ISMI catcher device, the manufacturer would first need to get its equipment certified before offering it to Canadian potential users. In the case at hand, the device would need to meet the before mentioned RSS 132, 133 and 139 covering the frequency bands generally used by cell/smart phones. By the nature of the device and the technical and administrative requirements necessitated by the Canadian certification process, it would be very difficult for a manufacturer of ISMI catcher device to obtain a certification.

Jean-Claude Brien from/du Blackberry Director, Directeur CEB/BHS DGEPS/DGGPN SITT/STIT Industry Canada/Industrie Canada

De: Duguay, Daniel: DGEPS-DGGPN Envoyé: Wednesday, September 03, 2014 01:01 PM À : Brien, Jean-Claude: DGEPS-DGGPN (NCR-RCN) G&M/ IMSI catchers/ Today 5m Objet: Fw: Follow-up: Media Call: 19(1) Note what was already provided. Ths msge thmb typd fm my Bkbry From: Hill, Peter: DGSO-DGOGS Sent: Tuesday, September 02, 2014 03:45 PM Eastern Standard Time To: Gillis, Kelly: STTT-STTT; Duguay, Daniel: DGEPS-DGGPN; Bérubé, Jean Luc: CRC (NCR-RCN); Pereira, Rachel: SITT-STIT (NCR-RCN) Subject: Fw: Follow-up: Media Call: G&M/ IMSI catchers/ Today 5m 19(1) We're getting this one on multiple fronts. Some more info below. From: Cepella, Rob: DGSO-DGOGS Sent: Tuesday, September 02, 2014 03:42 PM To: Corbin, Marc: DGSO-DGOGS Cc: Rathier, Gilles: DGSO-DGOGS; Hill, Peter: DGSO-DGOGS; Fleming, Philip: DGSO-DGOGS Subject: FW: Follow-up: Media Call: G&M/ IMSI catchers/ Today 5m 19(1) Marc – for your consideration:

#### **FOLLOW-UP REQUEST:**

- 1. So the company that develops an IMSI catcher must first obtain technical acceptance from Industry Canada. And then an operator must gain a license from Industry Canada authorizing its use?
- 2. What department or agency would deal with the unauthorized use of such a device in Canada, ie. an IMSI catcher that is used without a license and/or technical acceptance from industry Canada?
- 3. In addition, the reporter would like to know what role, if any, the CRTC plays in this process.

#### SUGGESTED RESPONSE:

As previously mentioned, legal use of radio equipment in Canada requires, as appropriate, technical acceptance be obtained from Industry Canada. This does not mean that Industry Canada would

authorize the use of these sorts of devices by issuing a licence. Industry Canada is responsible for enforcing the Radiocommunication Act and therefore would deal with unauthorized use of radio equipment in Canada. We suggest that you contact the CRTC directly regarding any role that it might play.

From: Rathier, Gilles: DGSO-DGOGS Sent: September-02-14 2:36 PM To: Cepella, Rob: DGSO-DGOGS Cc: Corbin, Marc: DGSO-DGOGS

Subject: FW: Follow-up: Media Call: 19(1

: 19(1) G&M/ IMSI catchers/ Today 5m

Rob - 2 follow up question on this media call.

Here is a start...

We've told the reporter to contact PS and RCMP on the subject on unauthorised use but 19(1) has one main follow-up question below. In addition, he'd like to know what role, if any, the CRTC plays in this process.

Industry Canada is responsible for the enforcement of the Radiocommunication Act.

#### **FOLLOW-UP REQUEST:**

- 1. So the company that develops an IMSI catcher must first obtain technical acceptance from Industry Canada. And then an operator must gain a license from Industry Canada authorizing its use?
- 2. What department or agency would deal with the unauthorized use of such a device in Canada, ie. an IMSI catcher that is used without a license and/or technical acceptance from industry Canada? **ANSWER:**

As previously mentioned, Legal use of radio equipment in Canada requires that technical acceptance be obtained from Industry Canada that it meets the applicable RSS. This does not mean that Industry Canada would permit such devices from entering Canada or authorized for it for use, however.

Again, Industry Canada is responsible for enforcing the Radiocommunication Act and therefore would be dealing with illegal use of radio equipment in Canada.

	CARRESTON CHARGE THE CO. CO. CO. CO.	A
From: Fleming, Philip: DGSO-DGOGS Sent: September-02-14 2:26 PM To: Sloan, Glen: CMB-DGCM Cc: Rathier, Gilles: DGSO-DGOGS		
Subject: RE: Follow-up: Media Call:	19(1)	G&M/ IMSI catchers/ Today 5m
Yes. Please contact Gilles Rathier.	pF	
From: Sloan, Glen: CMB-DGCM Sent: September-02-14 11:22 AM		
To: Fleming, Philip: DGSO-DGOGS Subject: FW: Follow-up: Media Call:	19(1)	G&M/ IMSI catchers/ Today 5m
Hi Philin I'm trying to find out who c	an respond	d to a couple of follow-up questions on a recent
media call on "Stingrays."	ан тезропе	a to a couple of follow up questions on a recent
Did you help James with this last wee	ek?	
Thanks,		
Glen		*
From: Sloan, Glen: CMB-DGCM Sent: September-02-14 2:20 PM		
<b>To:</b> Fancy, Lynne: DGSO-DGOGS <b>Subject:</b> FW: Follow-up: Media Call:	10(1)	G&M/ IMSI catchers/ Today 5m
•	19(1)	
Hi Lynne,		
19(1) so I have a que	estion for v	ou – did you help him with this "Stingray" media call
last week?	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	ou did you holp him that this banging mount can
Trying to find out who can respond t	o the two	follow-ups below.
Thanks		
Thanks, Glen		
Gieli		
From: CMB-Media Relations		
Sent: September-02-14 12:09 PM	ela Dalia (A	A Marcineth
To: CMB-ASG-SITT; CMB-ASG-Strates Cc: CMB-Media Relations; Vignola, Lu		
Subject: Follow-up: Media Call:	19(1)	G&M/ IMSI catchers/ Today 5m
Hi folks!		_
III IOING!		
We've told the reporter to contact P	S and RCM	IP on the subject on unauthorised use but 19(1)
		In addition, he'd like to know what role, if any, the

CRTC plays in	this process		
Thanks, Stéfar	nie		
REPORTER:	19(1)	Globe and Mail,	19(1)
TOPIC: IMSI ca		_	
<b>DEADLINE:</b> To	day, Sept 2,	, 5pm	

#### **FOLLOW-UP REQUEST:**

- 1. So the company that develops an IMSI catcher must first obtain technical acceptance from Industry Canada. And then an operator must gain a license from Industry Canada authorizing its use?
- 2. What department or agency would deal with the unauthorized use of such a device in Canada, ie. an IMSI catcher that is used without a license and/or technical acceptance from industry Canada?

#### **INITIAL REQUEST - RESPONSE PROVIDED AUGUST 22:**

19(1)
IMSI catchers—sometimes referred to colloquially as Stingrays—for The Globe and Mail and was wondering if Industry Canada has any knowledge of their use in Canada.

Stingrays are devices that masquerade as legitimate cellular base stations or cellular towers by piggy-backing onto a telecommunication provider's network, allowing law enforcement agencies to covertly collect and monitor identifying information about mobile devices in the immediate area. This all happens unbeknownst to the target(s) and others in the area. There are reports of their use in the U.S., but none that I can find in Canada. Stingray is manufactured by the Florida headquartered Harris Corporation.

Any information you can provide by the end of the week on how and where Stingrays are used in Canada—if at all—would be much appreciated.

#### **RESPONSE:**

In order for a IMSI catcher to be legally used in Canada it would have to be required to be certified under a Radio Standards Specification (RSS) - namely, RSS 132, RSS 133 or RSS 139 - and would also require a radio station licence.

#### **FOLLOW-UP REQUEST - RESPONSE PROVIDED AUGUST 28:**

When you say used legally, do you mean that the company manufacturing the equipment would need to certify the IMSI catcher under an RSS, and the operator would require a radio station license?

Also, what about illegal operation? Is there any way, at present, to detect the unauthorized use of IMSI catchers? ie. this Newsweek story from June suggests foreign intelligence services could use such devices to spy on Americans in the U.S., and I can't imagine they would acquire a radio station

(A-2018-00073) - Page: 79

license were they to do the same here. If you can suggest any other department government department that might be worth contacting on this particular question, I'd appreciate it. **RESPONSE**:

Legal use of radio equipment in Canada requires that technical acceptance be obtained from Industry Canada that it meets the applicable RSS. This does not mean it is authorized for use, however. With the exception of equipment exempt from this requirement, a licence from Industry Canada authorizing the use of this station or device must be obtained by an operator before it may be used.

From: To:		Nixon, Jason; DGEPS-DGGPN Proulx, Stephane: DGEPS-DGGPN; Brien, Jean-Claude; DGEPS-DGGPN (NCR-RCN); Desmarais, Nicolas; DGEPS-				
Subject: Date:	DGGPN RE: Follow-up: Media Call: September-19-14 8:05:50 Al	19(1) M	/ G&M/ IMSI catchers/ Today 5m			
Hi Steph,						
I read over m	ny summary again and rea	ilized that	l left out one point,			
For the FCC o	ertified device they all ha	d the follo	wing grant condition:			
law enforcen	nent officials only; and (2) with the FBI the acquisition	State and	be limited to federal, state, local public safety and local law enforcement agencies must advance of the equipment authorized under this			
This would m	nake the certification void	if someon	ne else was using the device.			
Jason						
Sent: Septen To: Brien, Jea	, Stephane: DGEPS-DGGP nber-18-14 6:28 PM an-Claude: DGEPS-DGGPN son: DGEPS-DGGPN		N); Desmarais, Nicolas: DGEPS-DGGPN			
	: Follow-up: Media Call:	19(1)	G&M/ IMSI catchers/ Today 5m			
A summary f	or your convenience.					
Tx Jason,						
Stephane Pro	pulx					
Sent via Black	kBerry					
Sent: Tuesda	, Jason: DGEPS-DGGPN ay, September 16, 2014 01 tephane: DGEPS-DGGPN	l:18 PM Ea	stern Standard Time			
	: Follow-up: Media Call:	19(1)	G&M/ IMSI catchers/ Today 5m			
Here is the ir	nfo I sent to JC for distribu	ition to Da	n.			
During the co	onference call with Dan th	ne followin	ng points were his take away:			

1) We would not knowingly certify one of these devices since it had a malicious intent and

2) A CB may have certified one of these devices as the company could have misrepresented

could be considered a jammer.

the device as a nano cell or femtocell.

- 3) RCMP/CISI could just be using them under the impression that they don't need to consult IC.
- 4) Regions could have provided RCMP/CISI with permission to use these without consulting DGEPS.

#### Summary of below:

- 1) Found 4 devices certified by Harris for use only by law enforcement. All documentation was held confidential.
- 2) FCC certified directly, no CB involved.
- 3) Another company DRT had devices certified in the same way as Harris. DTR is owned by Boeing.
- 4) None of the devices were found in the REL.

Jason

From: Nixon, Jason: DGEPS-DGGPN Sent: September-03-14 9:42 AM

To: Brien, Jean-Claude: DGEPS-DGGPN (NCR-RCN); Desmarais, Nicolas: DGEPS-DGGPN; Proulx,

Stephane: DGEPS-DGGPN

Subject: RE: Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m

HIJC,

I have looked through the Harris devices the I had found and there were 4 approved by the FCC (NK73092523, NK73100176, NK73186795 and NK73166210). They were all directly certified by the FCC and all of the documentation was held confidential except for the test reports, which have been scrubbed and do not contain any information to identify the device as a Stingray. I searched the REL for Harris device certified to RSS-132, RSS-133 and RSS-139 and there were no matches.

I did find another possible manufacturer of these types of devices, Digital Receiver Technology, Inc. (DRT) but they are not listed in the REL at all.

20(1)(b) are some of their devices). Products are not listed on their website and they are now owned by Boeing and the Boeing press release states it is specifically to enhance their presence in the intelligence market.

I read some articles on these devices and they seem indicate the FBI and US military can use Jammers and communications blockers. I am not sure if CISI and DND have the same exemption here. There seemed to also be an initiative to allow local law enforcement in the US to use these devices for things like blocking contraband cellphones in prisons. One article seemed to tie DRT to an NSA metadata data leak.

Regards, Jason Nixon

From: Brien, Jean-Claude: DGEPS-DGGPN (NCR-RCN)

Sent: September-03-14 8:21 AM

To: Desmarais, Nicolas: DGEPS-DGGPN; Proulx, Stephane: DGEPS-DGGPN; Nixon, Jason: DGEPS-

DGGPN Subject: Re: Follow-up: Media Call:	19(1)	G&M/ IMSI catchers/ Today 5m
	00/	1)(b)
Merci Nicolas. En passant,		1)(b)
Jean-Claude Brien from/du Blackbern	4	
Director, Directeur CEB/BHS		
DGEPS/DGGPN		
SITT/STIT		
Industry Canada/Industrie Canada		
De : Desmarais, Nicolas: DGEPS-DGGF Envoyé : Wednesday, September 03, À : Brien, Jean-Claude: DGEPS-DGGPN DGEPS-DGGPN Objet : RE: Follow-up: Media Call:	2014 08:19 A I (NCR-RCN);	M Proulx, Stephane: DGEPS-DGGPN; Nixon, Jason: G&M/ IMSI catchers/ Today 5m
		5-1
Even though we (IC) would deal with		
		Man in the Middle) attack so there wouldn't be
		ble for the base station and the customer's
		specialized phones that can recognize the digital
fingerprint of specific models of IMSI	catcher. Also	, an Android app to detect IMSI catcher is possibly
in development.		
From: Brien, Jean-Claude: DGEPS-DG Sent: September-02-14 4:12 PM To: Desmarais, Nicolas: DGEPS-DGGPI DGGPN Subject: RE: Follow-up: Media Call:	·	phane: DGEPS-DGGPN; Nixon, Jason: DGEPS-G&M/ IMSI catchers/ Today 5m
Jason :		
This all happens unbeknownst to the in the U.S., but none that I can find in		others in the area. There are reports of their use
headquartered Harris Corporation.	i Cariada. 3tii	igray is mandractured by the Florida
neadquartered harns corporation.		
From: Brien, Jean-Claude: DGEPS-DG Sent: September-02-14 4:03 PM To: Desmarais, Nicolas: DGEPS-DGGPI DGGPN	•	phane: DGEPS-DGGPN; Nixon, Jason: DGEPS-
Subject: FW: Follow-up: Media Call:	19(1)	G&M/ IMSI catchers/ Today 5m
4	. ,	
You know anything about theses ISM	I catcher or 'S	Stingray'?
From: Duguay, Daniel: DGEPS-DGGPN Sent: September-02-14 3:55 PM To: Brien, Jean-Claude: DGEPS-DGGP Cc: Hafez, Reema: DGEPS-DGGPN; Pr Subject: Fw: Follow-up: Media Call:	N (NCR-RCN)	; Chau, Peter: DGEPS-DGGPN DGEPS-DGGPN G&M/ IMSI catchers/ Today 5m

Jean-Claude/Peter,

We have a request to provide briefing on this for tomorrow morning. Can I kindly request a 16:15 call/meeting.

Peter - my office for 16:15; Jean-Claude - will dial you in.

Need to confirm a few points prior to tomorrow.

Reema - please join us as well.

Dan

Ths msge thmb typd fm my Bkbry

From: Hill, Peter: DGSO-DGOGS

Sent: Tuesday, September 02, 2014 03:45 PM Eastern Standard Time

To: Gillis, Kelly: STTT-STTT; Duguay, Daniel: DGEPS-DGGPN; Bérubé, Jean Luc: CRC (NCR-RCN);

Pereira, Rachel: SITT-STIT (NCR-RCN)

Subject: Fw: Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m

We're getting this one on multiple fronts. Some more info below.

From: Cepella, Rob: DGSO-DGOGS

Sent: Tuesday, September 02, 2014 03:42 PM

To: Corbin, Marc: DGSO-DGOGS

Cc: Rathier, Gilles: DGSO-DGOGS; Hill. Peter: DGSO-DGOGS; Fleming, Philip: DGSO-DGOGS Subject: FW: Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m

Marc - for your consideration;

#### **FOLLOW-UP REQUEST:**

- 1. So the company that develops an IMSI catcher must first obtain technical acceptance from Industry Canada. And then an operator must gain a license from Industry Canada authorizing its use?
- 2. What department or agency would deal with the unauthorized use of such a device in Canada, ie. an IMSI catcher that is used without a license and/or technical acceptance from industry Canada?
- 3. In addition, the reporter would like to know what role, if any, the CRTC plays in this process.

#### SUGGESTED RESPONSE:

As previously mentioned, legal use of radio equipment in Canada requires, as appropriate, technical acceptance be obtained from Industry Canada. This does not mean that Industry Canada would authorize the use of these sorts of devices by issuing a licence.

Industry Canada is responsible for enforcing the Radiocommunication Act and therefore would deal

with unauthorized use of radio equipment in Canada. We suggest that you contact the CRTC directly regarding any role that it might play.

From: Rathier, Gilles: DGSO-DGOGS Sent: September-02-14 2:36 PM To: Cepella, Rob: DGSO-DGOGS

Cc: Corbin, Marc: DGSO-DGOGS
Subject: FW: Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m

Rob - 2 follow up question on this media call.

Here is a start...

We've told the reporter to contact PS and RCMP on the subject on unauthorised use but 19(1) has one main follow-up question below. In addition, he'd like to know what role, if any, the CRTC plays in this process.

Industry Canada is responsible for the enforcement of the Radiocommunication Act.

#### **FOLLOW-UP REQUEST:**

- 1. So the company that develops an IMSI catcher must first obtain technical acceptance from Industry Canada. And then an operator must gain a license from Industry Canada authorizing its use?
- 2. What department or agency would deal with the unauthorized use of such a device in Canada, ie. an IMSI catcher that is used without a license and/or technical acceptance from industry Canada? **ANSWER:**

As previously mentioned, Legal use of radio equipment in Canada requires that technical acceptance be obtained from Industry Canada that it meets the applicable RSS. This does not mean that Industry Canada would permit such devices from entering Canada or authorized for it for use, however.

Again, Industry Canada is responsible for enforcing the Radiocommunication Act and therefore would be dealing with illegal use of radio equipment in Canada.

From: Fleming, Philip: DGSO-DGOGS

Sent: September-02-14 2:26 PM To: Sloan, Glen: CMB-DGCM Cc: Rathier, Gilles: DGSO-DGOGS G&M/ IMSI catchers/ Today 5m 19(1) Subject: RE: Follow-up: Media Call: Yes. Please contact Gilles Rathier. pF From: Sloan, Glen: CMB-DGCM Sent: September-02-14 11:22 AM To: Fleming, Philip: DGSO-DGOGS G&M/ IMSI catchers/ Today 5m 19(1) Subject: FW: Follow-up: Media Call: Hi Philip, I'm trying to find out who can respond to a couple of follow-up questions on a recent media call on "Stingrays." Did you help James with this last week? Thanks, Glen From: Sloan, Glen: CMB-DGCM Sent: September-02-14 2:20 PM To: Fancy, Lynne: DGSO-DGOGS Subject: FW: Follow-up: Media Call: 19(1) G&M/ IMSI catchers/ Today 5m Hi Lynne, 19(1) so I have a question for you - did you help him with this "Stingray" media call last week? Trying to find out who can respond to the two follow-ups below. Thanks, Glen From: CMB-Media Relations Sent: September-02-14 12:09 PM To: CMB-ASG-SITT; CMB-ASG-Strategic Policy (M. McGrath) Cc: CMB-Media Relations; Vignola, Lucie: CMB-DGCM Subject: Follow-up: Media Call: G&M/ IMSI catchers/ Today 5m 19(1) Hi folks! We've told the reporter to contact PS and RCMP on the subject on unauthorised use but 19(1) has one main follow-up question below. In addition, he'd like to know what role, if any, the CRTC plays in this process.

Thanks, Stéfanie

REPORTER:	19(1)	Globe and Mail,	19(1)

**TOPIC:** IMSI catchers

**DEADLINE:** Today, Sept 2, 5pm

#### **FOLLOW-UP REQUEST:**

1. So the company that develops an IMSI catcher must first obtain technical acceptance from Industry Canada. And then an operator must gain a license from Industry Canada authorizing its use?

2. What department or agency would deal with the unauthorized use of such a device in Canad	la, ie.
an IMSI catcher that is used without a license and/or technical acceptance from industry Canad	fa?

#### **INITIAL REQUEST - RESPONSE PROVIDED AUGUST 22:**

19(1)
IMSI catchers—sometimes referred to colloquially as Stingrays—for The Globe and Mail and was wondering if Industry Canada has any knowledge of their use in Canada.

Stingrays are devices that masquerade as legitimate cellular base stations or cellular towers by piggy-backing onto a telecommunication provider's network, allowing law enforcement agencies to covertly collect and monitor identifying information about mobile devices in the immediate area. This all happens unbeknownst to the target(s) and others in the area. There are reports of their use in the U.S., but none that I can find in Canada. Stingray is manufactured by the Florida headquartered Harris Corporation.

Any information you can provide by the end of the week on how and where Stingrays are used in Canada—if at all—would be much appreciated.

#### **RESPONSE:**

In order for a IMSI catcher to be legally used in Canada it would have to be required to be certified under a Radio Standards Specification (RSS) - namely, RSS 132, RSS 133 or RSS 139 - and would also require a radio station licence.

#### **FOLLOW-UP REQUEST - RESPONSE PROVIDED AUGUST 28:**

When you say used legally, do you mean that the company manufacturing the equipment would need to certify the IMSI catcher under an RSS, and the operator would require a radio station license?

Also, what about illegal operation? Is there any way, at present, to detect the unauthorized use of IMSI catchers? ie. this Newsweek story from June suggests foreign intelligence services could use such devices to spy on Americans in the U.S., and I can't imagine they would acquire a radio station license were they to do the same here. If you can suggest any other department government department that might be worth contacting on this particular question, I'd appreciate it.

(A-2018-00073) - Page: 87

#### **RESPONSE:**

Legal use of radio equipment in Canada requires that technical acceptance be obtained from Industry Canada that it meets the applicable RSS. This does not mean it is authorized for use, however. With the exception of equipment exempt from this requirement, a licence from Industry Canada authorizing the use of this station or device must be obtained by an operator before it may be used.

#### Noel, Sylvain (IC)

From:

Mark.Shelden@forces.gc.ca

Sent:

September-11-17 3:09 PM

To:

andrewm@smithmyers.com; CHRISTIAN.RENE@forces.gc.ca; MARIO.LAVOIE2

@forces.gc.ca; Kennedy, Caroline (IC); Noel, Sylvain (IC);

MARTIAL.LAPORTE@forces.gc.ca; JAMES.MCPHEE2@forces.gc.ca;

JEAN.LEROUX@forces.gc.ca; Peter.Earle@nrc-cnrc.gc.ca; Ovenden, Mark (Ext.); Craig, Gregory (Ext.); Kissmann, Paul (Ext.); Srinivasan, Ramesh (Ext.); Parent, Fabien (Ext.);

Jennings, Sion (Ext.); Day, James (Ext.)

Subject:

Minutes for the Digital Receiver Technology for SAR Operations held at NRC Flight

Labs, Ottawa 7 Sept 2017

Attachments:

20170907 Minutes.docx

Follow Up Flag:

Follow up Completed

Flag Status: Categories:

Catégorie bleue

Good afternoon everyone.

First of all, a big shout-out to NRC Flight Labs for hosting our meeting. I really appreciate your hospitality.

Thank you all for your participation in last Thursday's meeting. I was impressed with the lively discussion and the interest shown by everyone. I think we're in heated agreement that this project is worth pursuing to the end.

I was busy listening and didn't take many notes but encl., please find a summary of the discussions. I included a short list of action items we'll need to deal with IOT move forward. There shouldn't be any surprises in there.

If you have any questions or concerns, please advise.

For NRC – The missing lawyer mistakenly entered the meeting date in his calendar for this coming Thursday. If you see a guy carrying a briefcase wandering around aimlessly, please send him home.

Mark

Maj M.D. Shelden

Concepts Development and Experimentation, Canadian Forces Aerospace Warfare Centre Royal Canadian Air Force Mark.Shelden@forces.gc.ca / Tel: 613-392-2811 ext 5614 / CSN 827-5614 / Fax 613-965-2096

Développement de Concepts et Expérimentation / Centre de guerre aérospatiale des Forces canadiennes Aviation royale canadienne

Mark.Shelden@forces.gc.ca / Tél: 613-392-2811 poste 5614 / ATS: 827-5614 / Facsimile 613-965-2096

(A-2018-00073) - Page: 89

# Minutes of the Digital Receiver Technology for SAR Operations Meeting National Research Council Flight Labs 1920 Research Road, Ottawa 7 Sept 2017

#### Attendees

Maj Mark Shelden, CFAWC, Project Lead Sion Jennings, NRC, Project Team Lead Andrew Munro, Smith Myers Communications Company Lead Maj Christian Rene, DND FSM Mario Lavoie, DND FSM Caroline Kennedy, ISED Canada Sylvain Noel, ISED Canada Maj James McPhee, DAR 2-2 Maj Jean Leroux, DAR 2-6 MWO Martial Laporte, DAR 3-6 Pete Earl, NRC Mark Ovenden, NRC Gregory Craig, NRC Paul Kissmann, NRC Ramesh Srinivascan, NRC Fabian Parent, NRC James Day, NRC

A special thanks to NRC Flight Labs for providing their facilities and hosting the meeting.

1030 - Opening Remarks - The purpose of the meeting is to explore the feasibility of using commercial off-the-shelf (COTS) digital receiver technology to assist in Search and Rescue (SAR) operations in Canada. This will be a whole of government approach as it will require the assistance of several government departments and agencies to bring this to fruition.

NRC – Pete Earl provided a brief introduction as to how NRC Flight Labs conducts research using their fleet of in-house aircraft. NRC has an organic airworthiness program which does not rely on Transport Canada certification for aircraft modifications required for their test programs. NRC is interested in participating in a Canadian demonstration of the Smith Myers Artemis System.

The Military Problem – Maj Shelden explained the project background and how progress was very slow over the past two years until the recent discovery of the installation of the Artemis System on the Norwegian AW101 SAR helicopters. An explanation of the need to reduce the time required during the search phase of airborne SAR generated additional discussion among the participants. In addition to saving more lives and reducing unnecessary suffering, an understanding that the search phase is the most costly in terms of personnel, material and financial resources reinforced the validity of the project. With 30,675,632 cell phone subscribers in Canada as of 30 Jun 17 (participation rate of 84.5% of the total population), it is obvious that

the ability to locate a specific phone in a SAR scenario could lead to a faster rescue particularly in areas with limited or no cellular coverage.

The Artemis System – Andrew Munro, the representative from Smith Myers Communications, UK provided a very detailed explanation of the Artemis System including;

- a. a brief history of the company;
- b. the background and development of the Artemis System;
- c. how the cellular phone system operates;
- d. operation of the Artemis system;
- e. capabilities of the system;
- f. its compliance with UK privacy laws;
- g. its inability to record or reproduce the information of non-target cellular phones;
- h. its non-interference with non-target cellular customers and 911 service;
- i. how the system identifies and locates the target cell phone using its unique IMSI and IMEI numbers; and
- j. its accuracy.

The presentation was unusually long due to the frequent requests for clarification or additional information of the various topics which, for many of the participants, were new and unfamiliar. Those familiar with airborne SAR offered several new examples where the system could be beneficial in real-world operations. Overall, the presentation was very thorough and well received. Most of the participants' questions and concerns were addressed.

The overall assessment is that digital receiver technology could provide a valuable resource for use in RCAF SAR operations or aide to the civil power during natural disasters. This project has considerable merit and should be pursued with vigor.

#### Summary - The Artemis System;

- a. is a COTS product specifically designed for SAR;
- b. it has a detection range in excess of 25 km (altitude dependent and subject to local atmospheric and geographic conditions);
- c. does not violate UK privacy laws (similar to those in Canada);
- d. does not record any information;
- e. can operate inside or outside cellular coverage zones;
- f. does not interfere with the cellular network (its presence is not noticeable); and
- g. has no ITAR restrictions (Smith Myers has an open export license for Canada).

#### **Action Items**

Maj Shelden

a. 23

b. Draft an annex to the CFAWC / NRC MOU requesting support for testing of the Artemis System in Canada.

c. Confirm funding.

#### Smith Myers

- a. Complete frequency spectrum data sheets previously provided and forward to Maj Shelden cc Maj Rene as soon as possible.
- b. Prepare to provide a condensed version of the Smith Myers presentation IOT satisfy Government of Canada legal representatives that the Artemis System complies with Canadian rules and regulations.

#### NRC Flight Labs

- a. Draft a preliminary test plan which will;
  - a. confirm the ability of the Artemis System to function as advertised on the Canadian cellular network; and
  - b. provide an impartial assessment of the systems performance.
- b. Confirm rough costing details.

#### ISED Canada

- a. Begin drafting applicable documentation to approve trials of the Artemis System in anticipation of the arrival of the completed documentation from Smith Myers.
- b. If the approval requires geographic or operational restrictions, please advise soonest.
- c. Communications through DND FSM rep.

#### **DND FSM**

- a. Continue to act as the conduit between DND and ISED Canada.
- b. Provide additional support to the project as required.

1440 – Adjournment – The official meeting ended and was followed by a tour of the NRC Flight Labs facilities for those who were interested.

#### Noel, Sylvain (IC)

From:

Robichaud, Guy (IC)

Sent:

September-18-17 11:16 AM

To:

Florea, Adrian (IC); Noel, Sylvain (IC)

Cc:

Kennedy, Caroline (IC)

Subject:

TR: Teleconf before next week's meeting re ARTEMIS

Attachments:

ARTEMIS V1.0 April 2017.pdf; ARTEMIS Exec Summary.pdf; 20170407-U-CDE-

CP2016-03 Airborne Cell Tower for Search and Rescue Initi....pdf

Categories:

Catégorie bleue

Colleagues,

In advance of the teleconference this afternoon, please find attached FYI documentation provided by the DND client.

As noted below, I was informed the attached documentation could be shared amongst my ISED clients, noting that one doc is marked commercial confidence, restrict to government agencies.

Regards,

Guy Robichaud

Legal Counsel, ISED Legal Innovation, Science and Economic Development Canada / Government of Canada guy.robichaud@canada.ca / Tel: 343-291-2244 / TTY: 1-866-694-8389

Avocat, Services juridiques d'ISDE Innovations, Sciences et Développement économique Canada / Governement du Canada guy.robichaud@canada.ca / Tél: 343-291-2244 / ATS: 1-866-694-8389

Solicitor-Client Privilege – Not to be circulated Secret professionnel de l'avocat – Ne pas distribuer

This message, and the documents attached hereto, are intended only for the addressee and may contain privileged or confidential information, including information subject to solicitor-client privilege. Any unauthorized disclosure may be unlawful and is strictly prohibited. If you have received this message in error, please notify us immediately. Please then delete the original message and the documents attached thereto. Thank you.

Le présent message et les documents qui y sont joints sont destinés exclusivement au destinataire indiqué et leur teneur peut être confidentielle ou privilégiée. Il est strictement interdit à quiconque d'en prendre connaissance, de les utiliser ou de les divulger. Si vous recevez le present message par erreur, veuillez nous en aviser immédiatement et le détruire, ainsi que les documents qui y sont joints. Mercí.

De: NICK.HOWARD@forces.gc.ca [mailto:NICK.HOWARD@forces.gc.ca]

Envoyé: 18 septembre 2017 11:05

À: Robichaud, Guy (IC); Ken.Macinnes@forces.gc.ca

Objet: FW: Teleconf before next week's meeting re ARTEMIS

Good morning,

The DND client just provided the attached documentation. Guy, please feel free to share amongst your clients, noting that one doc is marked commercial confidence, restrict to government agencies.

You should have the teleconf details now,

Nick

(A-2018-00073) - Page: 112



# CANADIAN FORCES AEROSPACE WARFARE CENTRE



Concept Development & Experimentation Branch

RCAF INITIAL CONCEPT DOCUMENT
AIRBORNE CELLULAR COMMUNICATION CAPABILITY

Concept Number: CP2016-03

### **RCAF Initial Concept Document**

Prepared By:	198L		The state of the s	and the second s
M.D. Shelden	Maj	CD&E 3-2	CFAWC	7 Mar 2017
Name	Rank	Position	Unit	Date
Reviewed By:	Noo	Sem		
R.J. Stockermans	LCol	CD&E D/BH	CFAWC	7 Mar 2017
Name	Rank	Position	Unit	Date
Concept Director	Du			
K.P. Truss	Col	CO	CFAWC	
Name	Rank	Position	Unit	Date
. , .	. //	firmation or Unit CC	))	
M.C. Atkins	Col	SAR CAG Chair	19 Wg Comox	5 APRIL 2017
Name	Rank	Position	Unit	Date
Comments:				

### TABLE OF CONTENTS

TABLE OF CONTENTS	2
INTRODUCTION      1.1. Background/Context      1.2. Purpose of the Concept	3
2. TIME HORIZON, ASSUMPTIONS AND RISK  2.1. Time Horizon  2.2. Assumptions  2.3. Risk	3
3. DESCRIPTION OF THE MILITARY PROBLEM  3.1. The Operating Environment  3.2. The Military Problem	4
SYNOPSIS OF THE CONCEPT & DESIRED EFFECTS.  4.1. Describe the Concept	
LITERATURE REVIEW/BACKGROUND RESEARCH.      Literature Review      Similar Projects	6
6. SUMMARY/CONCLUSION	
7 RECOMMENDATIONS	7

#### 1. INTRODUCTION

#### 1.1. Background/Context

Search and Rescue (SAR) operations can be divided into two distinct phases; the search phase and the rescue phase. Although both offer their own unique challenges, it is the search phase which is typically longer, more urgent, more resource intensive and more costly.

The search phase can further be subdivided into three broad categories depending upon the size, type and anticipated location of the target. The personnel and material resources required will vary greatly depending on whether the search is for;

- a. an aircraft;
- b. ships or small vessels; or
- c. people.

Large or medium commercial aircraft and vessels are usually relatively easy to locate. Transportation regulations and insurance requirements most often result in good quality, well maintained emergency beacons designed to assist in determining their location during an emergency. However, in situations involving people or small craft where there was no beacon or it was damaged or lost, SAR has relied on visual cues for locating them. This can be difficult, particularly if the person(s) lack the equipment, knowledge or ability to provide visual clues to SAR personnel. RCAF SAR operations are conducted using fixed-wing and rotary-wing aircraft whose speed, although well suited for covering a wide area quickly, make it impossible to cover it *comprehensively*. Without some assistance, it can be a significant challenge.

#### 1.2. Purpose of the Concept

The purpose of this concept is to determine if the RCAF can utilize existing cellphone technology to increase the efficiency and therefore the success rate for SAR operations.

#### 2. TIME HORIZON, ASSUMPTIONS AND RISK

#### 2.1. Time Horizon

The concept presented herein is meant to be applied in the Horizon 1 timeframe (1-5 years) and beyond. Therefore, this document will be treated as a living document as the concept is further refined and updated over time.

<sup>&</sup>lt;sup>1</sup> Emergency Locator Transmitter (ELT), Emergency Position Indicating Radio Beacon (EPIRB), Personal Location Beacons (PLB)

#### 2.2. Assumptions

This concept proposal will focus on the particular case of a missing person(s) who is carrying a cellphone, but is not in range of a cellular communication provider. The assumption is that improvements in this particular subset of SAR operations would yield worthwhile results. It could also apply to the case of a missing airplane (forced landing/crash) or vessel where a cell phone is in working condition, even if the owner of that cell phone is not able to use it.

It should be understood that this concept would not impact every single SAR operation, only those where the missing person/aircraft/vessel had an operating cellphone. However, given that there are 23.9 million cell phones in Canada and that 85.6% of households reported having at least one cell phone in 2016,2 it can be expected that most users of the SAR system will carry a cell phone. Furthermore, given that modern cell phones are actually small computers which are useful even when they are out of range, it is reasonable to assume that many people would still carry a cellphone despite their distance from civilization.

#### 2.3. Risk

Mobile cellphone tower technology has been used by both Canadian and US law enforcement since at least 2007 however, there may be challenges in implementing its use by the RCAF. Although the systems are mature, there is an inherent element of risk associated with concept development when it involves the acceptance of any poorly understood or secretive technology. Any prediction made in this paper about future concepts is based on information currently available at the time of writing.

#### 3. DESCRIPTION OF THE MILITARY PROBLEM

#### 3.1. The Operating Environment

Canada has the second-largest land mass and the longest coastline in the world. Not surprisingly, the National Search and Rescue Program has to handle one of the world's largest SAR areas with an area of responsibility (AOR) corresponding to approximately 18-million square kilometres. It is characterized by large sparsely settled regions with limited infrastructure in some areas as well as extremes in geography and weather conditions. The topography includes vast territorial waters on three oceans as well as high mountain ranges, temperate rain forests, boreal forests and high plains. The country's temperature ranges from -45 to +35 degrees Celsius with Arctic conditions in the North during much of the year. The combination of these factors makes the Canadian AOR one of the most challenging in the world for SAR operations.<sup>3</sup>

 <sup>&</sup>lt;sup>2</sup> Canadian Wireless Telecommunications Association (CWTA) 2016 report.
 <sup>3</sup> RCAF Move Functional Concept for Domestic Search and Rescue

#### 3.2. The Military Problem

SAR is a core mandate of the RCAF. Primary Search and Rescue squadrons are located in Comox, Winnipeg, Trenton, Greenwood and Gander. Given the operating environment described in para 3.1, the vast areas that must covered and the difficulty of visually locating small, non-cooperative targets from the air, the challenge can be daunting. In much of Canada, this really is looking for the proverbial needle in a haystack.

#### 4. SYNOPSIS OF THE CONCEPT & DESIRED EFFECTS

#### 4.1. Describe the Concept

As discussed, locating a missing person/aircraft/vessel that is not collocated with some sort of electronic beacon is difficult and unfortunately, sometimes impossible. However, a clear majority of Canadians are in possession of a cell phone which can be considered a beacon as such. As the cost of ownership has fallen rapidly in recent years, it is reasonable to assume those people who can afford to participate in general aviation, snowmobiling, boating or other similar activities can afford, and would be in possession of, a cell phone. Although it might not be in range of a cellphone tower, as long as it is turned on, with the right technology, it could be used to help locate the missing person.

Cell phone service providers provide continuous coverage to their customers by having local towers communicate with and identify all of the cellphones in the local area. When there is no tower available, the cell phone will look for a cell tower to identify itself. Some law enforcement organizations and militaries have been using a mobile cellphone tower simulator to track persons of interest. This technology essentially mimics a cellphone tower to capture information from their cellphone. A cursory search of the internet revealed that this technology is widely available from several countries.

In a search and rescue context, this technology would be used overtly. If the person in distress had a functioning cellphone, they would obviously attempt to get a signal in order to call for help. If no signal is present, the cellphone would continue its attempt to locate a network until it was successful. A mobile cellphone tower simulator mounted in a SAR aircraft would provide this network if it was in range. Once contact was established, maneuvering the aircraft would allow crews to triangulate the cellphone position. In addition, it should then be possible to phone the person directly in order to establish their rescue requirements before deploying SAR personnel. Having direct communications with the missing person(s) even before they are located, would greatly facilitate the search effort as well as the follow-on rescue operation.

#### 5. LITERATURE REVIEW/BACKGROUND RESEARCH

#### 5.1. Literature Review

An extensive review of the internet and online enquiries to US manufacturers yielded the following:

- a. Digital Receiver Technology (DRT) uses international mobile subscriber identity (IMSI) technology and has been used in "fully mature" law enforcement surveillance programs since 2007.
- b. Unclassified articles report that cellphone location accuracy can be as little as ten feet.
- c. US manufacturers will not discuss their products over the phone but may respond to an on-line inquiry. A discussion with a Harris Corp (owned by Boeing) representative indicated that the recent change in the US Administration may make foreign sales much more difficult.
- d. The technology is manufactured in several countries. A Google search of "IMSI catcher for sale" is surprising.
- e. IMSI technology is widely understood and open-source developers have built cell tower simulators for as little as \$1000 (US) in parts for public demonstration at security conferences.

Discussion with DND personnel and a review of current regulations revealed the following:

a. 21(1)(b)

b. In accordance with DAOD 6002-4, it will be necessary to coordinate the implementation of this technology with Assistant Deputy Minister Information Management (ADM(IM)) - DND Frequency Spectrum Management (DFSM). ADM(IM) DFSM is collocated with Industry Canada and is tasked with streamlining DND's access to the domestic spectrum and leveraging Industry Canada's spectrum expertise, engineering resources, tools and databases.

#### 5.2. Similar Projects

a. 15(1).21(1)(b) 15(1).21(1)(b) however, the topic is not open for discussion.

b. There are no known similar DND/GC projects.

#### 6. SUMMARY/CONCLUSION

Search and rescue operations can be difficult, especially in the vast open spaces so common in Canada. Given the recent proliferation of modern cellphones, it should be possible to use cellphone technology onboard an aircraft to locate and perhaps even communicate with a person on the ground. This could significantly reduce the time and expense required to rescue a missing person, and could ultimately save more lives.

#### 7. RECOMMENDATIONS

This concept may provide a reasonable, cost effective solution to shorten the search phase in SAR operations under certain conditions. There are several possible options in pursuing this concept;

- a. use a company which is willing to provide a demonstration or initial sale of their product in order to ascertain its suitability for use in Canadian domestic SAR operations. ATESS would be used for testing and to assist in obtaining airworthiness certification. Three possible companies are Harris Corp (USA), Digital Receiver Technology Inc. (USA) and ASSA SAR (Poland);
- b. determine if it is feasible to design and build a mobile cellphone tower using IMSI technology with existing CAF/RCAF resources.

  21(1)(a).21(1)(b)

  21(1)(a).21(1)(b)
- c. investigate similar research currently underway at Canadian universities; and
- d. propose this project to the new RCAF Innovation Hub at Communitech in Waterloo. The initial response from Communitech is that there are no start-ups in the Waterloo region investigating this type of device. As this technology is already available commercially, it is unlikely that a small company would build a product without an identifiable market.

The recommended option is to purchase a COTS system in order to complete the Proof of Concept phase (para 7.a. above to involve testing through ATESS, and a field trial). Concurrent with this, option 7.c. will be undertaken and option 7.d. if a suitable company is found.

#### Noel, Sylvain (IC)

From:

Mark.Shelden@forces.gc.ca

Sent:

September-26-17 10:04 AM

To:

Jennings, Sion (Ext.)

CHRISTIAN.RENE@forces.gc.ca;

NICK.HOWARD@forces.gc.ca; Ken.Macinnes@forces.gc.ca; Noel, Sylvain (IC); Florea,

Adrian (IC); Robichaud, Guy (IC); BENJAMIN.HIEMSTRA@forces.gc.ca

19(1)

Subject:

Minutes from the Digital Receiver Technology for SAR in Canada Meeting at NRC

Ottawa, 20 Sept 2017

Attachments:

20 Sept 2017 Minutes.docx

Good morning Gentlemen.

Once again, thank you to NRC for allowing us to use their facilities.

Sorry for the delay but I'm involved with other projects that also demand attention.

Thank you all for your short notice participation in something that I consider to be a very worthwhile project. We have the opportunity to make a real change here and I appreciate your time and support.

Encl, please find the minutes from our meeting. I think we are moving the yardsticks forward and I am hoping to get this demonstration / proof of concept completed no later than early in the new year.

I look forward to hearing from our legal advisors.

Call me anytime if you have any questions.

Mark

Maj M.D. Shelden

Concepts Development and Experimentation, Canadian Forces Aerospace Warfare Centre
Royal Canadian Air Force

Mark.Shelden@forces.gc.ca / Tel: 613-392-2811 ext 5614 / CSN 827-5614 / Fax 613-965-2096

Développement de Concepts et Expérimentation / Centre de guerre aérospatiale des Forces canadiennes Aviation royale canadienne

Mark.Shelden@forces.gc.ca / Tél: 613-392-2811 poste 5614 / ATS: 827-5614 / Facsimile 613-965-2096

(A-2018-00073) - Page: 121

# Minutes of the Digital Receiver Technology for SAR Operations Meeting National Research Council Aeroacoustics and Structural Dynamics laboratory Second Street, Ottawa 20 Sept 2017

#### Attendees

Maj Mark Shelden, CFAWC, Project Lead
Sion Jennings, NRC, Project Team Lead
Andrew Munro, Smith Myers Communications Company Lead
Nick Howard, DND Legal Counsel
Ken MacInnis, DND Legal Counsel
Ben Heimstra, DND Legal Counsel
Maj Christian Rene, DND FSM
Sylvain Noel, ISED Canada
Guy Robichaud, ISED Canada Legal Counsel
Adrian Florea, Communications Research Council (CSC), GoC cellular communications advisor.

Thanks again to NRC for providing their facilities to host the meeting.

1330 - Opening Remarks — The second meeting continues to explore the feasibility of using commercial off-the-shelf (COTS) digital receiver technology to assist in Search and Rescue (SAR) operations in Canada. The purpose of this meeting is to determine the legal challenges we may face in using this technology in Canada while complying with all existing legislation.

1335 - The Military Problem – For the new attendees, Maj Shelden explained the project background and how progress was very slow over the past two years until the recent discovery of the installation of the Artemis System on the Norwegian AW101 SAR helicopters. After explaining the goal of reducing the time required for the search phase of airborne SAR in order to save lives and reduce suffering, the discussion sought to provide an understanding that the search phase is the most costly in terms of personnel, material and financial resources. With 30,675,632 cell phone subscribers in Canada as of 30 Jun 17 (participation rate of 84.5% of the total population), it is obvious that the ability to locate a specific phone in a SAR scenario could lead to a faster rescue particularly in areas with limited or no cellular coverage.

1345 - The Artemis System - Andrew Munro, the representative from Smith Myers Communications, UK provided a very detailed explanation of the Artemis System including;

- a. a brief history of the company;
- b. the background and development of the Artemis System;
- c. operation of the Artemis system both
  - a. in-coverage, and
  - b. out-of-coverage.
- d. capabilities of the system;
- e. its ability to be tailored to conform to national privacy laws;
- f. its inability to record or reproduce the information of non-target cellular phones;

- g. its non-interference with non-target cellular customers and 911 service;
- h. how the system identifies and locates the target cell phone using its unique IMSI and IMEI numbers; and
- i. its accuracy.

Although the presentation shorter than that of the 7 Sept meeting, frequent but necessary questioning by the CSC representative and legal counsel resulted in lengthy discussion.

Although SAR and the IMSI concept were new and unfamiliar topics for legal counsel, by the

end of the presentation

21(1)(a).21(1)(b).23

21(1)(a).21(1)(b).23

Mr. Florea was able to ask for, and seek clarification on, those technical areas which were pertinent to the discussion.

#### Summary - The Artemis System;

- a. is a COTS product specifically designed for SAR;
- b. it has a detection range in excess of 25 km (altitude dependent and subject to local atmospheric and geographic conditions);
- c. does not record any information;
- d. can operate inside or outside cellular coverage zones;
- e. does not interfere with the cellular network;
- f. is currently is used for SAR by 15(1),21(1)(b) Norway, 15(1),21(1)(b) without violating the laws of those countries; and
- g. has no ITAR restrictions (Smith Myers has an open export license for Canada).

My overall impression is that the participants found the logic behind the concept sound and that they now have a firm grasp on what we are attempting to do.

21(1)(b).23

21(1)(b).23

#### The Way Forward

21(1)(a),21(1)(b),23

CFAWC will provide funding for the demonstration. Approved.

CFAWC will establish contact with one or more of the major cellular communications carriers and seek their endorsement / support for the upcoming demonstration.

NRC is drafting the preliminary test plan and has tentatively scheduled the NRC Twin Otter as the demonstration platform for Jan 2018.

1540 – Adjournment – The official meeting ended although small discussion groups and sidebars continued until 1720 hrs.

#### Noel, Sylvain (IC)

From: CHRISTIAN.RENE@forces.gc.ca

**Sent:** October-04-17 2:56 PM

To: Parsons2, Eric (IC)

Cc: Kennedy, Caroline (IC); Noel, Sylvain (IC); James.Bronson@forces.gc.ca;

Mark.Shelden@forces.gc.ca; MARIO.LAVOIE2@forces.gc.ca

Subject: Letter of Intent - Search and Rescue Airbourne Cellular Base Station

Attachments: 171004 DND Letter of Intent SAR Airbourne Cellular.pdf; RCAF Initial Concept

Document CP2016-03.pdf; Smith Myers ARTEMIS Exec Summary for Canadian AG Sep 2017.pdf; Preliminary DND 552 Artemis Sep 2017.pdf; AV-289 Antenna description.pdf

Follow Up Flag: Follow up Flag Status: Completed

Categories: Catégorie bleue

#### Good afternoon Sir,

- 1. The Department of National Defence is seeking a capability that will shorten the time needed to find persons in distress, and thus increase the odds of a positive outcome for Search and Rescue scenarios. This capability aims to leverage the cellular telephones of persons in distress as beacons and as a means of communication, even if the person in distress is beyond cellular service coverage.
- 2. As advised by members of the Spectrum Operations group (cc's to this E-mail), I would like to submit the attached letter of intent and its enclosures as to enable your team to start its file on this issue. For the time being we would like to limit distribution of the attachments to ISED and DND addressees given that the prospective supplier considers a good part of the information as proprietary and that uncontrolled sharing could impact on its competitive position.

#### 21(1)(b),23

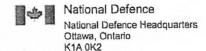
- 4. The next step is to provide a trial to satisfy the DND user community of the system's claimed capability prior to placing further commitments. This test is planned for January 2018 in the Ottawa region, given that NRC aircraft and facilities are in Ottawa. One option is to do this test beyond cellular coverage, at approximately 1 to 2 hours flight time (using Twin-Otter aircraft) North West of Ottawa, whilst the other is to obtain an agreement with a cellular provider to utilise its spectrum for this one-day test. Discussions have been initiated with Bell Canada on 29 September 2017 in this regard. Our desired course of action towards eventual deployment of this capability is to obtain buy-in and agreement from Bell to use its channels (and then from other providers if necessary) which would simplify the spectrum concerns. Initial discussion on 29 September 2017 yielded a positive view about this project from Bell, and that service interference concerns were not as problematic as we initially envisioned. As we obtain permission from the prospective supplier to share more information with Bell, continued discussion will allow Bell to form its official position.
- 5. Your team's support is solicited to geographically identify the gap in cellular service to enable the test described as the first option in the paragraph above. Your further subsequent support is solicited to obtain eventual ISED approval of the system for use in Canada. We will maintain communications with your team and we will cooperate to satisfy ISED requirements to make this capability a reality.

6. This capability is viewed by the Royal Canadian Air Force hierarchy as a key enabler for Search and Rescue, it being perhaps its highest profile domestic mission which contributes towards saving lives. Any and all assistance provided by ISED is greatly appreciated. Please do not hesitate to contact us at any time should you have any questions sir.

Major Christian René, CD

Head of Spectrum Engineering
DND FSM Eng, DG Cyber FD
Canadian Armed Forces
Christian.Rene@forces.gc.ca / Tel: 343-291-3823 / CSN-DSN: nil / TTY: nil

Gestionnaire - ingénierie du spectre GSFM Ing, DG DF Cyber Forces armées canadiennes Christian Rene@forces.gc.ca / Tel: 343-291-3823/ CSN-DSN: nil / TTY: nil



Défense nationale Quartier général de la Défense nationale Ottawa (Ontario) K1A 0K2

2772-4 (DND FSM Eng)

4 October 2017

Mr. Eric Parsons
Senior Director, Spectrum Development and Operations
Innovation, Science and Economic Development
235 Queen Street
Ottawa ON K1A 0H5

LETTER OF INTENT SEARCH AND RESCUE (SAR) AIRBOURNE CELLULAR BASE STATION

References: A. RCAF Initial Concept Document - Airborne Cellular Communication Capability, Concept Number CP2016-03 dated 7 March 2017 (enclosed)
B. ARTEMIS System Executive Summary for Canadian Government (enclosed)
C. Preliminary DND 552 form for ARTEMIS (enclosed)

#### ACCESS TO INFORMATION CONSIDERATIONS

1. Information contained therein discusses future capabilities of a defence establishment and technical information provided by a third party that could be prejudicial to the competitive position of this third party. Until further notice, we request that contents of this document and the enclosures be exempt from disclosure as per the Access to Information Act subsections 15(1)(c), 20(1)(a)(b) and (c), and 21(1)(a).

#### APPLICANT INFORMATION

2. The applicant is the Department of National Defence Frequency Spectrum Management section (DND FSM), 101 Colonel By Drive, Ottawa ON K1A 0K2. Points of contact are Major Christian René (DND FSM Eng) at 343-291-3823, and Major Mark Shelden (representing the end user) at 613-392-2811 extension 5614.

#### PURPOSE OF THE SYSTEM

- 3. DND's requirement is to increase the probability of successful rescue of persons in distress by decreasing the time of the search phase of the operation. The means sought to accelerate the search phase is to enable the cell phone of a person in distress to be used as a locating beacon in addition to a means of communication regardless of the presence of an active cellular network.
- 4. As a key mandate of DND, SAR for lost or missing individuals is carried out in all areas of Canada including urban, rural, forest, mountain and maritime environments.

Canadä

- 5. Not all scenarios benefit from the presence of an Emergency Locator Beacon, namely in the cases of small aircraft, vehicle or vessels where the beacon may be damaged, lost or otherwise unserviceable, or where the person in distress is on foot. In these cases, the search is done visually using SAR aircraft and the sought individual may not be in a position to make his/her presence conspicuous to the rescue party. This provides these search and rescue attempts an uncertain outcome at best.
- 6. Cellular telephones have become ubiquitous in Canada and are used for many purposes beyond voice communications. As such, these tend to be carried by individuals both within and outside of areas where cellular coverage is expected. Technology exists to leverage the cellular telephone carried by a person in distress to locate the person and to establish communications to ascertain the person's disposition and any injuries prior to the airdrop of rescue personnel and materiel. The acceleration of the search phase will significantly increase the odds of a positive outcome to the rescue attempt as it will minimize the victim's exposure to the elements and wildlife, as well as hasten the delivery of medical assistance. A side benefit of accelerating the search phase is a marked reduction in resources needed for the search, which at present can cost between \$850k to \$4M per attempt depending on the number of days for the search, and the number and type of air platforms used. Further details on the concept is enclosed at reference A, and the capabilities of the system are enclosed at reference B.

#### **CONCEPT OF OPERATIONS**

- 7. Upon receipt of a report of missing persons at the Rescue Coordination Centre, details of the lost or missing individual are taken including the person's cellular telephone number and last known location. A request is then made to the cellular provider via lawful means for the IMSI and/or IMEI number associated with the lost or missing individual's device. This number is programmed into the aircraft mounted system to search for this particular device whilst ignoring all others. Once the person's device is in range (approx. 35 km) of the system, the system can be used to do one of the following:
  - Command the telephone to provide its GPS coordinates if the e-911 feature is enabled within the telephone;
  - b. Ping the telephone, and using the time delay in the response, determine the slant distance between the telephone and the system. Repeating the pings as the search and rescue aircraft flies its search pattern will reveal the location of the telephone via triangulation;
  - c. Initiate communication with the person in distress via a text, or with a voice call; and
  - Allow the person in distress to initiate a call to the system.

- 8. The system can also be used to broadcast a text message to any cellular telephone within its range to solicit assistance in a search and to provide means to communicate back to the system on the aircraft.
- 9. The system immediately deletes from memory any hits from IMSI's and IMEI's that do not match its programming and deletes its memory related to the programmed IMSI/IMEI once the system is turned off at the end of the mission. The system is standalone and not connected to an external network.

#### NON-CONFORMING ASPECTS

- 10. Frequencies of operation. Given that the systems establishes communications with Canadian cellular telephones, the system necessarily uses spectrum that is assigned to cellular providers, in particular the GSM 5 band at 824-849 MHz (reception) and 869-894 MHz (transmission). Further technical parameters for the system is enclosed at reference C. Examples of the system are in use in 15(1)

  Norway 15(1) Although the system is also capable of using European GSM 8 band (880.0 915.0 MHz reception and 925.0 960.0 MHz transmission) which are allocated to other purposes in Canada and thus could be licenced for SAR use, there is no guarantee that all cellular telephones in Canada are enabled to use European frequencies. Consultations with Bell Canada have been initiated to establish the possibility of a field test and details of future implementation, and Bell representatives have shown themselves receptive to the concept.
- 11. <u>Use cases</u>. The system can be used in three cases that generate distinct spectrum sharing issues:
  - a. Person in distress and SAR aircraft outside of cellular coverage. This scenario is expected to account for the bulk of the SAR missions using the system. The person in distress would leave the telephone activated in the hopes of finding some service level, while the approaching system would broadcast itself as an available cellular tower. Once the system receives the reply from the few cellular telephones in its field of view, it draws the wanted cellular telephone in its "single subscriber" network. It is only this specific telephone that the system will track and communicate with. Because of the absence of cellular providers, no interference with licensees occurs. This scenario also applies in a disaster situation whereby infrastructure is destroyed or rendered inoperable by an unforeseen event, and the system is the only cellular base station in operation. Should government authorities wish to use this system as a replacement cellular capability during the disaster scenario, the system will need to be re-programmed to accept all IMSI/IMEI's in its field of view as valid cellular telephones;
  - b. Person in distress outside cellular coverage, SAR aircraft within cellular coverage. This scenario will occur when the person in distress is just beyond cellular coverage, and the SAR aircraft is within cellular coverage on account of its altitude. In this instance the telephones not sought by

the system will receive the system's presence broadcast and a channel will be occupied once a call is established with the system. To provide for this scenario, consultation with cellular providers is needed to determine if the providers would be agreeable to use of their spectrum in the case of SAR missions; and

c. Person in distress and SAR aircraft within cellular coverage. This scenario would rarely occur as the person in distress would likely establish a call via normal means. The system could be invoked in the case of a person in distress possessing an active telephone but not being able to provide his/her location. Such cases are envisioned in rural or "cottage country" areas. Consultation with cellular providers is necessary for the same reason as per sub-paragraph b above.

12.	Privacy concerns.	21(1)(b).23
	23	The system cannot actively intercept
telep	hone conversations	nor text messaging, as the IMSI/IMEI information is the only
data	that the system activ	rely hunts for prior to establishing communications with the
desir	ed cellular device.	

#### EXPECTED SERVICE DATE

13. DND aims to have a field test of the system in January 2018. If successful, DND will determine possible future procurement activities for such a system including spectrum use agreements with cellular providers.

#### CONCLUSION

14. The system represents a new and unorthodox capability that raises concerns that are nevertheless surmountable. The potential for this system to save lives has caught the attention of most senior levels within DND, and its adoption will facilitate DND's most high profile domestic mission. ISED's support of this capability is requested.

C.R. René

Major

for the Section Head

Coffee Continue Kolonie

DND Frequency Spectrum Management

343-291-3823

Enclosures: 3



# CANADIAN FORCES AEROSPACE WARFARE CENTRE



Concept Development & Experimentation Branch

RCAF INITIAL CONCEPT DOCUMENT
AIRBORNE CELLULAR COMMUNICATION CAPABILITY

Concept Number: CP2016-03

Title: Airborne Cellular Communication Capability

## **RCAF Initial Concept Document**

Prepared By:	1981		The second se	-
M.D. Shelden	Maj	CD&E 3-2	CFAWC	7 Mar 2017
Name	Rank	Position	Unit	Date
Reviewed By:	Klod	bem		
R.J. Stockermans	LCol	CD&E D/BH	CFAWC	7 Mar 2017
Name	Rank	Position	Unit	Date
Concept Director	Du			
K.P. Truss	Col	CO	CFAWC	
Name	Rank	Position	Unit	Date
Comments:				
	nization, Fo			
M.C. Atkins	Col	SAR CAG Chair	19 Wg Comox	5 APRIL 2017
Name	Rank	Position	Unit	Date
Comments:				

<sup>©</sup> Her Majesty the Queen as represented by the Minister of National Defence, 2017

#### TABLE OF CONTENTS

TABLE OF CONTENTS	2
1. INTRODUCTION	3
Background/Context	3 3
2. TIME HORIZON, ASSUMPTIONS AND RISK	3
2.1. Time Horizon 2.2. Assumptions 2.3. Risk	4
3. DESCRIPTION OF THE MILITARY PROBLEM	4
3.1. The Operating Environment	4 5
4. SYNOPSIS OF THE CONCEPT & DESIRED EFFECTS	5
4.1. Describe the Concept	5
5. LITERATURE REVIEW/BACKGROUND RESEARCH	<del>(</del>
5.1. Literature Review	6
6. SUMMARY/CONCLUSION	7
7. RECOMMENDATIONS	

#### 1. INTRODUCTION

#### 1.1. Background/Context

Search and Rescue (SAR) operations can be divided into two distinct phases; the search phase and the rescue phase. Although both offer their own unique challenges, it is the search phase which is typically longer, more urgent, more resource intensive and more costly.

The search phase can further be subdivided into three broad categories depending upon the size, type and anticipated location of the target. The personnel and material resources required will vary greatly depending on whether the search is for;

- a. an aircraft:
- b. ships or small vessels; or
- c. people.

Large or medium commercial aircraft and vessels are usually relatively easy to locate. Transportation regulations and insurance requirements most often result in good quality, well maintained emergency beacons<sup>1</sup> designed to assist in determining their location during an emergency. However, in situations involving people or small craft where there was no beacon or it was damaged or lost, SAR has relied on visual cues for locating them. This can be difficult, particularly if the person(s) lack the equipment, knowledge or ability to provide visual clues to SAR personnel. RCAF SAR operations are conducted using fixed-wing and rotary-wing aircraft whose speed, although well suited for covering a wide area quickly, make it impossible to cover it *comprehensively*. Without some assistance, it can be a significant challenge.

#### 1.2. Purpose of the Concept

The purpose of this concept is to determine if the RCAF can utilize existing cellphone technology to increase the efficiency and therefore the success rate for SAR operations.

#### 2. TIME HORIZON, ASSUMPTIONS AND RISK

#### 2.1. Time Horizon

The concept presented herein is meant to be applied in the Horizon 1 timeframe (1-5 years) and beyond. Therefore, this document will be treated as a living document as the concept is further refined and updated over time.

<sup>&</sup>lt;sup>1</sup> Emergency Locator Transmitter (ELT), Emergency Position Indicating Radio Beacon (EPIRB), Personal Location Beacons (PLB)

#### 2.2. Assumptions

This concept proposal will focus on the particular case of a missing person(s) who is carrying a cellphone, but is not in range of a cellular communication provider. The assumption is that improvements in this particular subset of SAR operations would yield worthwhile results. It could also apply to the case of a missing airplane (forced landing/crash) or vessel where a cell phone is in working condition, even if the owner of that cell phone is not able to use it.

It should be understood that this concept would not impact every single SAR operation, only those where the missing person/aircraft/vessel had an operating cellphone. However, given that there are 23.9 million cell phones in Canada and that 85.6% of households reported having at least one cell phone in 2016,<sup>2</sup> it can be expected that most users of the SAR system will carry a cell phone. Furthermore, given that modern cell phones are actually small computers which are useful even when they are out of range, it is reasonable to assume that many people would still carry a cellphone despite their distance from civilization.

#### 2.3. Risk

Mobile cellphone tower technology has been used by both Canadian and US law enforcement since at least 2007 however, there may be challenges in implementing its use by the RCAF. Although the systems are mature, there is an inherent element of risk associated with concept development when it involves the acceptance of any poorly understood or secretive technology. Any prediction made in this paper about future concepts is based on information currently available at the time of writing.

#### 3. DESCRIPTION OF THE MILITARY PROBLEM

#### 3.1. The Operating Environment

Canada has the second-largest land mass and the longest coastline in the world. Not surprisingly, the National Search and Rescue Program has to handle one of the world's largest SAR areas with an area of responsibility (AOR) corresponding to approximately 18-million square kilometres. It is characterized by large sparsely settled regions with limited infrastructure in some areas as well as extremes in geography and weather conditions. The topography includes vast territorial waters on three oceans as well as high mountain ranges, temperate rain forests, boreal forests and high plains. The country's temperature ranges from -45 to +35 degrees Celsius with Arctic conditions in the North during much of the year. The combination of these factors makes the Canadian AOR one of the most challenging in the world for SAR operations.<sup>3</sup>

 <sup>&</sup>lt;sup>2</sup> Canadian Wireless Telecommunications Association (CWTA) 2016 report.
 <sup>3</sup> RCAF Move Functional Concept for Domestic Search and Rescue

#### 3.2. The Military Problem

SAR is a core mandate of the RCAF. Primary Search and Rescue squadrons are located in Comox, Winnipeg, Trenton, Greenwood and Gander. Given the operating environment described in para 3.1, the vast areas that must covered and the difficulty of visually locating small, non-cooperative targets from the air, the challenge can be daunting. In much of Canada, this really is looking for the proverbial needle in a haystack.

#### 4. SYNOPSIS OF THE CONCEPT & DESIRED EFFECTS

#### 4.1. Describe the Concept

As discussed, locating a missing person/aircraft/vessel that is not collocated with some sort of electronic beacon is difficult and unfortunately, sometimes impossible. However, a clear majority of Canadians are in possession of a cell phone which can be considered a beacon as such. As the cost of ownership has fallen rapidly in recent years, it is reasonable to assume those people who can afford to participate in general aviation, snowmobiling, boating or other similar activities can afford, and would be in possession of, a cell phone. Although it might not be in range of a cellphone tower, as long as it is turned on, with the right technology, it could be used to help locate the missing person.

Cell phone service providers provide continuous coverage to their customers by having local towers communicate with and identify all of the cellphones in the local area. When there is no tower available, the cell phone will look for a cell tower to identify itself. Some law enforcement organizations and militaries have been using a mobile cellphone tower simulator to track persons of interest. This technology essentially mimics a cellphone tower to capture information from their cellphone. A cursory search of the internet revealed that this technology is widely available from several countries.

In a search and rescue context, this technology would be used overtly. If the person in distress had a functioning cellphone, they would obviously attempt to get a signal in order to call for help. If no signal is present, the cellphone would continue its attempt to locate a network until it was successful. A mobile cellphone tower simulator mounted in a SAR aircraft would provide this network if it was in range. Once contact was established, maneuvering the aircraft would allow crews to triangulate the cellphone position. In addition, it should then be possible to phone the person directly in order to establish their rescue requirements before deploying SAR personnel. Having direct communications with the missing person(s) even before they are located, would greatly facilitate the search effort as well as the follow-on rescue operation.

#### 5. LITERATURE REVIEW/BACKGROUND RESEARCH

#### 5.1. Literature Review

An extensive review of the internet and online enquiries to US manufacturers yielded the following:

- a. Digital Receiver Technology (DRT) uses international mobile subscriber identity (IMSI) technology and has been used in "fully mature" law enforcement surveillance programs since 2007.
- b. Unclassified articles report that cellphone location accuracy can be as little as ten feet.
- c. US manufacturers will not discuss their products over the phone but may respond to an on-line inquiry. A discussion with a Harris Corp (owned by Boeing) representative indicated that the recent change in the US Administration may make foreign sales much more difficult.
- d. The technology is manufactured in several countries. A Google search of "IMSI catcher for sale" is surprising.
- e. IMSI technology is widely understood and open-source developers have built cell tower simulators for as little as \$1000 (US) in parts for public demonstration at security conferences.

Discussion with DND personnel and a review of current regulations revealed the following:

a. 21(1)(b)

b. In accordance with DAOD 6002-4, it will be necessary to coordinate the implementation of this technology with Assistant Deputy Minister Information Management (ADM(IM)) - DND Frequency Spectrum Management (DFSM). ADM(IM) DFSM is collocated with Industry Canada and is tasked with streamlining DND's access to the domestic spectrum and leveraging Industry Canada's spectrum expertise, engineering resources, tools and databases.

#### 5.2. Similar Projects

a. 15(1).21(1)(b) 15(1).21(1)(b) however, the topic is not open for discussion.

b. There are no known similar DND/GC projects.

#### 6. SUMMARY/CONCLUSION

Search and rescue operations can be difficult, especially in the vast open spaces so common in Canada. Given the recent proliferation of modern cellphones, it should be possible to use cellphone technology onboard an aircraft to locate and perhaps even communicate with a person on the ground. This could significantly reduce the time and expense required to rescue a missing person, and could ultimately save more lives.

#### 7. RECOMMENDATIONS

This concept may provide a reasonable, cost effective solution to shorten the search phase in SAR operations under certain conditions. There are several possible options in pursuing this concept;

- a. use a company which is willing to provide a demonstration or initial sale of their product in order to ascertain its suitability for use in Canadian domestic SAR operations. ATESS would be used for testing and to assist in obtaining airworthiness certification. Three possible companies are Harris Corp (USA), Digital Receiver Technology Inc. (USA) and ASSA SAR (Poland);
- b. determine if it is feasible to design and build a mobile cellphone tower using IMSI technology with existing CAF/RCAF resources.

  21(1)(a).21(1)(b)

  21(1)(a).21(1)(b)
- c. investigate similar research currently underway at Canadian universities; and
- d. propose this project to the new RCAF Innovation Hub at Communitech in Waterloo. The initial response from Communitech is that there are no start-ups in the Waterloo region investigating this type of device. As this technology is already available commercially, it is unlikely that a small company would build a product without an identifiable market.

The recommended option is to purchase a COTS system in order to complete the Proof of Concept phase (para 7.a. above to involve testing through ATESS, and a field trial). Concurrent with this, option 7.c. will be undertaken and option 7.d. if a suitable company is found.

10000		broom
202	ALE.	1002
100	787	200
200		2009

National Defence nationale

Délense

Classification:

# Application for Spectrum Supportability Demande d'octroi de Fréquences

Date

Го: À :	From (Office r De (Bureau qu	naking request): ui présente la demande) :	
Equipment nomenclature and / or its smith Myers ARTEMIS Search & Re		du matériel et numéro de modèle	
2. Status of supportability request (ch	eck one) - Centre de demand	le d'octroi (cochez une seule case)	
Experimental research or explora Recherche expérimentale ou dév			Operational Utilisation opérationnelle
,	1. Equipment Usage	- Utilisation du matériel	
<ol> <li>Functional and purpose - Fonction Search &amp; Rescue System</li> </ol>	et but		
<ol> <li>Method of operation - Mode de for Geolocation of Specific Cellular Ha</li> </ol>			
5. Extent of use - Étendue de l'utilisa	tion		
6. Operational environment - Milieu o	'utilisation		
7. Geographical area of experimenta Région géographique de la recher			110 OM 100 100 100 100 100 100 100 100 100 10
8. Geographical area of operational	use - Région géographique de	e l'utilisation opérationnelle	
9. Number of equipments in initial ph	ase - Nombre d'appareils per	ndant la phase initiale	A A A A A A A A A A A A A A A A A A A
10. Number of equipments planned	or operational use - Nombre	d'appareils prévu pour l'utilisation opérationne	lle
Number of these equipments op Nombre d'appareils fonctionnant	erating simultaneously in the simultanément dans le mêm	same electromagnetic environment e milieu électromagnétique	
12. Target date for the start and end Date prévue pour le commencer	of experimental or developm nent et la fin de l'évaluation e	ental evaluation xpérimentale ou de l'évaluation ou développer	nent
13. Target date for operational use -	Date prévue d'utilisation opé	rationnelle	
14. Compliance with requirements of Conformité aux exigences du MI	the DND/CF Radio Frequenc DN/FC Programme de sécurite	cy Safety Program (RFSP des radiofréquences (PSRF)	
In accordance with DAOD 3025-1 (Radio Frequevices under their control have been evaluate Conformément au DOAD 3025-1 (Programme	iency Safety Program) LCMMs, Procud to establish the extent and type of R	rement Officers and Project Managers are responsible for F hazards that may be associated with the devices. GCVM, les agents d'approvisionnement et les gestionnaires e évaluation visant à déterminer l'étendue et la nature des	do amint cont abornée de cuitles
I confirm that a formal request to the RF an RF safety assessment for the relevant	t HERP, HERF and HERO requireme	cordance with DAOD 3026-0, DAOD 3026-1 and CFTO C-5 nts under QETE project no	
Je confirme qu'une demande formelle a DOAD 3026-1 et ITFC C-55-040-001/TS en HERP, HERF et HERO, sous le num	-uui, pour executer l'evaluation de la	Programme de sécurité des radiofréquences du CETQ cor sécurité des radiofréquences, conformément aux exigences	nformément aux DOAD 3026-0, s qui relèvent des besoins
Name (print) - Nom (lettres	moullier)	Signature	Date

DND 552 (08-2012)

Design: Forms Management 613-957-6899 Conception: Gestion des formulaires 613-957-6906

Classification:

Canad'ä

Page 1 /4

Classification:

2. Transmitter Equipment Characteristics - Caractéristiques du matériel émetteur

Nomenclature, Manufacturer's Model No.: ARTEMIS     Désignation, n° de modèle du fabricant :	Manufacturer's Name: Smith Myers Communications Ltd     Nom du fabricant :
Transmitter Installation:     Installation émettrice :	Transmitter Type:     Type d'èmetteur :     Linear Power Amplifier
5. Tuning Range: GSM Band 5 & 8	6. Method of Tuning: Méthode d'accord : Synthesizer
7. RF Channelling Capability: 200KHz Steps Répartition des voles RF :	Emission Designator(s):     Identificateur(s) d'émission :
9. Frequency Tolerance: Tolerance de fréquence :  0.1ppm	
10. Filter Employed	11. Spread Spectrum: Yes - Oui X No - Non
Emission Bandwidth     Largeur de bande de l'émission :	13. Maximum Bit Rate: Debit binaire maximal: GSM Specification Data Rate
Calculated Measured Mesurée	Modulation Techniques and Coding:     Techniques de modulation et de codage :
(a) -3 dB GSM Specification	GMSK
(b) -20 dB GSM Specification	
(c) -40 dB GSM Specification	
(d) -60 dB GSM Specification	
(e) OCCBWGSM Specification  Largeur de bande occupée	15 Movimum Modulation Francis
Largeur de bande occupee	15. Maximum Modulation Frequency: Fréquence de modulation et de codage : N/A
16. Pre-emphasis: Yes - Oui X No - Non Préaccentuation :	17. Deviation Ratio: Rapport de déviation : N/A
18. Pulse Characteristics: Caractéristiques des impulsions :	19. Power - Puissance :
(a) Rate - Fréq. de récurrence GSM Specification	(a) Mean - Moyenne 10W
(b) Width - Durée GSM Specification	
(c) Rise Time - Temps de montée GSM Specification	
(d) Fall Time - Temps de descente GSM Specification	(b) PEP - En crête 10W
(e) Comp Ratio - Rapport de comp. GSM Specification	
Largeur de bande occupée	20. Output Douglast
Largedi de Daride Occupée	20. Output Device: Dispositif de sortie :
21. Harmonic Level: Niveau des harmoniques :	Spurious Level:     Niveau du rayonnement non essentiel: -60dBm
(a) 2 <sup>nd</sup> - 2 <sup>e</sup> -36dBm	
(b) 3 <sup>rd</sup> - 3 <sup>e</sup> -36dBm	23. Industry Canada Type Approval No.:
(c) Other - Autres -36dBm	N° d'homologation de l'industrie Canada :
24. Equipment Frequency Plan:	
Plan de fréquences de l'équipement :	
As per GSM Specification for GSM900 (Band 8) & GSM850 (Ba	nd 5)

DND 552 (06-2012)

Classification:

Classification:	THE PROPERTY OF THE PROPERTY O
3. Receiver Equipment Characteristics	- Caractéristiques du matériel récepteur
Nomenclature, Manufacturer's Model No.     Désignation, n° de modèle du fabricant :     ARTEMIS	Manufacturer's Name: Smith Myers Communications Ltd     Nom du fabricant :
Receiver Installation:     Installation réceptrice :	4. Receiver Type: Type de récepteur :
5. Tuning Range: GSM Specification Band 8 & 5	Method of Tuning:     Méthode d'accord :
7. RF Channelling Capability: 200KHz Répartition des voles RF:	Emission Designator(s):     Identificateur(s) d'émission :
Frequency Tolerance;     Tolérance de fréquence :	1
10. IF Selectivity:     Sélectivité FI:     1st	11. RF Selectivity: Calculated Measured Mesurée  (a) -3 dB 98KHz  (b) -20 dB 152KHz  (c) -40 dB 178KHz
12. IF Frequency: Fréquence intermédiaire :  (a) 1st - 1ére 153MHz	13. DFSM use only: Rèservé au GSFM :
(b) 2 <sup>nd</sup> - 2 <sup>e</sup> (c) 3 <sup>rd</sup> - 3 <sup>e</sup>	14. DFSM use only: Rěservé au GŠFM :
15. Oscillator Tuned: Oscillateur accordé:  (a) Above Tuned Frequency	16. Maximum Bit Rate: Débit binaire maximal : GSM Specification
(b) Below Tuned Frequency Au-dessous de la fréq. d'accord  (c) Either Above or Below the Frequency Ou au-dessus ou au-dessous de la fréq.	17. Sensitivity: Sensibilité:  (a) Sensitivity - Sensibilité -110 dBm  (b) Criteria - Critère  (c) Noise Fig - Facteur de bruit dB
Désaccentuation : 1 res - Oui 12 No - Non	(d) Noise Temp - Temp. de bruit Kelvin  20. Spurious Rejection:
Rejet de fréquence image : 70dB	Rejet des fréquences parasites :
Remarques:	
22. Industry Canada Type Approval No.:  N° d'homologation de l'industrie Canada :	
DND 552 (06-2012) Classification:	Page 3 / 4
	i i

4. Antenna Equipm	ent Characteristics -	Ca	aractéristiques du	ım	atériel d'an	tenne	
— Transmitting Émission	Receiving Réception			×	Transmittin Émission e	g and Re t réceptio	ecelving on
<ol> <li>Nomenclature, Manufacturer's Model No.: Désignation, n° de modèle du fabricant :</li> </ol>	RAMI AV-289	3.	Manufacturer's Nan Nom du fabricant :	ne:	RAMI		
4. Frequency Range: 700 MHZ - 2.70 Gamme de fréquences :	3HZ	5.	Туре:	·····	Broadband	l Airborn	e
5. Polarization: Vertical Polarisation :		7.	Scan Characteristic Caractéristiques de		layage :		
(a) Main Beam Faisceau principal  (b) 1st Major Side Lobe 1st lobe lateral important  9. Beamwidth: Largeur du faisceau :  (a) Horizontal  (b) Vertical  10. Remarks: - Remarques : See attached Data Sheet			(a) Type  (b) Vertical Scan: Balayage vertic  (1) Max Elev Angle de s  (2) Min Elev Angle de s  (3) Scan Rate Vitesse de  (1) Sector Sc Secteur b  (2) Scan Rate Vitesse de  (d) Sector Blankin Effacement de	site site e ba cal: cal: cal: cal: cal: cal: cal: cal	max	s - Oui	√ No - Non
Originator: Position:	To	um	ohone Number: éro de téléphone :			Date:	
DND 552 (06-2012) Classification	n:						Page 4 /

Classification:



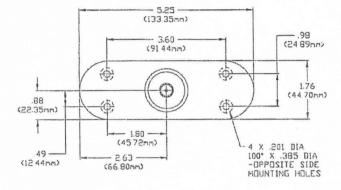
## AV-289

#### **LOUD AND CLEAR**

Part Number: AV-289

#### PRODUCT DESCRIPTION

The AV-289 is a broadband blade type antenna for applications such as Transponder, Cellular, 4G, GSM, PCS, WIFI, and UMTS, however, it is FAA Qualified as a Transponder antenna. The antenna housing is constructed of a Polyarylamide Plastic shell and the base is 6061-T6 aluminum with a chemical conversion coating per MIL-C-5541. The antenna is supplied with an o-ring and mounting hardware. The antenna is designed to operate at speeds up to Mach 1 and altitudes up to 55,000 feet.



4.07 (103.38nm)

#### PRODUCT SPECIFICATIONS

Application Transponder, Cellular, 4G, GSM, PCS,

WIFI, UMTS

Frequency 700-799 MHz (Non TSO Function)

800-849 MHz (Non TSO Function) 850-1029 MHz (Non TSO Function) 1030-1090 MHz (TSO C74d)

1091-2700 MHZ (Non TSO Function)

Impedance 50 Ohms Nominal

VSWR 700-799 MHz 2.8 Max. 800-850 MHz 2.2 Max.

800-850 MHz 2.2 Max. 850-1029 MHz 2.0 Max. 1030-1090 MHz 1.5 Max. 1091-2700 MHz 2.0 Max.

Polarization Vertical

Pattern Omni-Directional

Connector "TNC" Female (Optional: SMA, BNC & N)

RF Power Handling 100 Watts Continuous, 1000 Watts Peak

Gain on 4 ft. Round 4 dBi Nominal Ground Plane 3.5 dBi Nominal

Gain on 2 ft. Round
Ground Plane
3.5 dBl Nominal

Max. Weight 0.60 lbs (0.273 kg)

Color Gloss White, Skydrol resistant polyurethane enamel



	19(1)	
Sent:	October-16-17 5:40 PM	
To:	Mark.Shelden@forces.gc.ca; 19(1)	Jennings, Sion (Ext.);
	19(1) CHRISTIAN.RENE@fc	orces.gc.ca; 19(1)
	Noel, Sylvain (IC)	
Subject:	RE: Teleconference Wed 18 Oct - Digital Receiver	Technology for SAR Operations in
	Canada, Artemis System Technical Discussion	
Categories:	Catégorie bleue	
Good afternoon all, see belo an hour to give enough tim		ether we are available for more than
Functional Overview  1. Please provide a fur	nctional overview of the system	
	pport WCDMA or only GSM? Note from	20(1)(b)
	20(1)(b)	
<ol> <li>How the system wo</li> <li>Who and where the</li> <li>Radio &amp; Spectrum Sp</li> <li>What is the EIRP of control used?</li> <li>What kind of testing</li> <li>Any field test result</li> <li>What is the advers and to all device ty</li> </ol>	their GSM base station/network emulator? What kin g/certification does the equipment undergo? is or experience with European operator? e impact (degradation in RX sensitivity etc.) will the se	ected as per their IMSI?  Id of antenna is used? Is power  ystem generate (to WCDMA/LTE site
transmitting 10W.  12. Besides B5 and B8  13. Is this an FDD syst  14. Any restriction with between B' and A''  15. Minimum requirem a. BW require	d, number of channels, etc. and the BW per channels	and power per channel
transmitting 10W.  12. Besides B5 and B8  13. Is this an FDD syst  14. Any restriction with between B' and A''  15. Minimum requirem a. BW require b. Can we put 200kHz?	tem? How much guard band is required? Inin the bands? For example, could we use B5 expande? ? Itent for the system to work.	and power per channel e same 200kHz? Or we need multipl
transmitting 10W.  12. Besides B5 and B8  13. Is this an FDD syst  14. Any restriction with between B' and A''  15. Minimum requirem a. BW require b. Can we put 200kHz?  16. Can these ARFCN b  Testing  17. Can test plan/time 18. What is the expect	tem? How much guard band is required? Inin the bands? For example, could we use B5 expands? It is it is a system to work. It is a system? 238, 239, 240 and 241 for B5	and power per channel e same 200kHz? Or we need multipl

From: Mark.Shelden@forces.gc.ca [mailto:Mark.Shelden@forces.gc.ca] Sent: Monday, October 16, 2017 3:09 PM To: 19(1) sion.jennings@nrc-cnrc.gc.ca CHRISTIAN.RENE@forces.gc.ca; 19(1) 19(1) sylvain.noel@canada.ca Subject: Teleconference Wed 18 Oct - Digital Receiver Technology for SAR Operations in Canada, Artemis System Technical Discussion Good afternoon Ladies and Gentlemen. Everyone has accepted the teleconference request so it looks like we're good to go on Wed morning. As discussed in our previous correspondence, it will be much easier for Smith Myers to provide a detailed response to questions if they have them in advance. If possible, please send them directly to 19(1) Thank you. Mark Maj M.D. Shelden Concepts Development and Experimentation, Canadian Forces Aerospace Warfare Centre Royal Canadian Air Force Mark.Shelden@forces.gc.ca / Tel: 613-392-2811 ext 5614 / CSN 827-5614 / Fax 613-965-2096

Développement de Concepts et Expérimentation / Centre de guerre aérospatiale des Forces canadiennes

Mark.Shelden@forces.gc.ca / Tél: 613-392-2811 poste 5614 / ATS: 827-5614 / Facsimile 613-965-2096

Aviation royale canadienne

Noel, Sylvain (IC)			
From: Sent: To:	19(1) November-08-17 6:28 PM 19(1) Mark.Shelden@ Sion (Ext.); CHRISTIAN.RENE		19(1) Jennings, 9(1) Noel, Sylvain (IC); 19(1)
Subject:	RE: Minutes of the 18 Oct 20 Rescue Operations TELECON		echnology for Domestic Search and
Good morning/afternoon all.			
19(1) sorry for the delay in getting	g back to you as	19(1)	
To answer your questions below:			
	20(1)(b),21(1)(b)		*
Let me know if you require anyth	ing else at this stage.		
-best			
19(1)			
From: 19(1)			
Sent: 23 October 2017 22:46			
To: Mark.Shelden@forces.gc.ca;		19(1)	
sion.jennings@nrc-cnrc.gc.ca;	19(1)	СН	RISTIAN.RENE@forces.gc.ca 19(1)
19(1) Subject: RE: Minutes of the 18 O TELECONFERENCE Good afternoon all,	sylvain.noel@canada.ca; ct 2017 Digital Receiver Tech	nnology for Domestic	19(1) Search and Rescue Operations
The	19(1)	and has th	e following comments and request:
			io Frequency Energy, from pg. 321 to

The section that I thought would be most relevant is Section 21 – Emission of Radio Frequency Energy, from pg. 321 to 349. What I find though is that although the relative requirements are stated, the actual minimum requirements are not identified in this document. As an example, in section 21.3 1<sup>st</sup> paragraph it is stated...

"This section does not measure or control spurious signals conducted out of the antenna terminals of receivers or transmitters. That control should be specified in the equipment performance standard for that receiver or transmitter. Radio transmitters or receiver/transmitters must meet specified emissions requirements (including the selected +/-50% of the band of frequencies between adjacent channels) while in a non-transmitting or receive mode."

Thus, there's not much one can glean from the document wrt the Artemis system.

To simplify this analysis, could we obtain a compliance summary for whether the Artemis system (i.e., TX) meets or exceeds minimum requirements in the following ETSI specs,

http://www.etsi.org/deliver/etsi gts/05/0505/05.00.00 60/gsmts 0505v050000p.pdf . And where the 3GPP specs are not met, what the adverse impact is to our network and users. I've also attached the relevant 3GPP specs on BTS tests.

Following are specific items we are concerned about:

- 1. spurious emissions across our entire WCDMA/LTE bands in use, not just 850 (which we plan to propose to use)
- 2. mean/peak TX power and EIRP
- 3. Adjacent channel power leakage.

Thanks very much,				
	20(1)(b),1	9(1)		
From: Mark.Shelden@forces.gc.ca [mailto	:Mark.Shelden@fo	rces.gc.ca]		
Sent: Friday, October 20, 2017 1:29 PM				
То		9(1)		
sion.jennings@nrc-cnrc.gc.ca;		HRISTIAN.RENE@forces.g	<u>gc.ca</u> ; 19	0(1)
sylvain.noel@canada.ca;	19(1)	04(4)(1)		
Subject: Minutes of the 18 Oct 2017 TELECONFERENCE		21(1)(b)		
Good afternoon.  Thank you for your participation in subj te time to support this project.				taking the
As I said during the teleconference, I am a				19(1)
and Christian René for providing the bulk omissions are mine alone. If there are any reply all so we can collectively correct it quality	y errors which may		tes. However, any er 21(1)(b)	please
After 1600 today, I will be out of the office	e returning next Fri,	27 Oct. If you need to re	each me, my cell nun	nberis 19(1)
Thanks again.				
Mark			•	

Maj M.D. Shelden

Concepts Development and Experimentation, Canadian Forces Aerospace Warfare Centre Royal Canadian Air Force

Mark.Shelden@forces.gc.ca / Tel: 613-392-2811 ext 5614 / CSN 827-5614 / Fax 613-965-2096

Développement de Concepts et Expérimentation / Centre de guerre aérospatiale des Forces canadiennes

Aviation royale canadienne Mark.Shelden@forces.gc.ca / Tél: 613-392-2811 poste 5614 / ATS: 827-5614 / Facsimile 613-965-2096

#### Noel, Sylvain (IC)

From:

CHRISTIAN.RENE@forces.gc.ca

Sent:

November-14-17 5:04 PM

To:

Souliere, James (IC); Mulvihill, Matthew (IC); Lander, Elisabeth (IC)

Cc:

Noel, Sylvain (IC)

Subject:

Re: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and

Rescue Operations TELECONFERENCE

Attachments:

image002.png; image001.png

Good afternoon all,

As indicated below I will coordinate with James for developmental licencing, and I am certain that it will involve a meeting or a teleconference of some sort which I am looking forward to.

Because the capability we are studying involves propietary information of a commercial entity as well as a new DND capability for search and rescue, I would like to ensure that discussion on this topic within ISED and DND please.

Many thanks for your assistance on this project,

Major Rene DND Frequency Spectrum Management (Engineering) 343-291-3823

Sent from my BlackBerry 10 smartphone on the Rogers network.

From: Rene Maj CR@ADM(IM) D Strat CS@Ottawa-Hull

Sent: Tuesday, November 14, 2017 16:06

To: Souliere, James (IC) Cc: Noel, Sylvain (IC)

Subject: RE: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations

**TELECONFERENCE** 

Hi James,

My right hand person who normally does the licence legwork for me is away on business trip in Europe for the week, and I am away for the next two days. I would like to ask if you can look at the info in this E-mail and see what info is missing for application of the needed developmental license. I would like to then discuss with you on Friday at a time of your convenience of the steps I need to take.

Many thanks,

Major Christian René, CD

Head of Spectrum Engineering DND FSM Eng, DG Cyber FD Canadian Armed Forces

Christian.Rene@forces.gc.ca / Tel: 343-291-3823/ CSN-DSN: nil / TTY: nil

Gestionnaire - ingénierie du spectre

GSFM Ing, DG DF Cyber Forces armées canadiennes

Christian.Rene@forces.gc.ca / Tel: 343-291-3823 / CSN-DSN: nil / TTY: nil

From: Noel, Sylvain (IC) [mailto:sylvain.noel@canada.ca]

Sent: November-14-17 3:31 PM

To: Rene Maj CR@ADM(IM) D Strat CS@Ottawa-Hull < CHRISTIAN.RENE@forces.gc.ca>

Cc: Lavoie MJ@ADM(IM) D Strat CS@Ottawa-Hull <MARIO.LAVOIE2@forces.gc.ca>; Kennedy, Caroline (IC) <caroline.kennedy@canada.ca>; Souliere, James (IC) <james.souliere@canada.ca>; Lander, Elisabeth (IC)

<elisabeth.lander@canada.ca>; Mulvihill, Matthew (IC) <matthew.mulvihill@canada.ca>

Subject: RE: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations

**TELECONFERENCE** 

Hello Christian,

Thank you for the invite, but DOS will not attend the demonstration.

Besides your 20(1)(b).21(1)(b) , DND will need a developmental licence for the demonstration. It will be the first licence to be issued under our new developmental spectrum licence process. My colleague James Souliere will now be your contact person here in ISED HQ concerning this part of the project (demonstration).

I think the gist of the needed information is covered within the current email thread, but I will let James go through the details with you.

Regards,

Sylvain

From: CHRISTIAN.RENE@forces.gc.ca<mailto:CHRISTIAN.RENE@forces.gc.ca> [mailto:CHRISTIAN.RENE@forces.gc.ca]

Sent: November-14-17 10:49 AM

To: Noel, Sylvain (IC); Kennedy, Caroline (IC)

Cc: MARIO.LAVOIE2@forces.gc.ca<mailto:MARIO.LAVOIE2@forces.gc.ca>

Subject: RE: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations

**TELECONFERENCE** 

Bonjour Caroline et Sylvain,

Je ne sais pas si l'un ou l'autre désirez être présents pour le test décrit ci-bas, surtout si votre présence est nécessaire pour éventuellement approuver l'usage de l'appareil. Il me ferait bien sur plaisir de pouvoir vous accompagner dans cette activité.

Tel que décrit dans les courriels ci-bas, nous avons une fenêtre d'une semaine pour le test, et je ne sais pas à ce point-ci si le test va durer une journée pendant cette fenêtre, ou plusieurs journées. Le Centre National des Recherches est en train de concevoir le test et les détails vont sortir prochainement. Ce qui est certain est que l'avion pour le test est disponible dans ces dates.

Il y a plusieurs gens qui vont y être en particulie des gens de Recherche et Sauvetage qui auront les places prioritaires à bord de l'avion, et nous devons penser qui doit être sur l'avion et qui reste au sol basé sur qui sera là. Nous allons demander à Smith Myers si on peut filmer le test, comme ça on ne sera pas une dizaine de personnes tous empilés autour de l'écran dans le petit avion.

Je n'ai pas le budget d'alloué pour emmener des gens autres que moi et Mario, donc il faut voir si vous avez du budget pour ce voyage.

Petawawa est à une heure et demie de route d'ici le long de la 17, et l'endroit choisi, quoique le long d'un chemin, c'est « un peu dans le clos » comme on dit. Il faudra être habillé pour la température surtout si on est au sol. Une autre question est je ne sais pas à ce point-ci est si l'avion part et revient à Ottawa pour chaque vol (ce qui simplifie le voyagement pour les gens qui témoignent du test dans l'avion), ou si le décollage et l'atterrissage de fait à Petawawa (ce qui forcera tout le monde à être à Petawawa). Si ça dure plus qu'une journée, ceux qui vont à Petawawa devront coucher à l'hôtel étant donné la distance avec Ottawa.

Svp m'aviser si vous voulez/pouvez participer, et si vous avez besoin d'une place à bord de l'avion ou si votre témoignage à partir du sol est suffisant.

Merci bien!

Major Christian René, CD

Head of Spectrum Engineering DND FSM Eng, DG Cyber FD Canadian Armed Forces

Christian.Rene@forces.gc.ca<mailto:Christian.Rene@forces.gc.ca> / Tel: 343-291-3823/ CSN-DSN: nil / TTY: nil

Gestionnaire - ingénierie du spectre

GSFM Ing, DG DF Cyber

Forces armées canadiennes

Christian.Rene@forces.gc.ca<mailto:Christian.Rene@forces.gc.ca> / Tel: 343-291-3823 / CSN-DSN: nil / TTY: nil

From: Shelden Maj MD@CFAWC@Trenton

Sent: November-11-17 8:34 AM

To:	19(1)			
Cc:	19(1)			
	19(1)	sion.jennings@	nrc-cnrc.gc.ca <mailto:sion.jennings@nrc-< td=""></mailto:sion.jennings@nrc-<>	
cnrc.gc.ca>;	19(1)		Rene Maj CR@ADM(IM) D Strat	
CS@Ottawa-Hull < CHI	RISTIAN.RENE@forces.gc.ca <ma< td=""><td>ilto:CHRISTIAN.RENE@</td><td>oforces.gc.ca&gt;&gt;;</td></ma<>	ilto:CHRISTIAN.RENE@	oforces.gc.ca>>;	
19(1)		sylvain.noel@c	sylvain.noel@canada.ca <mailto:sylvain.noel@canada.ca>;</mailto:sylvain.noel@canada.ca>	
	19(1)			

Subject: RE: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations TELECONFERENCE

Good morning 19(1) Good morning everyone.

Thank you to you and your team for all of your work and especially to 19(1) for the analysis.

This was the final hurdle to move forward with the demonstration. From the location indicated on the map provided, it appears there is good road access so we can get the simulated survivors into position without making them hike through the woods in Feb. I will contact Petawawa Range Control to make the final arrangements. The army has indicated that they are very interested in supporting and there were no major exercises scheduled as of mid-Oct.

The assigned aircraft is the NRC Falcon 20. Although it is a jet aircraft, it can operate within the flight envelope of the RCAF's soon to be acquired C295 during its search phase.

Artemis system installation scheduled 29 Jan - 2 Feb Flight demonstration scheduled 5 - 9 Feb

Eventually I will need to know who from Bell will be participating and where they would like to be; in the aircraft, in the field or at NRC.

I'll be in the field on and off for the next two weeks. Expect an update NLT 30 Nov once I have the plan worked out a bit better.

Thanks again.

Mark

Maj M.D. Shelden

Concepts Development and Experimentation, Canadian Forces Aerospace Warfare Centre Royal Canadian Air Force Mark.Shelden@forces.gc.ca
/ Tel: 613-392-2811 ext 5614 / CSN 827-5614 / Fax 613-965-2096

Développement de Concepts et Expérimentation / Centre de guerre aérospatiale des Forces canadiennes Aviation royale canadienne Mark.Shelden@forces.gc.ca<mailto:Mark.Shelden@forces.gc.ca> / Tél: 613-392-2811 poste 5614 / ATS: 827-5614 / Facsimile 613-965-2096

From:	19(1)	
Sent: November-	-10-17 3:47 PM	
To: Shelden Maj	MD@CFAWC@Trenton < Mark	Shelden@forces.gc.ca <mailto:mark.shelden@forces.gc.ca>&gt;; 19(1)</mailto:mark.shelden@forces.gc.ca>
	19(1)	
	19(1)	sion.jennings@nrc-cnrc.gc.ca <mailto:sion.jennings@nrc-< td=""></mailto:sion.jennings@nrc-<>
cnrc.gc.ca>;	19(1)	Rene Maj CR@ADM(IM) D Strat
CS@Ottawa-Hull	I < CHRISTIAN.RENE@forces.gc.	ca <mailto:christian.rene@forces.gc.ca>&gt;;</mailto:christian.rene@forces.gc.ca>
	19(1)	sylvain.noel@canada.ca <mailto:sylvain.noel@canada.ca>;</mailto:sylvain.noel@canada.ca>
	19(1)	
Subject: RE: Min	utes of the 18 Oct 2017 Digital	Receiver Technology for Domestic Search and Rescue Operations
TELECONFERENC	CE	
Good afternoon	all,	
		nendations for frequency and location to perform the Artemis test in
	nks specifically to 19(1)	who performed this analysis. Please note that for now this is a
		nd does not yet represent an assignment for 'production' use on a
national scale.	(a) test cases and	participate in the testing given the interaction with our customer devices
		nt in the field to perform this testing activity. We are ready to
participate in a v	working team as a next step.	
Best regards,		
19(1)		
Frequency/Char	inel to use:	

ARFCN 240 (center freq 891.6 DL and 846.6 UL). This is a 200 KHz channel totally in our expended spectrum at the edge of our B'. As discussed this might not be the final channel we would like them to use, but good enough for testing purposes. This band is not being used now in that region, so no impact to surrounding sites during our test

See below a website that provides center frequencies of ARFCN numbers (we can click on the link and select GSM850):

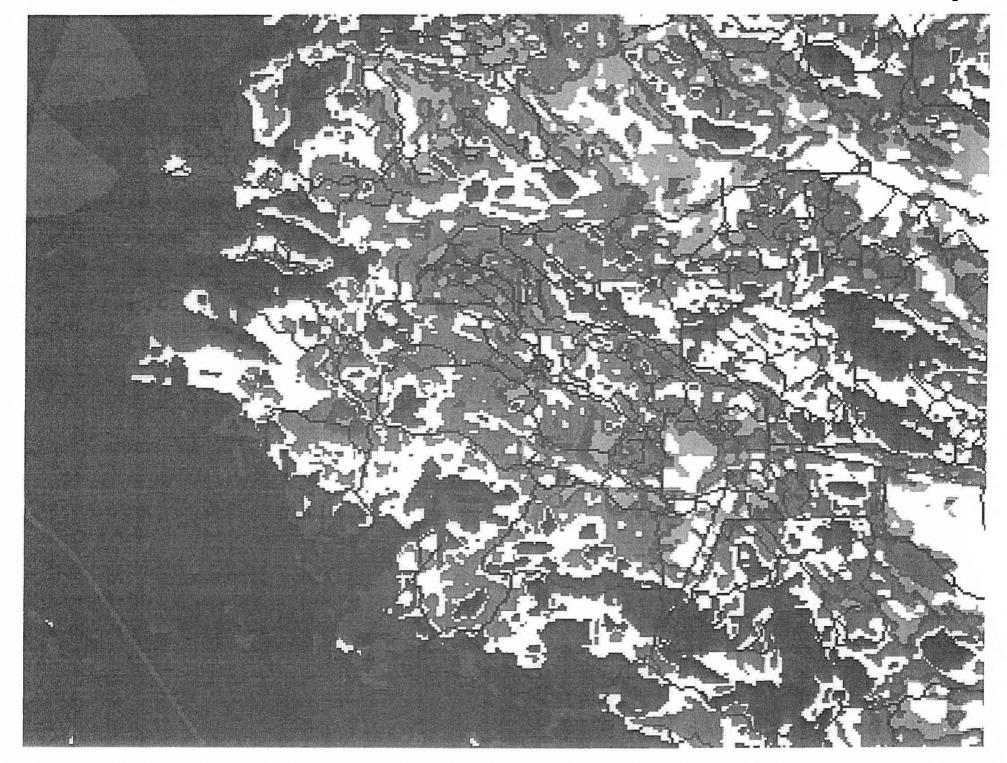
http://niviuk.free.fr/gsm\_arfcn.php<http://esfsecev-ty3013>

[cid:image001.png@01D35D62.8242F240	0]
[cid:image002.png@01D35D62.8242F240	0]
From: Mark.Shelden@forces.gc.ca <mailt Sent: Friday, October 20, 2017 1:29 PM To:</mailt 	to:Mark.Shelden@forces.gc.ca> [mailto:Mark.Shelden@forces.gc.ca]
	19(1)
19(1)	sion.jennings@nrc-cnrc.gc.ca <mailto:sion.jennings@nrc-< td=""></mailto:sion.jennings@nrc-<>
cnrc.gc.ca>;	19(1)
CHRISTIAN.RENE@forces.gc.ca <mailto:c< th=""><td></td></mailto:c<>	
19(1)	sylvain.noel@canada.ca <mailto:sylvain.noel@canada.ca>;</mailto:sylvain.noel@canada.ca>
Subject: Minutes of the 18 Oct 2017 Digi TELECONFERENCE	tal Receiver Technology for Domestic Search and Rescue Operations
Good afternoon.	
As I said during the teleconference, I am and Christian René for providing the bull	an operator not a technician. Therefore, I would like to thank  19(1)  k of the technical notes contained in the minutes. However, any errors or ny errors which may adversely affect decision making process, please quickly.
After 1600 today, I will be out of the offi 19(1)	ice returning next Frì, 27 Oct. If you need to reach me, my cell number is 19(1)
Thanks again.	
Mark Maj M.D. Shelden	
	ration, Canadian Forces Aerospace Warfare Centre Royal Canadian Air Force rk.Shelden@forces.gc.ca> / Tel: 613-392-2811 ext 5614 / CSN 827-5614 / Fax
	nentation / Centre de guerre aérospatiale des Forces canadiennes Aviation

Area to perform the test (Star on simulation represent the area with the dot on the Map):

ATS: 827-5614 / Facsimile 613-965-2096





#### Noel, Sylvain (IC)

From:

MARIO.LAVOIE2@forces.gc.ca

Sent:

November-22-17 2:18 PM

To:

Souliere, James (IC)

Cc:

Noel, Sylvain (IC); CHRISTIAN.RENE@forces.gc.ca

Subject:

DND Developmental Licence Request - Airborne Cell Base Station Trials - Petawawa - 5

- 9 Feb. 2018

Attachments:

DND Developmental Licence Request Letter of Intent - Testing Aeronautical Cell Base Station.docx; FW: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations TELECONFERENCE; 171004 DND Letter of Intent SAR Airbourne Cellular.pdf; DND Form Draft 2.pdf; AV-289 Antenna description.pdf; RCAF

Initial Concept Document CP2016-03.pdf

Maybe with a better title...

Mario Lavoie DND Frequency Spectrum Management Spectrum Engineering DND FSM Engr 2 Work: 343-291-3822 Cell: 613-697-7925

mario.lavoie2@forces.gc.ca

From: Lavoie MJ@ADM(IM) D Strat CS@Ottawa-Hull

Sent: November-22-17 2:16 PM

To: 'Souliere, James (IC)' <james.souliere@canada.ca>; 'Noel, Sylvain (IC)' <sylvain.noel@canada.ca>

Cc: 'Kennedy, Caroline (IC)' <caroline.kennedy@canada.ca>; 'Lander, Elisabeth (IC)' <elisabeth.lander@canada.ca>;

'Mulvihill, Matthew (IC)' <matthew.mulvihill@canada.ca>; Rene Maj CR@ADM(IM) D Strat CS@Ottawa-Hull

<CHRISTIAN.RENE@forces.gc.ca>

Subject: RE: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations

**TELECONFERENCE** 

James, Sylvain,

Find attached the filled in form as requested. Let me know if you need anything else. Although the actual testing is occurring in the first week of February, we would like to know fairly quickly if this is going to be accepted for planning purpose (lots of logistics to organize and reserve).

thanks.

Mario Lavoie DND Frequency Spectrum Management Spectrum Engineering DND FSM Engr 2 Work: 343-291-3822

Cell: 613-697-7925

mario.lavoie2@forces.gc.ca

From: Lavoie MJ@ADM(IM) D Strat CS@Ottawa-Hull

Sent: November-21-17 9:56 AM

To: 'Souliere, James (IC)' < james.souliere@canada.ca>; Noel, Sylvain (IC) < sylvain.noel@canada.ca>

Cc: Kennedy, Caroline (IC) < <a href="mailto:caroline.kennedy@canada.ca">caroline.kennedy@canada.ca</a>; Lander, Elisabeth (IC) < <a href="mailto:elisabeth.lander@canada.ca">elisabeth.lander@canada.ca</a>; Rene Maj CR@ADM(IM) D Strat CS@Ottawa-Hull

<CHRISTIAN.RENE@forces.gc.ca>

Subject: RE: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations

**TELECONFERENCE** 

roger on that...

I will fill the form and attach any other pertinent documentation and forward to you guys... thanks.

Mario Lavoie
DND Frequency Spectrum Management
Spectrum Engineering
DND FSM Engr 2
Work: 343-291-3822
Cell: 613-697-7925

mario.lavoie2@forces.gc.ca

From: Souliere, James (IC) [mailto:james.souliere@canada.ca]

Sent: November-21-17 9:37 AM

To: Lavoie MJ@ADM(IM) D Strat CS@Ottawa-Hull <MARIO.LAVOIE2@forces.gc.ca>; Noel, Sylvain (IC)

<sylvain.noel@canada.ca>

Cc: Kennedy, Caroline (IC) < <a href="mailto:caroline.kennedy@canada.ca">caroline.kennedy@canada.ca</a>; Lander, Elisabeth (IC) < <a href="mailto:elisabeth.lander@canada.ca">elisabeth.lander@canada.ca</a>; Rene Maj CR@ADM(IM) D Strat CS@Ottawa-Hull < CHRISTIAN.RENE@forces.gc.ca>

**Subject:** RE: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations TELECONFERENCE

Hi Mario.

For this particular situation, and in light of the evolving process for developmental licences we will handle the licensing process at our HQ and can bypass the SMS application. We would be happy to have the letter of intent (as referred in your previous email) completed and sent to DGSO staff (myself, Caroline, Elisabeth, Matthew and Sylvain).

I hope that this helps,

James Souliere Tel: 613-854-1979

From: MARIO.LAVOIE2@forces.qc.ca [mailto:MARIO.LAVOIE2@forces.qc.ca]

Sent: November-21-17 9:17 AM

To: Noel, Sylvain (IC); Souliere, James (IC)

Cc: Kennedy, Caroline (IC); Lander, Elisabeth (IC); Mulvihill, Matthew (IC); CHRISTIAN.RENE@forces.gc.ca

Subject: RE: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations

**TELECONFERENCE** 

Hello again Sylvain and James,

Just noticed that we do have the attached letter of intent for us to fill in. So I assume that we do start an SMS application as per usual and attach a fill in version of the letter along with any other pertinent documentation ... do I have this right?

thanks.

Mario Lavoie
DND Frequency Spectrum Management
Spectrum Engineering
DND FSM Engr 2
Work: 343-291-3822
Cell: 613-697-7925
mario.lavoie2@forces.gc.ca

From: Lavoie MJ@ADM(IM) D Strat CS@Ottawa-Hull

Sent: November-21-17 9:08 AM

To: Noel, Sylvain (IC) < sylvain.noel@canada.ca >; Souliere, James (IC) < james.souliere@canada.ca >

Cc: Kennedy, Caroline (IC) < <a href="mailto:caroline.kennedy@canada.ca">caroline.kennedy@canada.ca</a>; Lander, Elisabeth (IC) < <a href="mailto:elisabeth.lander@canada.ca">elisabeth.lander@canada.ca</a>; Mulvihill, Matthew (IC) < <a href="mailto:matthew.mulvihill@canada.ca">matthew.mulvihill@canada.ca</a>; Rene Maj CR@ADM(IM) D Strat CS@Ottawa-Hull < < CHRISTIAN.RENE@forces.gc.ca>

**Subject:** RE: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations TELECONFERENCE

Hello Sylvain and James,

In regards to the new developmental spectrum licence process you are mentioning, what is the official document which we are supposed to be

following. Other than the present GL-03 which dates back to 2014, is there new official directives? I remember a few months ago where there was

a consultation on a new framework for developmental licences, I do not remember seeing a decision document or new guidelines.

As far as I can see, it's only a matter of applying through SMS. Please forward us the new guidelines and/or whatever else we are supposed to be doing. Maybe a meeting between us would be required?

thanks.

Mario Lavoie
DND Frequency Spectrum Management
Spectrum Engineering
DND FSM Engr 2
Work: 343-291-3822
Cell: 613-697-7925
mario.lavoie2@forces.gc.ca

From: Noel, Sylvain (IC) [mailto:sylvain.noel@canada.ca]

Sent: November-14-17 3:31 PM

To: Rene Maj CR@ADM(IM) D Strat CS@Ottawa-Hull < CHRISTIAN.RENE@forces.gc.ca > Cc: Lavoie MJ@ADM(IM) D Strat CS@Ottawa-Hull < MARIO.LAVOIE2@forces.gc.ca >; Kennedy, Caroline (IC) < caroline.kennedy@canada.ca >; Souliere, James (IC) < james.souliere@canada.ca >; Lander, Elisabeth (IC) < elisabeth.lander@canada.ca >; Mulvihill, Matthew (IC) < matthew.mulvihill@canada.ca >

Subject: RE: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations TELECONFERENCE

Hello Christian,

Thank you for the invite, but DOS will not attend the demonstration.

Besides your agreement with DND will need a developmental licence for the demonstration. It will be the first licence to be issued under our new developmental spectrum licence process. My colleague James Souliere will now be your contact person here in ISED HQ concerning this part of the project (demonstration).

I think the gist of the needed information is covered within the current email thread, but I will let James go through the details with you.

Regards,

Sylvain

From: CHRISTIAN.RENE@forces.gc.ca [mailto:CHRISTIAN.RENE@forces.gc.ca]

Sent: November-14-17 10:49 AM

To: Noel, Sylvain (IC); Kennedy, Caroline (IC)

Cc: MARIO.LAVOIE2@forces.gc.ca

Subject: RE: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations

TELECONFERENCE

Bonjour Caroline et Sylvain,

Je ne sais pas si l'un ou l'autre désirez être présents pour le test décrit ci-bas, surtout si votre présence est nécessaire pour éventuellement approuver l'usage de l'appareil. Il me ferait bien sur plaisir de pouvoir vous accompagner dans cette activité.

Tel que décrit dans les courriels ci-bas, nous avons une fenêtre d'une semaine pour le test, et je ne sais pas à ce point-ci si le test va durer une journée pendant cette fenêtre, ou plusieurs journées. Le Centre National des Recherches est en train de concevoir le test et les détails vont sortir prochainement. Ce qui est certain est que l'avion pour le test est disponible dans ces dates.

Il y a plusieurs gens qui vont y être en particulier des gens de Recherche et Sauvetage qui auront les places prioritaires à bord de l'avion, et nous devons penser qui doit être sur l'avion et qui reste au sol basé sur qui sera là. Nous allons demander à Smith Myers si on peut filmer le test, comme ça on ne sera pas une dizaine de personnes tous empilés autour de l'écran dans le petit avion.

Je n'ai pas le budget d'alloué pour emmener des gens autres que moi et Mario, donc il faut voir si vous avez du budget pour ce voyage.

Petawawa est à une heure et demie de route d'ici le long de la 17, et l'endroit choisi, quoique le long d'un chemin, c'est « un peu dans le clos » comme on dit. Il faudra être habillé pour la température surtout si on est au sol. Une autre question est je ne sais pas à ce point-ci est si l'avion part et revient à Ottawa pour chaque vol (ce qui simplifie le voyagement pour les gens qui témoignent du test dans l'avion), ou si le décollage et l'atterrissage de fait à Petawawa (ce qui forcera tout le monde à être à Petawawa). Si ça dure plus qu'une journée, ceux qui vont à Petawawa devront coucher à l'hôtel étant donné la distance avec Ottawa.

Svp m'aviser si vous voulez/pouvez participer, et si vous avez besoin d'une place à bord de l'avion ou si votre témoignage à partir du sol est suffisant.

Merci bien!

Major Christian René, CD

Head of Spectrum Engineering DND FSM Eng, DG Cyber FD Canadian Armed Forces

Christian.Rene@forces.gc.ca / Tel: 343-291-3823/ CSN-DSN: nil / TTY: nil

Gestionnaire - Ingénierie du spectre GSFM Ing, DG DF Cyber Forces armées canadiennes

Christian.Rene@forces.gc.ca / Tel: 343-291-3823/ CSN-DSN: nil / TTY: nil

From: Shelden Maj MD@CFAWC@Trenton

Sent: November-11-17 8:34 AM

19(1)			
	19(1)		sion.jennings@nrc-cnrc.gc.ca
Rene Ma	j CR@ADM(IM) D Stra	t CS@Ottawa-Hull < <u>C</u> H	IRISTIAN.RENE@forces.gc.ca>;
sylvain.noel	@canada.ca;	19(1)	
	Rene Ma	19(1)	19(1) Rene Maj CR@ADM(IM) D Strat CS@Ottawa-Hull < <u>C</u> H

Subject: RE: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations

TELECONFERENCE

Good morning 19(1) Good morning everyone.

Thank you to you and your team for all of your work and especially to 19(1) for the analysis.

This was the final hurdle to move forward with the demonstration. From the location indicated on the map provided, it appears there is good road access so we can get the simulated survivors into position without making them hike through the woods in Feb. I will contact Petawawa Range Control to make the final arrangements. The army has indicated that they are very interested in supporting and there were no major exercises scheduled as of mid-Oct.

The assigned aircraft is the NRC Falcon 20. Although it is a jet aircraft, it can operate within the flight envelope of the RCAF's soon to be acquired C295 during its search phase.

Artemis system installation scheduled 29 Jan - 2 Feb

Flight demonstration scheduled 5 - 9 Feb

Eventually I will need to know who from will be participating and where they would like to be; in the aircraft, in the field or at NRC.

I'll be in the field on and off for the next two weeks. Expect an update NLT 30 Nov once I have the plan worked out a bit better.

Thanks again.

Mark

Maj M.D. Shelden

Concepts Development and Experimentation, Canadian Forces Aerospace Warfare Centre

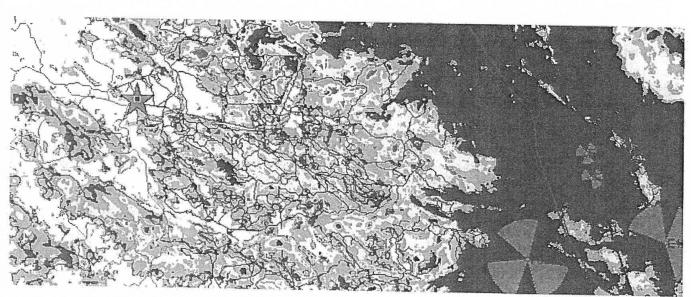
Royal Callaulali All Force				
Mark.Shelden@forces.gc.ca / Tel: 61	3-392-2811 ext 5614 / CSN 827-561	.4 / Fax 613-965-209	96	
Développement de Concepts et Expé Aviation royale canadienne Mark.Shelden@forces.gc.ca / Tél: 61:	4			
From: 19(1)				
Sent: November-10-17 3:47 PM				
To: Shelden Maj MD@CFAWC@T	renton < Mark. Shelden@forces.s	<u>(c.ca</u> >;	19	9(1)
19(1)	sion.jennings@nrc-cnrc.gc.ca	19(1)	R	Rene Maj CR@ADM(IM)
D Strat CS@Ottawa-Hull < CHRIST	AN.RENE@forces.gc.ca>;	19(1)	; sylvain.no	el@canada.ca;
19(1)				
Subject: RE: Minutes of the 18 Oct TELECONFERENCE	t 2017 Digital Receiver Technolo	gy for Domestic S	earch and Ro	escue Operations
Good afternoon all,				
The 20(1)(b),21(1)(b) can provide the following the provide the following the provide the following team as a control of the provide the following team as a control of the provide the following team as a control of the provide the following team as a control of the provide the following team as a control of the provide the following team as a control of the provide the following team as a control of the provide the following team as a control of the provide the following team as a control of the provide the following team as a control of the provide the following team as a control of the provide the following team as a control of the provide the following team as a control of the provide the following team as a control of the provide the following team as a control of the provide the following team as a control of the provide the following team as a control of the provide the provi	19(1) who performed the testing and does not yet repeat cases and participate in the trees/equipment in the field to p	this analysis. Plea present an assignment esting given the in	ase note tha nent for 'pro nteraction w	it for now this is a oduction' use on a rith our customer device:
Best regards, 19(1)				
Frequency/Channel to use:				
ARFCN 240 (center freq 891.6 DL of our B'. As discussed this might		uld like them to us	se, but good	enough for testing

purposes. This band is not being used now in that region, so no impact to surrounding sites during our test

See below a website that provides center frequencies of ARFCN numbers (we can click on the link and select GSM850):

http://niviuk.free.fr/gsm\_arfcn.php

Area to perform the test (Star on simulation represent the area with the dot on the Map):





From: Mark.Shelden@forces.gc.ca [mailto:Mark.Shelden@forces.gc.ca]
Sent: Friday, October 20, 2017 1:29 PM

,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	1 141			
To: 19(1)		< <u>19(1)</u>		
sion.jennings@nrc-cnrc.gc.ca;	19(1)	CHRISTIAN.RENE@forces.gc.ca	19(1)	
sylvain.noel@canada.ca;	19(1)		19(1)	

Subject: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations TELECONFERENCE

Good afternoon.

Thank you for your participation in subj telecon. I know everyone has busy schedules and I appreciate you taking the time to support this project.

As I said during the teleconference, I am an operator not a technician. Therefore, I would like to thank 19(1) and Christian René for providing the bulk of the technical notes contained in the minutes. However, any errors or omissions are mine alone. If there are any errors which may adversely affect decision making process, please reply all so we can collectively correct it quickly.

After 1600 today, I will be out of the office returning next Fri, 27 Oct. If you need to reach me, my cell number is 19(1)

19(1)

Thanks again.

Mark

Maj M.D. Shelden

Concepts Development and Experimentation, Canadian Forces Aerospace Warfare Centre Royal Canadian Air Force

Mark.Shelden@forces.gc.ca / Tel: 613-392-2811 ext 5614 / CSN 827-5614 / Fax 613-965-2096

Développement de Concepts et Expérimentation / Centre de guerre aérospatiale des Forces canadiennes Aviation royale canadienne Mark.Shelden@forces.gc.ca / Tél: 613-392-2811 poste 5614 / ATS: 827-5614 / Facsimile 613-965-2096

# Testing and Trialing of Services in Canada

### Letter of Intent

#### **Notes for Applicants**

- 1. This Letter of Intent sets out the standard information which is required for obtaining authority to test/trial wireless technology/services in Canada.
  - ISED may seek further information or clarification from the applicant at any point throughout the application process or authorization period.
- 2. Upon completion of the application form below, please send to the <u>district or regional office</u> closest to your intended testing site.
- To submit a complete application, it is necessary to complete all sections of the form relevant to your application. If there is insufficient space on the form, please append additional information with a secondary form. Your District or Regional Office can provide additional guidance to this regard.
- 4. The fee for a developmental radio licence is \$41.00 for 12 months, or \$3.40 per month. This fee is applied to each apparatus in your radio licence test/trial
- 5. The fee for a developmental spectrum licence has yet to be established and will not be applied until such a time. In order to obtain a developmental spectrum licence, the applicant must demonstrate that the nature of the testing concerns high density, low-powered systems across a specified area.
- 6. General inquiries related to the process for which to obtain a developmental radio or spectrum licence in Canada may be sent to:
  - ic.spectrumoperations-operationsduspectre.ic@canada.ca

<sup>&</sup>lt;sup>1</sup> This fee will be established through a future fee review process.

# **Developmental Spectrum Licence Application - Letter of Intent**

# Section 1 - Contact Details

1	Applicant's name	
	National Defence Headquarters	
2	Address	
	DND FSM	
	101 Colonel By Drive	
	Ottawa ON K1A 0K2	•
3	Telephone number	
	Mario Lavoie (343-291-3822) / Maj Christian René (343-291-3823)	
4	E-mail address	
	Mario.lavoie2@forces.gc.ca / Christian.rene@forces.gc.ca	
5	Proof of Canadian citizenship, residency or registration as per	[Not necessary for DND]
	section 9 of the <u>Radiocommunication Regulations</u> to determine	
	eligibility to hold a licence	

# Section 2 - Test Details

6	Nature of your test, i.e. business case, proof of concept, purpose of the system/device Please see attached already submitted letter of intent number 171004 Intended results?  Please provide us with an abstract of what this test/trial aims to discover/prove.	[please provide as much information as possible and take as much space as you need]
6.1	Sector that your apparatus/service concerns (i.e. health, manufacturing, two-way communication, agriculture, etc.) DND Search and Rescue	
6.2	How does your test relate to research and development, i.e. differ from existing wireless rules or standards Use of airborne mobile cell phone base station	[ATTACH]
6.3	If publicly funded, please attach project and funding approval documentation  Not Available	
7	General location of the test CFB Petawawa Training area	
8	Total number of apparatus One airborne base station and one ground cell phone	
9	Frequency/band of test Ch 240 (downlink at 891.6 and uplink at 846.4 MHz)	
10	Are there alternative frequencies/bands that you could use to conduct this test?  No	
11	Are multiple channels required? If so, for what purpose?  No	

# Developmental Spectrum Licence Application - Letter of Intent

12	Duration of test	
	Currently slated for 5 – 9 Feb, 2018	

# Section 3 - Technical Details

Please complete all sections, if applicable.

## Station Information

Jta	CONTINUO MACION	
13	Please provide the site/area location(s) for the station(s)	
	As per map in attached email, in CFB Petawawa	
14	Latitude &	[can provide areas in a
	Longitude of site/area location(s)	general way (i.e. cities) or on a
	As per map in attached email, in CFB Petawawa	map]
15	Antenna Structure Height Above Ground (m)	[since this will be a mobile
	Searching aircraft will use altitudes from 1000 to 10000 feet ASL	station operating from the sky
	Cell phone will be on the ground	(aerial), please describe the
		operating height]
16	Antenna Beamwidth (Horizontal and Vertical Planes)	
	OMNI	
17	Radius of Operation [km]	
	5 km	
18	Polarization	
	Vertical	
19	Azimuth [deg]	
	Omni	
20	Elevation Angle [deg]	
	Omni	
21	Equivalent Isotropically Radiated Power (EIRP) of the station	
	(range)	
	10 Watts transmitter + 4 db antenna = 25.1 Watts EIRP	

# **Apparatus Information**

22	Manufacturer		
	Smith Myers Communications		
23	Make/Model Type		
	Artemis		
24	Operating Frequency (MHz)	TX	RX
	869.2 – 894 MHz Transmission		
	824 – 849 MHz Reception		
25	Occupied Bandwidth (kHz)		
	200		
26	Please describe the intended use of apparatus:		
	As per attached letter of intent 171004, we are searching for a		
	person in an unknown location, max EIRP is always at		
	maximum power. The cell base station will be searching for		

# Developmental Spectrum Licence Application - Letter of Intent

	the cellular phone of the person in distress in an attempt to locate and communicate with the her/him.	
27	Description of type of traffic that will be carried Cell phone type GSM standard	

# Other Technical Details

28	Please provide any other technical information that will help us
	provide you with the appropriate authorization.
	As per all included documentation

# Attestation of Safety Code 6

29	Will your test meet the safety standards concerning radio frequency exposure as stated in <u>TN-261</u> ? Yes		
30	Please sign the box to the right to confirm that your test will meet the compliance standards related to safety code 6.	Sign:	Mario Lavoie

# Towers

31	Does your test require the construction of a tower? (yes/no) No	
32	If yes, please complete form <u>IC-2430</u> - <i>Radiocommunication and Broadcasting Antenna Systems Attestation</i>	[ATTACH FORM]

# Submitting your Letter of Intent

33	I understand that any developmental licence issued will be subject to such terms and conditions as may be set by the Minister.		
	I am aware that any such developmental licence will be of a temporary nature only and will not convey an entitlement to its renewal, the issue of a full authorisation or the continued use of radio spectrum.	Date:	22 Nov 2017
		Sign:	Mario Lavoie
	I confirm that the information provided in this application is true and that it gives an accurate and complete account of the circumstances for which this application is made.	3	

## Noel, Sylvain (IC)

From:

CHRISTIAN.RENE@forces.gc.ca

Sent:

November-21-17 9:11 AM

To:

MARIO.LAVOIE2@forces.qc.ca

Subject:

FW: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and

Rescue Operations TELECONFERENCE

Attachments:

SITT-STIT-#837583-v1-Letter\_of\_Intent\_-\_Testing\_Aerial.docx

Major Christian René, CD

Head of Spectrum Engineering DND FSM Eng, DG Cyber FD Canadian Armed Forces

Christian.Rene@forces.gc.ca / Tel: 343-291-3823 / CSN-DSN: nil / TTY: nil

Gestionnaire - ingénierie du spectre GSFM Ing, DG DF Cyber Forces armées canadiennes

Christian.Rene@forces.gc.ca / Tel: 343-291-3823/ CSN-DSN: nil / TTY: nil

From: Souliere, James (IC) [mailto:james.souliere@canada.ca]

Sent: November-15-17 9:11 AM

To: Rene Maj CR@ADM(IM) D Strat CS@Ottawa-Hull < CHRISTIAN.RENE@forces.gc.ca>

Cc: Noel, Sylvain (IC) <sylvain.noel@canada.ca>

Subject: RE: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations

**TELECONFERENCE** 

Hi Christian,

Thank-you for the email. I'm looking forward to diving into this file. I have attached a document that would greatly help us here at DOS with the licence-issuing process. Given that this process (area-based developmental licences) is very new, the attached form is a work-in-progress. Saying that, if we could fill out as many fields as possible, it would give us a great head start. For the fields that cannot be completed, please ignore (or better yet, provide some feedback to us as a user to let us know if the questions are unclear or irrelevant). I annotated some of the sections for you since I have some background already. I am to understand that Bell Canada is a partner and will be allowing use of its existing spectrum for this trial. Will they be operating any element of the service? We will need to know a bit more about Bell's role.

Once we have this information, we can begin drafting the authorization document and creating licence conditions.

Please do not hesitate to contact me at any point.

Thank-you,

James Souliere Tel: 613-854-1979

From: CHRISTIAN.RENE@forces.gc.ca [mailto:CHRISTIAN.RENE@forces.gc.ca]

Sent: November-14-17 4:06 PM

To: Souliere, James (IC) Cc: Noel, Sylvain (IC)

Subject: RE: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations

TELECONFERENCE

Hi James.

My right hand person who normally does the licence legwork for me is away on business trip in Europe for the week, and I am away for the next two days. I would like to ask if you can look at the info in this E-mail and see what info is missing for application of the needed developmental license. I would like to then discuss with you on Friday at a time of your convenience of the steps I need to take.

Many thanks,

Major Christian René, CD

Head of Spectrum Engineering
DND FSM Eng, DG Cyber FD
Canadian Armed Forces
Christian.Rene@forces.gc.ca / Tel: 343-291-3823/ CSN-DSN: nil / TTY: nil

Gestionnaire - ingénierie du spectre
GSFM Ing, DG DF Cyber
Forces armées canadiennes
Christian.Rene@forces.gc.ca / Tel: 343-291-3823/ CSN-DSN: nil / TTY: nil

From: Noel, Sylvain (IC) [mailto:sylvain.noel@canada.ca]

Sent: November-14-17 3:31 PM

To: Rene Maj CR@ADM(IM) D Strat CS@Ottawa-Hull < CHRISTIAN.RENE@forces.gc.ca >

 $\begin{tabular}{l} \textbf{Cc: Lavoie MJ@ADM(IM) D Strat CS@Ottawa-Hull < $$\underline{MARIO.LAVOIE2@forces.gc.ca}$; Kennedy, Caroline (IC) < $$\underline{caroline.kennedy@canada.ca}$; Souliere, James (IC) < $$\underline{james.souliere@canada.ca}$; Lander, Elisabeth (IC) < $$\underline{impacts of the content of th$ 

<elisabeth.lander@canada.ca>; Mulvihill, Matthew (IC) <matthew.mulvihill@canada.ca>

Subject: RE: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations

**TELECONFERENCE** 

Hello Christian,

Thank you for the invite, but DOS will not attend the demonstration.

Besides your agreement with DND will need a developmental licence for the demonstration. It will be the first licence to be issued under our new developmental spectrum licence process. My colleague James Souliere will now be your contact person here in ISED HQ concerning this part of the project (demonstration).

I think the gist of the needed information is covered within the current email thread, but I will let James go through the details with you.

Regards,

Sylvain

From: CHRISTIAN.RENE@forces.qc.ca [mailto:CHRISTIAN.RENE@forces.qc.ca]

Sent: November-14-17 10:49 AM

To: Noel, Sylvain (IC); Kennedy, Caroline (IC)

Cc: MARIO.LAVOIE2@forces.qc.ca

Subject: RE: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations

**TELECONFERENCE** 

Bonjour Caroline et Sylvain,

Je ne sais pas si l'un ou l'autre désirez être présents pour le test décrit ci-bas, surtout si votre présence est nécessaire pour éventuellement approuver l'usage de l'appareil. Il me ferait bien sur plaisir de pouvoir vous accompagner dans cette activité.

Tel que décrit dans les courriels ci-bas, nous avons une fenêtre d'une semaine pour le test, et je ne sais pas à ce point-ci si le test va durer une journée pendant cette fenêtre, ou plusieurs journées. Le Centre National des Recherches est en train de concevoir le test et les détails vont sortir prochainement. Ce qui est certain est que l'avion pour le test est disponible dans ces dates.

Il y a plusieurs gens qui vont y être en particulier des gens de Recherche et Sauvetage qui auront les places prioritaires à bord de l'avion, et nous devons penser qui doit être sur l'avion et qui reste au sol basé sur qui sera là. Nous allons demander à Smith Myers si on peut filmer le test, comme ça on ne sera pas une dizaine de personnes tous empilés autour de l'écran dans le petit avion.

Je n'ai pas le budget d'alloué pour emmener des gens autres que moi et Mario, donc il faut voir si vous avez du budget pour ce voyage.

Petawawa est à une heure et demie de route d'ici le long de la 17, et l'endroit choisi, quoique le long d'un chemin, c'est « un peu dans le clos » comme on dit. Il faudra être habillé pour la température surtout si on est au sol. Une autre question est je ne sais pas à ce point-ci est si l'avion part et revient à Ottawa pour chaque vol (ce qui simplifie le voyagement pour les gens qui témoignent du test dans l'avion), ou si le décollage et l'atterrissage de fait à Petawawa (ce qui forcera tout le monde à être à Petawawa). Si ça dure plus qu'une journée, ceux qui vont à Petawawa devront coucher à l'hôtel étant donné la distance avec Ottawa.

Svp m'aviser si vous voulez/pouvez participer, et si vous avez besoin d'une place à bord de l'avion ou si votre témoignage à partir du sol est suffisant.

Merci bien!

Major Christian René, CD

Head of Spectrum Engineering
DND FSM Eng, DG Cyber FD
Canadian Armed Forces
Christian.Rene@forces.gc.ca / Tel: 343-291-3823/ CSN-DSN: nil / TTY: nil

Gestionnaire - Ingénierie du spectre
GSFM Ing, DG DF Cyber
Forces armées canadiennes
Christian.Rene@forces.gc.ca / Tel: 343-291-3823/ CSN-DSN: nil / TTY: nil

From: Shelden Maj MD@CFAWC@Trenton

Sent: November-11-17 8:34 AM

**To:** 19(1)

Cc:	19(1)	;	sion.jennings@nrc-cnrc.gc.ca;
19(1)	Rene Maj CR@ADM(IM) D Strat CS	@Ottawa-Hull < <u>CHR</u>	ISTIAN.RENE@forces.gc.ca>;
19(1)	sylvain.noel@canada.ca;	19(1)	
iubject: RE: Minutes ( ELECONFERENCE	of the 18 Oct 2017 Digital Receiver Techno	ogy for Domestic Se	arch and Rescue Operations
Good morning Kelly.	Good morning everyone.		
hank you to you and	your team for all of your work and especia	lly to Danick for the	analysis.
appears there is good through the woods in	dle to move forward with the demonstration road access so we can get the simulated so Feb. I will contact Petawawa Range Contr re very interested in supporting and there we	urvivors into positio ol to make the final	n without making them hike arrangements. The army has
RCAF's soon to be acc	is the NRC Falcon 20. Although it is a jet ai quired C295 during its search phase. lation scheduled 29 Jan – 2 Feb scheduled 5 – 9 Feb	rcraft, it can operate	within the flight envelope of the
Eventually I will need field or at NRC.	to know who from Bell will be participatin	g and where they wo	ould like to be; in the aircraft, in the
I'll be in the field on a better. Thanks again.	and off for the next two weeks. Expect an i	ipdate NLT 30 Nov o	nce I have the plan worked out a bi
Mark			
Maj M.D. Shelden			
Royal Canadian Air For	t and Experimentation, Canadian Forces Aerosp ce <u>gc.ca</u> / Tel: 613-392-2811 ext 5614 / CSN 827-5		96
	ncepts et Expérimentation / Centre de guerre a	érospatiale des Forces	canadiennes
Aviation royale canadie Mark.Shelden@forces.	enne <u>gc.ca</u> / Tél: 613-392-2811 poste 5614 / ATS: 82	7-5614 / Facsimile 613	3-965-2096
From:	19(1)		
Sent: November-10-	17 3:47 PM		
To: Shelden Maj MD	@CFAWC@Trenton < Mark. Shelden@force		19(1)
19(1)	; sion.jennings@nrc-cnrc.gc.ca		Rene Maj CR@ADM(IM)
D Strat CS@Ottawa-	Hull < CHRISTIAN.RENE@forces.gc.ca>	19(1)	sylvain.noel@canada.ca;
<b>Subject:</b> RE: Minutes TELECONFERENCE	19(1) s of the 18 Oct 2017 Digital Receiver Technol	ology for Domestic S	earch and Rescue Operations
Good afternoon all,			
The 20(1)(b).21(1)(b) can prearly 2018. Thanks	rovide the following recommendations for specifically to 19(1) who perform		ion to perform the Artemis test in ase note that for now this is a

frequency assignment specific for the testing and does not yet represent an assignment for 'production' use on a national scale with case and participate in the testing given the interaction with our customer devices and network & can provide resources/equipment in the field to perform this testing activity. We are ready to participate in a working team as a next step.

--Best regards,

19(1)

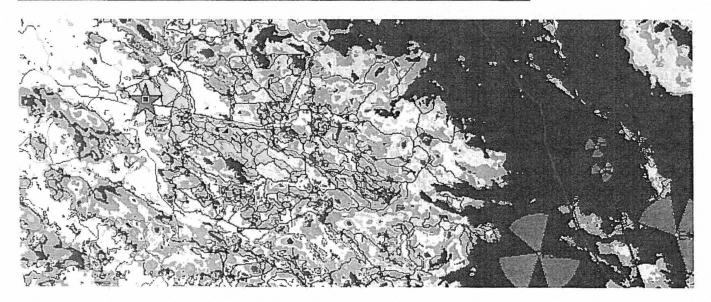
### Frequency/Channel to use:

ARFCN 240 (center freq 891.6 DL and 846.6 UL). This is a 200 KHz channel totally in our expended spectrum at the edge of our B'. As discussed this might not be the final channel we would like them to use, but good enough for testing purposes. This band is not being used now in that region, so no impact to surrounding sites during our test

See below a website that provides center frequencies of ARFCN numbers (we can click on the link and select GSM850):

http://niviuk.free.fr/gsm arfcn.php

### Area to perform the test (Star on simulation represent the area with the dot on the Map):





From: Mark.Shelden@forces.gc.ca [mailto:Mark.Shelden@forces.gc.ca]

Sent: Friday, October 20, 2017 1:29 PM

To:		19(1)		
sion.jennings@nrc-cnrc.gc.ca;	19(1)	CHRISTIAN.RENE@forces.gc.ca;	19(1)	
sylvain noel@canada.ca	10/1)			

Subject: Minutes of the 18 Oct 2017 Digital Receiver Technology for Domestic Search and Rescue Operations TELECONFERENCE

Good afternoon.

Thank you for your participation in subj telecon. I know everyone has busy schedules and I appreciate you taking the time to support this project.

As I said during the teleconference, I am an operator not a technician. Therefore, I would like to thank 19(1) and Christian René for providing the bulk of the technical notes contained in the minutes. However, any errors or omissions are mine alone. If there are any errors which may adversely affect decision making process, please reply all so we can collectively correct it quickly.

After 1600 today, I will be out of the office returning next Fri, 27 Oct. If you need to reach me, my cell number is 19(1)

Thanks again.

Mark.

Maj M.D. Shelden

Concepts Development and Experimentation, Canadian Forces Aerospace Warfare Centre Royal Canadian Air Force

Mark.Shelden@forces.gc.ca / Tel: 613-392-2811 ext 5614 / CSN 827-5614 / Fax 613-965-2096

Développement de Concepts et Expérimentation / Centre de guerre aérospatiale des Forces canadiennes Aviation royale canadienne

Mark.Shelden@forces.gc.ca / Tél: 613-392-2811 poste 5614 / ATS: 827-5614 / Facsimile 613-965-2096

Royal Canadian Mounted Police



Gondamiente rui, als du Cana Le

Outsty Commission Care March Miller Herrich

South of mm sabre was to the public to the p

Protected B

July 25, 2016

Ms. Corinne Charette
Senior Assistant Deputy Minister
Innovation, Science and Economic Development Canada
Spectrum, Information Technologies and Telecommunications
235 Queen Street, Building CD Howe Building, Room 196B
Ottawa, Ontario K1A 0H5

Dêar Ms. Charette,

Re: The Radiocommunication Act and Mobile Devices Identifiers

I am writing concerning the applicability of the *Radiocommunication Act* to the Royal Canadian Mounted Police's (RCMP) use of Mobile Device Identifiers (MDIs), also referred to as International Mobile Subscriber Identity (IMSI) catchers.

By way of background, the RCMP uses MDI technology to assist in criminal investigations relating to national security, serious and organized crime, and other Criminal Code offences that impact the safety and security of Canadians. An MDI is an invaluable law enforcement tool that simulates a cellular tower to attract and collect limited data from mobile devices during an investigation. The RCMP deploys MDI technology in a manner that is consistent with federal laws and judicial oversight requirements. Specifically, absent exigent circumstances, judicial authorization is sought prior to deploying an MDI. Moreover, MDI technology is only deployed in a limited number of priority circumstances where MDI capabilities are best suited to achieve specific public safety objectives. Contrary to recent media coverage, the MDI equipment used by the RCMP does not, and cannot, intercept or receive any form of private communications, including voice and audio communications, text messages, email messages and encryption keys.

The RCMP considers its use of MDI technology to be lawful and consistent with the Radiocommunication Act (Subsection 4(4) and Paragraph 9(1)(b)) Exemption Order, No. 2015-1 which exempts certain RCMP employees from the application of specific provisions of the Act in relation to jammers (insofar as MDI technology is capable of causing limited interference or obstruction to radiocommunications).

That identified, we understand that Innovation, Science and Economic Development Canada (ISED) has been examining whether MDI technology falls within the definition of a "jammer" under the *Radiocommunication Act*, and whether a separate radio authorization may be required to possess and operate an MDI. The RCMP was first made aware of ISED views on the RCMP's use of MDIs through media coverage in late March 2016.

The RCMP is committed to addressing this issue in a timely manner. I am therefore seeking the assistance of ISED to ensure that the RCMP deploys MDI technology in full compliance with the Radiocommunication Act. Furthermore, while the immediate need focuses on MDIs, the RCMP uses other, sensitive investigative techniques that may also warrant further analysis vis-à-vis any potential application to the Radiocommunication Act.

Let me thank you in advance for supporting RCMP efforts to protect Canada and Canadians. Your staff is invited to communicate directly with Superintendent Maury Medjuck, Officer in Charge, Technical Investigation Services Operations at 613-949-8905 or Maury.Medjuck@rcmp-grc.gc.ca.

Sincerely,

Peter Kenychel, Deputy Commissioner

Specialized Policing Services



Innovation, Science and Economic Development Canada

Innovation, Sciences et Développement économique Canada

AUG 12 2016

Mr. Peter Henschel Deputy Commissioner Specialized Policing Services Royal Canadian Mounted Police 273 Leikin Drive Ottawa, Ontario K1A 0R2

Dear Mr. Henschel,

Thank you for your letter of July 25, 2016, seeking our advice on the use of mobile device identifiers (MDIs) in accordance with the requirements of the *Radiocomunication* Act.

We appreciate the importance of ensuring the RCMP has at its disposal the necessary tools, including those involving radiocommunications, to conduct its mandate and ensure the safety and security of Canadians. As such, I have asked Philip Fleming, Director, Spectrum Regulatory Policy, to work with your officials to review the RCMP's requirements and pursue any actions that may be needed in the most expeditious manner.

We look forward to working with you and expect to be able to confirm our advice over the next few months.

Sincerely,

Corinne Charette

Senior Assistant Deputy Minister

c Conte

Spectrum, Information Technologies and Telecommunications

c.c. Phillip Fleming, Director, Spectrum Regulatory Policy, Spectrum, Information Technologies and Telecommunications 604-666-1415 or <a href="mailto:phillip.fleming@canada.ca">phillip.fleming@canada.ca</a>.



# Nolan, Stephen (IC)

From:

Mike Roach <michael.roach@rcmp-grc.gc.ca>

Sent:

November-02-16 11:15 AM

То:

Nolan, Stephen (IC)

Subject:

RE: Follow Up

Attachments:

MDI POLICY Roach edit Oct 17.docx; MDI ISED info.docx

Hi Steve.

I have attached a word doc that has a description of the MDI and how we use it. Let me know if that meets your need. If this is for your internal use, go ahead and use that info. If you are sending it out, please allow us to review it first.

Also, one of your female employees from the legislation side (I have already forgotten names) asked for a copy of our draft policy. I have attached it for her, but it may also supplement the information you are looking for. Again, this is a draft that hasn't been through our legal department, so please do not distribute it outside of your group.

If you need anything further, let me know.

Thanks again for your help on this!

Mike

>>> "Nolan, Stephen (IC)" <<u>stephen.nolan@canada.ca</u>> 2016/10/31 1:07 PM >>> Great, thanks.

From: Mike Roach [mailto:michael.roach@rcmp-qrc.qc.ca]

Sent: October-31-16 12:50 PM

To: Nolan, Stephen (IC) Subject: RE: Follow Up

Ok Steve,

I will look through what we have and find something that fits. Standby...

Mike

>>> "Nolan, Stephen (IC)" <<u>stephen.nolan@canada.ca</u>> 2016/10/31 12:44 PM >>> Hi Mike,

At this point we want to be able to communicate a) what these devices are (e.g. how the RCMP describes/defines them) and how they function and b) some public lines related to the nature of the RCMP's use of the devices.

I hope that helps. Feel free to give me a call if you would like to discuss.

Thanks,

Steve

## Stephen Nolan

Regulatory Officer | Agent de la réglementation Telephone | Téléphone 343-291-3467 Facsimile | Télécopieur 343-291-3526

From: Mike Roach [mailto:michael.roach@rcmp-grc.gc.ca]

Sent: October-31-16 12:22 PM

**To:** Nolan, Stephen (IC) **Subject:** Re: Follow Up

Hi Stephen,

Sorry for the late response, I was out in Calgary last week.

I will likely have something that you can use. What are you looking to communicate?

Mike

>>> "Nolan, Stephen (IC)" <<u>stephen.nolan@canada.ca</u>> 2016/10/25 10:19 AM >>> Good morning Mike,

Thanks again for taking the time to meet with ISED last week.

Following the meeting, you had mentioned the RCMP had put together some communication lines it had used previously in some of its court cases that you were willing to share. Just wondering if it might be possible to obtain a copy of that as well as anything you think might be helpful in our briefings up the line.

Thanks,

## Stephen Nolan

Regulatory Officer | Agent de la réglementation

Spectrum Management Operations Branch | Direction générale des opérations de la gestion du spectre Spectrum, Information Technologies and Telecommunications Sector | Secteur du Spectre, des technologies de l'information et des télécommunications

Innovation, Science and Economic Development Canada | Innovation, Sciences et Développement économique Canada

235 Queen Street, Ottawa ON K1A 0C8 | 235, rue Queen, Ottawa ON K1A 0H5

#### Stephen.Nolan@canada.ca

Telephone | Téléphone 343-291-3467 Facsimile | Télécopieur 343-291-3526 Government of Canada | Gouvernement du Canada OM - Ch. XX.XX Mobile Device Identifier

Directive Amended: 2016-10-17

For information regarding this policy, contact Technical Information Services.

- 1. Definitions
- 2. Policy
- 3. General
- 4. Assistance to Outside Agencies
- 5. Identifying Cellular Devices
- 6. Locating a Specific Cellular Device
- 7. Technical Investigation Services Responsibilities
- 8. Special "I" Unit Commander Responsibilities
- 9. MDI Operator Responsibilities
- 10. Retention
- 11. Disclosure
- 1. Definitions
- 1.1. ESN means Equipment Serial Number
- 1.2. IMEI means International Mobile Equipment Identity
- 1.3. IMSI means International Mobile Subscriber Identity
- 1.4. MDI means Mobile Device Identifier. The MDI is also known as an IMSI catcher. This device, or combination of devices, has two primary functions:
  - 1) To identify the unique identifiers for unknown cellular devices being used by subjects of an investigation.
  - 2) To physically locate a specific cellular device when the unique identifiers are already known.
- 1.5. MDI Data means the transmission data obtained from cellular devices, or data that is derived from the transmission data obtained from cellular devices. MDI data includes unique identifiers, device make and model, and cellular network information. MDI Data does not include private communications or data/information stored on a cellular device. See section 2.2 of this part.
- 1.6. MDI Operator means an employee of the RCMP that has been trained in the operation of the MDI device.
- 1.7. MSID means Mobile Subscriber Identification Number
- 1.8. Personal information is information listed in sec. 3, of the Privacy Act.

Roach Draft 2016-10-17 Page 1 of 5

- 1.9. Private Communication is defined in section 183 of the Criminal Code of Canada.
- 1.10. SIM means subscriber Identity Module
- 1.11. TIS means Technical Investigation Services.
- 1.12. Unique Identifiers are serial numbers that are unique to mobile devices. Unique identifiers include ESN, MSID, IMEI, and IMSI.

#### 2. Policy

- 2.1. The primary role of the Mobile Device Identifier (MOI) is to enhance public safety, by assisting law enforcement agencies in locating specific cellular devices already known to police, as well as in determining the unique identifiers of an unknown cellular device. The MOI will only be deployed in accordance with a valid Judicial Authorization, or by reason of exigent circumstances, where an imminent threat to public safety exists and it would be impracticable to obtain a Judicial Authorization. In addition to a Judicial Authorization, approval is also required from the Officer in Charge of Criminal Operations.
- 2.2. The MDI is not capable of collecting, or intercepting, GPS location information, voice or audio communications, text messages, email messages, contact lists, images, or any other forms of private communications and personal data from a cellular device. The MDI is also not capable of obtaining encryption keys or accessing the GPS location information from a cellular device.
- 2.3. Only the unique identifiers that the MDI operator believes upon reasonable grounds to be associated to the subject of an investigation will be provided to the investigating unit. Any unique identifiers belonging to third parties not involved in the investigation will be withheld from the investigating unit and secured as Protected "B" information.
- 2.4. A Judicial Authorization is required to obtain the subscriber information for any unique identifiers obtained by the MDI.
- 2.5. The information obtained through the use of the MDI is protected information and will only be accessed for the purpose of an investigation, or for court proceedings as ordered by the courts. This information will be stored in a Protected "B" environment during the course of the investigation. The information will be destroyed upon conclusion of the investigation and all court proceedings relating to that investigation, including any appeal periods.

#### 3. General

- 3.1. The Mobile Device Identifier (MDI) functions as a cellular site simulator. Cellular devices in the proximity of the MDI identify the MDI as the most attractive cellular tower in the area and then identify themselves to the MDI using unique identifiers in the same way that they would with a network tower. Once the MDI obtains the unique identifiers for the cellular device, the cellular device returns to its own cellular network.
- 3.2. The MDI will only be deployed by a trained operator in accordance with a valid Judicial Authorization, or in exigent circumstances, and with the approval of the Officer in Charge of Criminal Operations for the division in which the MDI will be deployed.

Comment [RM1]: Do we want delegate? It wasn't there in the past as the authority was moved from tech ops to Crops. We do know they have delegated it in some divisions, but they are accepting risk on behalf of the RCMP.

#### 4. Assistance to Outside Agencies

- 4.1. Approval from the OIC of Criminal Operations and a valid Judicial Authorization is required before the MDI is deployed to assist a non-RCMP agency.
- 4.2. The MDI equipment deployed while assisting a non-RCMP agency will be operated by an RCMP MDI operator and the equipment will not be exposed to the assisted agency.

#### 5. Identifying Cellular Devices

- 5.1. Operators of the MDI will ensure that the MDI is used in accordance with the conditions specified in the Judicial Authorization.
- 5.2. The MDI is deployed to gather the unique identifiers of the cellular devices within its range, or to confirm if the subject of an investigation is using a specific cellular device.
- 5.3. The MDI will only be deployed to confirm that the subject of an investigation is in possession of a specific device when the location of the person is known.
- 5.4. The MDI will only be deployed in an area where there are reasonable grounds to believe that the subject of the investigation is located.
- 5.5. The MDI will only be deployed at as many locations as is necessary to provide the MDI operator with enough information to identify, through a process of elimination, the common unique identifier that belongs to a cellular device believed to be in the possession of a person named in the Judicial Authorization.
- 5.6. The MDI will be activated for no more than three minutes at a time per frequency, with rest periods of at least two minutes between activation on the same frequency.
- 5.7. The only MDI data that will be provided to the investigating unit is the common unique identifier, believed on reasonable grounds, to be in the possession of the subject named in the Judicial Authorization. Any MDI data relating to other third parties that are not subjects of the investigation will be handled and stored as Protected "B" information.

#### 6. Locating a Specific Cellular Device

- 6.1. A tracking warrant is required to locate a specific cellular device, unless there are exigent circumstances that would make it impractical to obtain a warrant.
- 6.2. Operators of the MDI will ensure that the MDI is deployed in accordance with the conditions specified in the Judicial Authorization.
- 6.3. The MDI locating function happens in two stages. In the first stage, the MDI attracts nearby cellular devices to obtain the unique identifiers, so that it can find the targeted cellular device. Once the targeted phone contacts the MDI, the MDI stops attracting other phones and will only affect the targeted phone. The MDI will then provide a direction and estimated distance to the targeted cellular device.

- 6.4. During the first stage, The MDI will be activated for no more than three minutes at a time per frequency, with rest periods of at least two minutes between activation on the same frequency. In the event of exigent circumstances, this step may be omitted if the delay would increase the risk to public safety.
- 6.5. Once the MDI is tracking the targeted cellular device, the MDI can remain activated until such time as the cellular device is located.
- 7. Technical Investigation Services Responsibilities
- 7.1. Developing and maintaining policy and standing operating procedures relating to MDI technology.
- 7.2. Approving the type/make/model and installation of MDI equipment that will be used by the RCMP.
- 7.3. Evaluating the operational effectiveness of MDI systems across Canada.
- 7.4. Conducting research and development on MDI technology.
- 7.5. Provide MDI operator training.
- 7.6. To provide approved template wording for use in Information to obtain documents and warrants.
- 8. Special "I" Unit Commander Responsibilities
- 8.1. Ensure only trained persons operate the MDI equipment.
- 8.2. Ensure all MDI data collected by the MDI is handled and stored as Protected "B" information.
- 9. MDI Operator Responsibilities
- 9.1. Ensure that they are properly trained in the operation of the MDI device.
- 9.2. Maintain the MDI equipment in accordance with manufacturer recommendations and as instructed by Technical Investigation Services.
- 9.3. Ensure that OIC CrOps approval has been obtained and a valid Judicial Authorization exists before the MDI equipment is deployed.
- 9.4. Review the Judicial Authorization to ensure that the wording properly applies to the equipment and techniques being used.
- 9.5. Review the Judicial Authorization to ensure that all conditions within that authorization are followed.
- 9.6. Report any deviations of standardized wording or conditions of operation to Technical Investigation Services.
- 10. Retention
- 10.1. MDI data will be destroyed, in accordance with RCMP policy on the destruction of Protected "B" information, upon the conclusion of the investigation and all related court proceedings, including any appeal periods.

10.2. If an order is made within the Judicial Authorization regarding the storage and/or destruction of the MDI data which is in contradiction to this policy, the order contained within the Judicial Authorization will be followed while respecting RCMP policy for the storage and destruction of data.

#### 11. Disclosure

- 11.1. MDI data will be disclosed as required by the courts.
- 11.2. The MDI data will be vetted by an MDI operator as necessary in order to protect police techniques and the sensitivities of the MDI equipment.
- 11.3. The OIC of Technical Investigation Services, or delegate, will review the disclosure package before it is provided to the courts in order to ensure compliance with disclosure policy.

#### MDI use

The RCMP has different makes and models of MDI equipment, but the way they are used and the type of information obtained from each device is similar. The MDI equipment used by the RCMP does not, and cannot, intercept or receive any form of private communications. This includes voice or audio communications, text messages, email messages, encryption keys, or basic subscriber information.

The RCMP uses the MDI for two specific purposes. The primary use of the MDI equipment is to identify mobile devices that are being used by suspects of criminal investigations. It is understood by the RCMP that the criminal element often uses mobile devices that are not properly registered to them, in an attempt to evade law enforcement and make it more difficult to become known. In these cases, the MDI is deployed in an attempt to identify those devices and link them to those specific suspects. Currently, the RCMP obtains prior judicial authorization to deploy the MDI in this way.

When attempting to identify a suspect's phone, the MDI is operated in proximity of the suspect in several different locations. At each location, the MDI acts like a cellular tower, attracting as many mobile devices in the area as possible to quickly collect unique identifiers, such as the International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI) numbers. After operating in at least three locations, the data is filtered to identify which unique identifiers were in the same locations as the suspect. The unique identifiers that are produced can be eventually associated to the suspect of the investigation. In order to make that association to the suspect, another judicial authorization is used to order a telecommunications service provider to connect a name, address and phone number to the mobile device that was identified through the use of the MDI, which would help corroborate any association between the mobile device and the suspect.

Any MDI data collected on suspects and third parties is maintained so that it can be made available to produce the information during court proceedings. Data on third parties, however, cannot be linked to specific, identifiable persons without a subsequent judicial authorization. Moreover, the RCMP would not seek judicial authorization to obtain identifiable information on third parties as it would not provide any investigative value. Data on third parties is withheld from the investigators, and is only stored for the purposes of providing to a judge if the RCMP is ordered to produce the information during court proceedings. No further action is taken with respect to third party information. The second use of the MDI typically occurs in emergency situations, such as a kidnapping, where a specific phone needs to be located quickly. In this situation, police already know the IMSI and IMEI information associated to that phone. The MDI can be configured to use direction-finding technology and lead the operator to the location of that specific mobile device.

#### MDI data

As previously stated, the MDI equipment used by the RCMP does not, and cannot, intercept or receive any private communications. This includes voice or audio communications, text messages, email messages, encryption keys, or basic subscriber information.

The transmission data that is collected by the MDI that is specific to any mobile device includes the following: service provider for the device; make and model of detected mobile devices; Electronic Serial Number (ESN); Mobile Station Identification (MSID); IMSI and IMEI. The ESN and MSID numbers are specific to older Code Division Multiple Access (CDMA) cellular technology that is in the process of being phased out by network providers. The MDI is rarely used on the CDMA network as it is only older devices that continue to use the CDMA network. In cases where the MDI is used on the CDMA network, the MSID number obtained is often the mobile device's telephone number. The technology for the more current networks that comprise the majority of the MDI deployments does not provide the MSID, and is limited to the IMSI and IMEI.

The IMSI and IMEI numbers are 15 digit serial numbers that are unique to the subscriber and the mobile device. It is not possible, however, to know any identifying information associated to those IMSI and IMEI numbers without performing a "subscriber check" with the network providers. A judicial authorization is obtained to access that subscriber information from the network provider.

The MDI equipment does collect additional information that is specific only to the cellular telephone networks in the area where the MDI is deployed and is not related to any individual person or device. This type of information includes, but is not limited to, frequencies, channels, country codes, and network provider.

#### **Authorities**

The RCMP obtains judicial authorization to deploy the MDI equipment, absent exigent circumstances. Most often, this is in the form of a Transmission Data Recorder Warrant (TDRW) in accordance with section 492.2 of the *Criminal Code*. However, some jurisdictions obtain a General Warrant (section 487.01 of the *Criminal Code*) instead of a TDRW.

Once the MDI identifies the IMSI/IMEI numbers for a mobile device used by the person (suspect) named within the judicial authorization, a production order and/or an assistance order may be obtained to access the identifying information (e.g., name, address, phone number) associated to the IMSI/IMEI numbers to corroborate the mobile device and its association with the suspect.

In situations where exigent circumstances exist, such as in the case of a kidnapping, missing person, imminent murder, or terrorist activities, the RCMP may use an MDI without prior judicial authorization in order to prevent loss of life or grievous bodily harm. MDI deployments of this nature are infrequent and strictly controlled. In these situations and pursuant to judicial processes, the RCMP may subsequently articulate its reasons to a judge for using an MDI under exigent circumstances and without prior judicial authorization. In 2015, the RCMP used an MDI under exigent circumstances in connection with only one operational file.

#### Collection

The transmission data collected by the MDI equipment is temporarily held on a secured computer that is used during the operation of the MDI. This information is accessible only to the operator of the MDI equipment. Only the unique identifiers (such as IMSI/IMEI numbers) that have been linked specifically to a suspect of the investigation that has been named in the judicial authorization are provided to the investigators. The remainder of the transmission data collected, including that of third parties, is withheld from the investigators and is stored in a way that it can be made available if ordered by a judge to produce the information during court proceedings.

#### Other procedures

The MDI equipment does briefly interfere with the use of mobile devices. Most often, the user of a mobile device will not detect any interference. However, there are times when the ability of any person to make a call will be interrupted for a short period of time, typically between 10-15 seconds. This can include the ability to make a 911 call. It is for this reason that the RCMP does not allow the MDI to be deployed without first obtaining approval from the Divisional Criminal Operations Officer. Before approving the use of the MDI, the Criminal Operations Officer will consider the risk of potential interference the MDI may cause against the benefit that the MDI may have on the investigation. It is for this reason that the MDI is only typically deployed in serious criminal investigations. In 2015, the RCMP used an MDI in connection with 24 operational files, and only for priority criminal investigations, such as those linked to national security, serious and organized crime, and financial crime.

Once the use of the MDI is approved by the Criminal Operations Officer, and a judicial authorization has been obtained, the MDI is only operated by specially trained members of the RCMP. These members have specific training in order to operate the equipment safely and in accordance with the judicial authorization. Currently, the RCMP has 32 trained operators for MDI technology, operating a total of seven MDI devices across Canada.

#### Conclusion

The MDI is a sensitive investigative tool used by the RCMP, pursuant to judicial authorization unless there are exigent circumstances, to identify the mobile devices used by a suspect of an investigation. The MDI is not capable of collecting private communications, nor does it conduct mass surveillance. The MDI collects transmission data from the mobile devices within its range, and through a process of elimination, is able to determine which unique serial numbers belong to the suspect of the investigation. These unique serial numbers cannot be attributed to any one person without first obtaining another judicial authorization that orders a telecommunications service provider to provide the subscriber information associated to a particular mobile device.

Ontario Provincial Police Police provinciale de l'Ontario



# OFFICE OF THE BUREAU COMMANDERS COMMANDANTS DE BUREAU

777 Memorial Ave. Orillia, ON L3V 7V3

777, ave. Memorial Orillia, ON L3V 7V3

Tel: 705-329-6325 Fax: 705-329-6318 Tél.: 705-329-6325 Téléc: 705-329-6318

File Reference:

600-00

February 17, 2017

Ms. Corinne Charette
Senior Assistant Deputy Minister
Innovation, Science and Economic Development Canada
Spectrum, Information Technologies and Telecommunications
235 Queen Street, CD Howe Building, Room 196B
Ottawa, Ontario K1A 0H5

Dear Ms. Charette.

### Re: The Radiocommunication Act and Mobile Devices Identifiers

I am writing concerning the applicability of the *Radiocommunication Act* to the Ontario Provincial Police (OPP) use of Mobile Device Identifiers (MDIs), also referred to as International Mobile Subscriber Identity (IMSI) catchers.

The OPP uses MDI technology to assist in criminal investigations relating to national security, serious and organized crime and other Criminal Code offences that impact the safety and security of Ontarians. An MDI is an invaluable law enforcement tool that simulates a cellular tower to attract and collect limited data from mobile devices during an investigation. The OPP deploys MDI technology in a manner that is consistent with federal laws and judicial oversight requirements. Specifically, absent exigent circumstances, judicial authorization is sought prior to deploying an MDI. MDI technology is only deployed in a limited number of priority circumstances where MDI capabilities are best suited to achieve specific public safety objectives. Contrary to recent media coverage, the MDI function of the OPP's device does not intercept or receive any form of private communications, including voice and audio communications, text messages, email messages and encryption keys.

We understand that Innovation, Science and Economic Development Canada (ISED) has been examining whether MDI technology falls within the definition of a "jammer" under the *Radiocommunication Act* and whether a separate radio authorization may be required to possess and operate an MDI. The OPP was first made aware of ISED views on the RCMP's use of MDIs through media coverage in late March 2016.

The Radiocommunication Act and Mobile Devices Identifiers Page two

I am seeking the assistance of ISED to ensure that the OPP deploys its MDI technology in full compliance with the *Radiocommunication Act*. Furthermore, while the immediate need focusses on MDIs, the OPP uses other sensitive investigative techniques that may also warrant further analysis vis- $\dot{\alpha}$ -vis any potential application to the *Radiocommunication Act*.

The OPP is requesting an authorization issued under section 5(1)(a)(v) of the Radiocommunication Act for employees of the Technical Support Branch, as well as employees of the OPP who fall under the direction of that Branch. This authorization applies only to the installation, operation and possession of radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain data associated with a mobile device or the mobile network that, as per section 492.2(6) of the Criminal Code:

- (a) relates to the telecommunication functions of dialing, routing, addressing or signalling;
- (b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2) of the *Criminal Code*, in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and
- (c) does not reveal the substance, meaning or purpose of the communication.

Thank you in advance for supporting our efforts to protect Canadians. Your staff is invited to communicate directly with Detective Inspector Robert Longstreet, Officer In Charge, Technical Support Branch at (705) 329-6492 or <a href="mailto:robert.longstreet@opp.ca">robert.longstreet@opp.ca</a>.

Sincerely.

J.E. (John) Tod Chief Superintendent Bureau Commander

Investigation & Support Bureau

Innovation, Sciences et Développement économique Canada

Our File: 46081700382

# APR 0 6 2017

Mr. J.E. (John) Tod Chief Superintendent Bureau Commander Investigation & Support Bureau Ontario Provincial Police 777 Memorial Avenue Orillia, Ontario L3V 7V3

Mr. Tod,

This letter constitutes an authorization issued under section 5(1)(a)(v) of the Radiocommunication Act, for employees of the Ontario Provincial Police (OPP) Technical Support Branch, as well as employees of the OPP who fall under the direction of that Branch. This authorization applies only to the installation, operation and possession of radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain data associated with a mobile device or the mobile network that, as per section 492.2 of the Criminal Code:

- (a) relates to the telecommunication functions of dialing, routing, addressing or signalling;
- (b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2) of the Criminal Code, in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and
- (c) does not reveal the substance, meaning or purpose of the communication.



This authorization is subject to the attached terms and conditions, and expires five years from the day it is signed. In particular, these radio apparatus may be installed, operated or possessed only in accordance with the purposes under section 54 of the *Radiocommunication Regulations*.

Yours Sincerely,

Peter Hill

Director General

Spectrum Management Operations Branch

Attachment

## **Attachment**

### **Terms and Conditions**

- 1. The authorization applies only to employees of the Ontario Provincial Police (OPP) Technical Support Branch, as well as employees of the OPP who fall under the direction of that Branch, and is limited to the installation, operation and possession of radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain data associated with a mobile device or the mobile network that, as per section 492.2 of the Criminal Code:
  - (a) relates to the telecommunication functions of dialing, routing, addressing or signalling;
  - (b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2) of the Criminal Code, in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and
  - (c) does not reveal the substance, meaning or purpose of the communication.
- 2. All employees of the OPP installing, operating and possessing these radio apparatus must be appropriately trained.
- 3. Every reasonable effort shall be made to localize, confine or restrict, to the extent possible, interference and obstruction to radiocommunication.
- 4. The radio apparatus must be turned off and stored in a secure location when not in use, including when being transported.
- 5. Every reasonable effort shall be made to ensure that the installation and operation of these radio apparatus complies with Safety Code 6 (Limits of Human Exposure to Radiofrequency Electromagnetic Fields in the Frequency Range from 3 kHz to 300 GHz) at all times, including the consideration of combined effects of nearby installations within the local radio environment.

- 6. The authorization to install, operate and possess these radio apparatus applies only for the purposes under section 54 of the *Radiocommunication Regulations*, restated as follows:
  - (a) preserving or protecting any property, or the prevention of serious harm to any person, including the bringing of emergency assistance to any person,
  - (b) giving evidence in any criminal or civil proceeding or in any other proceeding in which the persons may be required to give evidence on oath,
  - (c) investigation or prosecution of an alleged contravention of any law of Canada or a province or in the interests of the administration of justice,
  - (d) international affairs or national defence or security.

# Nolan, Stephen (IC)

From:

Pichette, Laura (IC) on behalf of Hill2, Peter (IC)

Sent:

March-13-17 3:34 PM

To:

peter.henschel@rcmp-grc.gc.ca

Cc:

Hill2, Peter (IC)

Subject:

Letter regarding MDIs

Attachments:

2017-03-13 RCMP P. Henschel.pdf

#### Good afternoon

Please find attached a letter regarding the use of radio apparatus which communicates with mobile devices.

Sincerely,

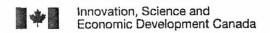
#### Peter Hill

Director General, Spectrum Management Operations I Directeur general, Opérations de la gestion du spectre Spectrum Management Operations Branch I Direction générale des operations de la gestion du spectre Spectrum, Information Technologies and Telecommunications Sector I Secteur du Spectre, des technologies de l'information et des télécommunications

Innovation, Science and Economic Development Canada | Innovation, Sciences et Développement économique Canada 235 Queen Street, Ottawa ON K1A 0H5l 235, rue Queen, Ottawa, ON K1A 0H5

Telephone I Téléphone 343-291-3462

Government of Canada I Gouvernement du Canada



Innovation, Sciences et Développement économique Canada

Our File: 49081700428

# MAR 1 3 2017

Mr. Peter Henschel Deputy Commissioner Specialized Policing Services Royal Canadian Mounted Police 273 Leikin Drive Ottawa, Ontario K1A 0R2

Mr. Henschel,

This letter constitutes an authorization issued under section 5(1)(a)(v) of the Radiocommunication Act, for employees of the Royal Canadian Mounted Police (RCMP) Technical Investigation Services Branch, as well as employees of the RCMP who fall under the direction of that Branch. This authorization applies only to the installation, operation and possession of radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain data associated with a mobile device or the mobile network that, as per section 492.2 of the Criminal Code:

- (a) relates to the telecommunication functions of dialing, routing, addressing or signalling;
- (b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2) of the Criminal Code, in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and
- (c) does not reveal the substance, meaning or purpose of the communication.



This authorization is subject to the attached terms and conditions, and expires five years from the day it is signed. In particular, these radio apparatus may be installed, operated or possessed only in accordance with the purposes under section 54 of the *Radiocommunication Regulations*.

Yours Sincerely,

Peter Hill

Director General

Spectrum Management Operations Branch

Attachment

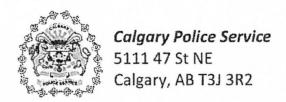
## Attachment

## **Terms and Conditions**

- 1. The authorization applies only to employees of the Royal Canadian Mounted Police (RCMP) Technical Investigation Services Branch, as well as employees of the RCMP who fall under the direction of that Branch, and is limited to the installation, operation and possession of radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain data associated with a mobile device or the mobile network that, as per section 492.2 of the Criminal Code:
  - (a) relates to the telecommunication functions of dialing, routing, addressing or signalling;
  - (b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2) of the Criminal Code, in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and
  - (c) does not reveal the substance, meaning or purpose of the communication.
- 2. All employees of the RCMP installing, operating and possessing these radio apparatus must be appropriately trained.
- 3. Every reasonable effort shall be made to localize, confine or restrict, to the extent possible, interference and obstruction to radiocommunication.
- 4. The radio apparatus must be turned off and stored in a secure location when not in use, including when being transported.
- 5. Every reasonable effort shall be made to ensure that the installation and operation of these radio apparatus complies with Safety Code 6 (*Limits of Human Exposure to Radiofrequency Electromagnetic Fields in the Frequency Range from 3 kHz to 300 GHz*) at all times, including the consideration of combined effects of nearby installations within the local radio environment.
- 6. The authorization to install, operate and possess these radio apparatus applies only for the purposes under section 54 of the *Radiocommunication Regulations*, restated as follows:

- a. preserving or protecting any property, or the prevention of serious harm to any person, including the bringing of emergency assistance to any person,
- b. giving evidence in any criminal or civil proceeding or in any other proceeding in which the persons may be required to give evidence on oath,
- c. investigation or prosecution of an alleged contravention of any law of Canada or a province or in the interests of the administration of justice,
- d. international affairs or national defence or security.

Nolan, Stephen (IC)			
From:	Scott Campbell	19(1)	
Sent:	April-06-17 4:41 PM		
To:	Jensen, Amy (IC)	i'an	
Subject: Attachments:	request for authorizat		ft_MDI_AuthorizationCPS.docx
Attachments.	170400 CF3 request r	or authorization.pui, bra	TC_MOX_Addition2adon_=_CF3.docx
Good afternoon Amy,			
i i i i i i i i i i i i i i i i i i i	authorization under the R	Radiocommunication Act	my Inspector has asked that I make an . There is some urgency to try to get this
Please find attached a letter service	with the official request. I 13(1)(d)	have also attached a dra	aft authorization for Calgary Police
I provided your name to for the same authorization.	19(1) and I understand	d he was also going to be	contacting you on behalf of his agency
Thanks,			
Scott			
Sgt. Scott Campbell #3356			
Calgary Police Service			
13(1)(d),19(1)			



Amy Jensen A/Manager, Spectrum Management Operations Branch Innovation, Science and Economic Development Canada

Dear Amy,

Please accept this letter as an official request for the Calgary Police Service to obtain an authorization under section 5(1)(a)(v) of the *Radiocommunication Act* to install, operate and possess radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain transmission data, as defined in section 487.011 of the Criminal Code, associated with a mobile device or the mobile network.

The Calgary Police Service also possesses this equipment and therefore is seeking the same authorization. We will provide ISED access to the equipment or supporting documentation as required. As previously discussed 13(1)(d) and therefore if your ISED technicians have examined their equipment and are satisfied that this equipment, either the specific make/model or the type of equipment in general, meets the definition of a radio apparatus potentially there will be no need for an actually examination of ours.					
Please contact me for any further information t	hat is required.				
Sincerely,					
Sgt. Scott Campbell #3356 Calgary Police Service					
13(1)(d),19(1)					

Cc: Insp. Ryan Jepson, TOS S/Sgt. Mark Rahn, TIS

## Draft - For Discussion Purposes Only

Date#

File # ########

Mr. Paul Cook
Deputy Chief
Bureau of Investigative Support
Calgary Police Service
5111 47 St NE
Calgary, Alberta T3J 3R2

Mr. Cook.

This letter constitutes an authorization for employees of the Calgary Police Service (CPS), issued under section 5(1)(a)(v) of the *Radiocommunication Act*, to install, operate and possess radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain transmission data, as defined in section 487.011 of the *Criminal Code*, associated with a mobile device or the mobile network.

This authorization is subject to the attached terms and conditions, and expires five years from the day it is signed. In particular, these radio apparatus may be installed, operated or possessed only in accordance with the purposes under section 54 of the *Radiocommunication Regulations*.

This authorization will be published on the Innovation, Science and Economic Development Canada website.

Yours Sincerely,

Peter Hill
Director General
Spectrum Management Operations Branch

Attachment

#### **Draft - For Discussion Purposes Only**

#### **Attachment**

#### **Terms and Conditions**

- The authorization applies only to employees of the Calgary Police Service Technical
  Operations Section, as well as other employees of the Calgary Police Service who fall
  under the direction of that Section and, is limited to the installation, operation and
  possession of radio apparatus designed to communicate with mobile devices on
  commercial mobile networks to obtain transmission data, as defined in s.487.011 of the
  Criminal Code, associated with a mobile device or the mobile network.
- 2. All employees of the CPS installing, operating and possessing these radio apparatus must be appropriately trained.
- 3. Every reasonable effort shall be made to localize, confine or restrict, to the extent possible, interference and obstruction to radiocommunication.
- 4. The radio apparatus must be turned off and stored in a secure location when not in use, including when being transported.
- 5. Every reasonable effort shall be made to ensure that the installation and operation of these radio apparatus complies with Safety Code 6 (*Limits of Human Exposure to Radiofrequency Electromagnetic Fields in the Frequency Range from 3 kHz to 300 GHz*) at all times, including the consideration of combined effects of nearby installations within the local radio environment.
- 6. The authorization to install, operate and possess these radio apparatus applies only for the purposes under section 54 of the *Radiocommunication Regulations*, restated as follows:
  - preserving or protecting any property, or the prevention of serious harm to any person, including the bringing of emergency assistance to any person,
  - b. giving evidence in any criminal or civil proceeding or in any other proceeding in which the persons may be required to give evidence on oath,
  - c. investigation or prosecution of an alleged contravention of any law of Canada or a province or in the interests of the administration of justice,
  - d. international affairs or national defence or security.

## Nolan, Stephen (IC)

From:

Ketler, Trevor

19(1)

Sent:

April-13-17 1:49 PM

To:

Jensen, Amy (IC)

Cc:

Ketler, Trevor; Conway, Jeff

Subject:

Official Request

Attachments:

Scanned Request from Chief.pdf

Hi Amy,

This email is a follow up to our phone conversation on Friday, April 7.

Please find the attached request for exemption under the Radiocommunication Act.

Best Regards,



#### **Trevor Ketler**

Sergeant, Technical Surveillance Unit Division 42, Winnipeg Police Service

City of Winnipeg

Phone:

Mobile: 19(1)

Email:

Website: winnipeg.ca

Address: P.O. Box 1680, Winnipeg, MB R3C 0R6





Connect with us:





CONFIDENTIALITY NOTICE: The information contained in this message is intended solely for the person or entity to which it is addressed and may contain confidential and/or privileged information. Any use, dissemination, distribution, copying or disclosure of this message and attachments, in whole or in part, by anyone other than the intended recipient is strictly prohibited. If you have received this message in error, please notify the sender and permanently delete the complete message and any attachments. Thank you.



# Winnipeg Police Service • Service de police de Winnipeg

"A Culture of Safety for All" « Cultiver la sécurité pour tous »

April 10, 2017

Ms. Amy Jensen A/Manager, Spectrum Management Operations Branch Innovation, Science and Economic Development Canada

Dear Ms. Jensen,

I understand that the RCMP have obtained an authorization under section 5(1)(a)(v) of the Radiocommunication Act to install, operate and possess radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain transmission data, as defined in section 487.011 of the Criminal Code, associated with a mobile device or the mobile network.

I am advised that this authorization was granted after an examination of their equipment by ISED technicians and that a determination was made that the equipment was a radio apparatus as defined in the act.

The Winnipeg Police Service also possesses this equipment and is also seeking an authorization. We will provide ISED access to the equipment or supporting documentation as required, however since we have the same equipment as the RCMP, I anticipate that there is potentially no need for an actual examination of ours.

I understand that Sgt. Trevor Ketler has contacted you. Please contact him at 19(1) if further information is required.

19(1)

or

Sincerely,

Danny Smyth Chief of Police

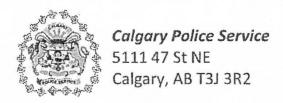
An Internationally Accredited
Law Enforcement Agency
Organisms d'application de la

loi reconnu internationalement

P.O. Box 1680 Winnipeg, Manitoba R3C 2Z7 Bus; 204-986-6037 Fax; 204-986-6077
 B.P. 1680 Winnipeg, Manitoba R3C 2Z7 Trav; 204-986-6037 Téléc; 204-986-6077
 www.winnipeg.ca/police







Amy Jensen
A/Manager, Spectrum Management Operations Branch
Innovation, Science and Economic Development Canada

Dear Amy,

Please accept this letter as an official request for the Calgary Police Service to obtain an authorization under section 5(1)(a)(v) of the *Radiocommunication Act* to install, operate and possess radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain transmission data, as defined in section 487.011 of the Criminal Code, associated with a mobile device or the mobile network

network.		
	13(1)(d)	
The Calgary Police Service also possesses this equauthorization. We will provide ISED access to the As previously discussed, 13(1)(d) have examined their equipment and are satisfied the type of equipment in general, meets the defineed for an actually examination of ours.	equipment or supporting documentation and therefore if your IS that this equipment, either the specific	ion as required. ED technicians c make/model or
I have attached a draft copy of an authorization there are any changes that are required.	13(1)(d)	Please advise if
Please contact me for any further information that	at is required.	
Sincerely,		
Sgt. Scott Campbell #3356 Calgary Police Service		
13(1)(d),19(1)		

Cc: Insp. Ryan Jepson, TOS S/Sgt. Mark Rahn, TIS



Sgt. Scott Campbell #3356
Calgary Police Service
Technical Operations Section
Electronic Surveillance Team
scampbell@calgarypolice.ca
19(1)

July 12, 2017

To: Amy Jensen

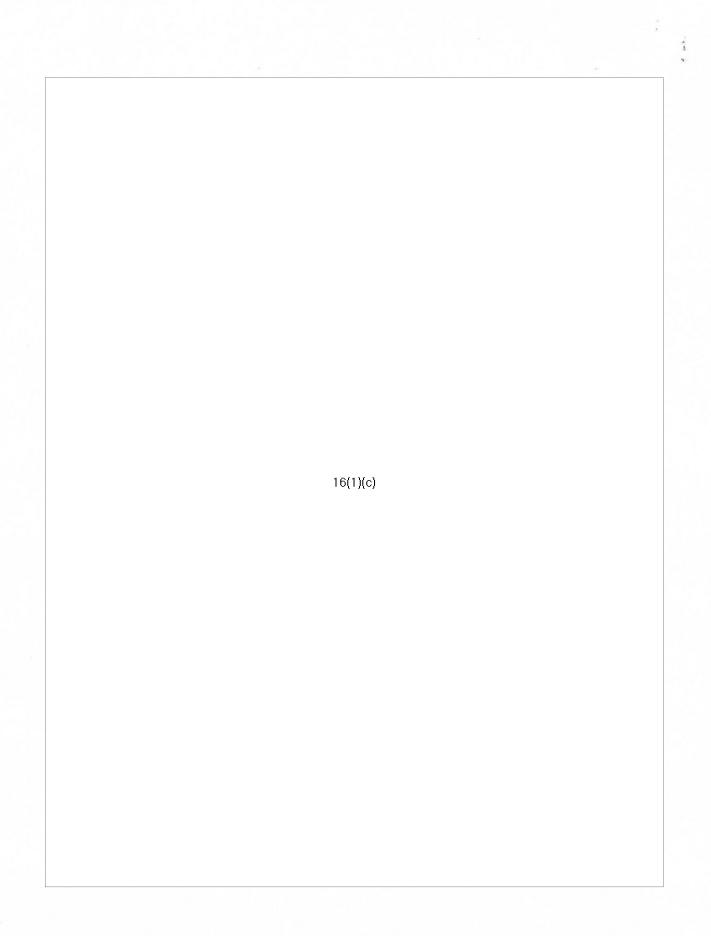
A/Manager, Spectrum Management Operations Branch Innovation, Science and Economic Development Canada (ISED)

RE: Calgary Police Service Radiocommunications Act Authorization

In support of the Calgary Police Service (CPS) request for an authorization under s. 5(1)(a)(v) of the *Radiocommunication* Act, please find below information regarding the CPS radio apparatus.

This information is submitted in confidence to ISED and contains confidential information that is the property of the Calgary Police Service. This information is protected from disclosure pursuant to sections 16(1) and 20(1) of the <u>Freedom of Information and Protection of Privacy Act</u> as well as pursuant to sections 13(1)(d) and 20(1) of the <u>Access to Information Act</u>. This information is not to be disclosed outside of ISED except with express written permission of the Chief of the Calgary Police Service. Any request for access to this record must be transferred to the Calgary Police Service for response pursuant to section 8(1) of the <u>Access to Information Act</u>.

ithorization:	ormation sp	ecific to the device for which	on we are seeking a
		16(1)(c)	



	16(1)(c)	

Sgt. Scott Campbell Calgary Police Service



nnovation, Sciences et Economic Development Canada Développement économique Canada

AUG 1 8 2017

Sgt. Scott Campbell Calgary Police Service **Technical Operations Section** 5111 47 Street NE Calgary, Alberta T3J 3R2

Sgt. Campbell,

This letter constitutes an authorization issued under section 5(1)(a)(v) of the Radiocommunication Act, for members of the Electronic Surveillance Team of the Calgary Police Service's Technical Operations Section. This authorization applies only to the installation, operation and possession of radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain data associated with mobile devices or the mobile network that, as per section 492.2 of the Criminal Code:

- (a) relates to the telecommunication functions of dialing, routing, addressing or
- (b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2) of the Criminal Code, in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and
- (c) does not reveal the substance, meaning or purposes of the communication.

This authorization is subject to the attached terms and conditions, and expires five years from the day it is signed. In particular, these radio apparatus may be installed, operated or possessed only in accordance with the purposes under section 54 of the *Radiocommunication Regulations*.

Sincerely,

Lynne Fancy

**Director General** 

Spectrum Management Operations Branch

Attachment

#### Attachment

#### **Terms and Conditions**

- 1. The authorization applies only to members of the Electronic Surveillance Team of the Calgary Police Service's (CPS) Technical Operations Section, and is limited to the installation, operation and possession of radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain data associated with mobile devices or the mobile device network that, as per section 492.2 of the Criminal Code:
  - (a) relates to the telecommunication functions of dialing, routing, addressing or signalling;
  - (b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2) of the *Criminal Code*, in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and
  - (c) does not reveal the substance, meaning or purposes of the communication.
- 2. All members of the CPS Electronic Surveillance Team installing, operating and possessing these radio apparatus must be appropriately trained.
- 3. Every reasonable effort shall be made to localize, confine or restrict, to the extent possible, interference and obstruction to radiocommunication.
- 4. The radio apparatus must be turned off and stored in a secure location when not in use, including when being transported.
- 5. Every reasonable effort shall be made to ensure that the installation and operation of these radio apparatus complies with Safety Code 6 (*Limits of Human Exposure to Radiofrequency Electromagnetic Fields in the Frequency Ranger from 3KHz to 300 GHz*) at all times, including the consideration of combined effects of nearby installations within the local radio environment.

- 6. The authorization to install, operate and possess these radio apparatus applies only for the purposes under section 54 of the *Radiocommunication Regulations*, restated as follows:
  - (a) Preserving or protecting any property, or the prevention of serious harm to any person, including the bringing of emergency assistance to any person;
  - (b) Giving evidence in any criminal or civil proceeding or in any other proceeding in which the persons may be required to give evidence on oath;
  - (c) Investigation or prosecution of an alleged contravention of any law of Canada or a province or in the interests of the administration of justice; and
  - (d) International affairs or national defence or security.

Innovation, Science and

nnovation, Sciences et Economic Development Canada Développement économique Canada

AHG	4	0	7	01	7
Allia	-1	n	- /	88 Es	ŧ.

19(1) Sergeant Winnipeg Police Service Technical Surveillance Unit 245 Smith Street Winnipeg, Manitoba R3C 1K1

19(1) Sqt.

This letter constitutes an authorization issued under section 5(1)(a)(v) of the Radiocommunication Act, for members of the Winnipeg Police Service's Technical Surveillance Unit. This authorization applies only to the installation, operation and possession of radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain data associated with mobile devices or the mobile network that, as per section 492.2 of the Criminal Code:

- (a) relates to the telecommunication functions of dialing, routing, addressing or signalling;
- (b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2) of the Criminal Code, in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and
- (c) does not reveal the substance, meaning or purposes of the communication.

This authorization is subject to the attached terms and conditions, and expires five years from the day it is signed. In particular, these radio apparatus may be installed, operated or possessed only in accordance with the purposes under section 54 of the *Radiocommunication Regulations*.

Sincerely,

Lynne Fandy

Director General

1140 1

Spectrum Management Operations Branch

Attachment

## Attachment

#### **Terms and Conditions**

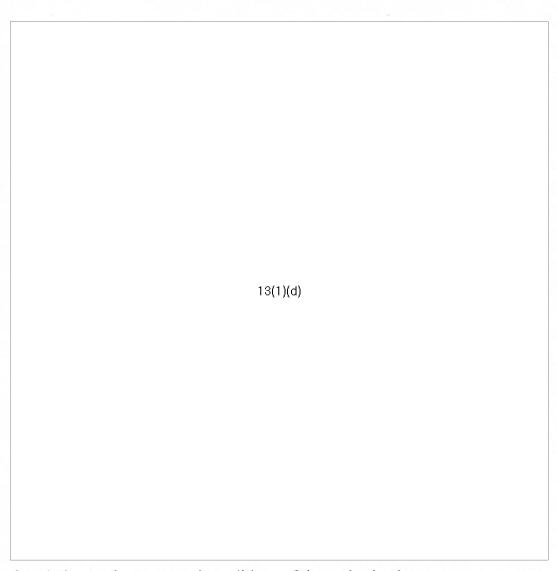
- 1. The authorization applies only to members of the Technical Surveillance Unit of the Winnipeg Police Service (WPS), and is limited to the installation, operation and possession of radio apparatus designed to communicate with mobile devices on commercial mobile networks to obtain data associated with mobile devices or the mobile device network that, as per section 492.2 of the Criminal Code:
  - (a) relates to the telecommunication functions of dialing, routing, addressing or signalling;
  - (b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2) of the *Criminal Code*, in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and
  - (c) does not reveal the substance, meaning or purposes of the communication.
- All members of the WPS Technical Surveillance Unit installing, operating and possessing these radio apparatus must be appropriately trained.
- 3. Every reasonable effort shall be made to localize, confine or restrict, to the extent possible, interference and obstruction to radiocommunication.
- 4. The radio apparatus must be turned off and stored in a secure location when not in use, including when being transported.
- 5. Every reasonable effort shall be made to ensure that the installation and operation of these radio apparatus complies with Safety Code 6 (*Limits of Human Exposure to Radiofrequency Electromagnetic Fields in the Frequency Ranger from 3KHz to 300 GHz*) at all times, including the consideration of combined effects of nearby installations within the local radio environment.
- 6. The authorization to install, operate and possess these radio apparatus applies only for the purposes under section 54 of the *Radiocommunication Regulations*, restated as follows:
  - (a) Preserving or protecting any property, or the prevention of serious harm to any person, including the bringing of emergency assistance to any person;

- (b) Giving evidence in any criminal or civil proceeding or in any other proceeding in which the persons may be required to give evidence on oath;
- (c) Investigation or prosecution of an alleged contravention of any law of Canada or a province or in the interests of the administration of justice; and
- (d) International affairs or national defence or security.



# Winnipeg Police Service

	willing ronce service	
TO:	Amy Jensen A/Manager, Spectrum Management Operations Branch Innovation, Science and Economic Development (ISED	
FROM:	Sergeant Trevor Ketler  Technical Surveillance Unit, Winnipeg Police Service  19(1) (O) 19(1) (M) 19(1)	
DATE:	July 6, 2017	
RE:	Authorization pursuant to Radiocommunication Act	
Developinforma authoria Winnip For use the Can	cument is provided to Innovation, Science and Economent Canada (ISED) in confidence. It contains sention and is not to be disclosed outside of ISED unlegation is first obtained from or on behalf of the Chineg Police Service.  Strictly in compliance with section 13(1)(d) and second addian Access to Information Act. Not to be disclosed to Information request.	ess written of Police,
Overvie	ew of the device we are seeking authorization for:	
	13(1)(d)	



In relation to the terms and conditions of the authorization:

# 1. Organization - who is being authorized (which section)?

 The authorization is being sought by the Winnipeg Police Service, Technical Surveillance Unit (TSU). Only members of TSU are trained and authorized by the Winnipeg Police Service to operate the device.

# 2. Training framework

• Members of TSU responsible for operating the apparatus complete

30 hours of training in its operation by the manufacturer 13(1)(d)

13(1)(d)

#### 13(1)(d)

- Additional training and is based on updates from the manufacturer.
- Operators routinely communicate with subject matter experts from other police agencies.

# 3. Policies and procedures to limit the reach of the device (and minimize interference to the extent possible)

The deployment and operation of the device is regulated by the
judicial authorization that has been obtained in relation to an
investigation. Time limits for operation of the device on specific
frequencies are included in the authorization. The purpose of these
time limits is to minimize interference to mobile devices within
range of the device. In addition, operators use the minimum power
settings necessary in order to obtain results.

# 4. Storage and security

• The device it secured by members of TSU and is not accessible to any other members of the Winnipeg Police Service. The device is stored in a locked vehicle within a secure facility belonging to the Winnipeg Police Service when not in use.

# 5. Any procedures or tests completed to comply with Safety Code 6

- Operators are trained to utilize the minimum power settings required in order to achieve the objectives
- Operators are aware of the surroundings while operating the
  equipment and should persons be in close range of the device for
  any period of time the equipment will not be activated or will be
  shut down to minimize exposure.

Respectfully,	
Sergeant Trevo Winnipeg Police	

#### Noel, Sylvain (IC)

From:

STS DGSO / DGOGS SST (IC)

Sent:

October-13-17 1:11 PM

To:

Parsons2, Eric (IC); Kennedy, Caroline (IC)

Cc:

Fancy, Lynne (IC); STS DGSO / DGOGS SST (IC)

Subject:

FW: For ADM approval - FW: Media Request: 19(1) / G&M / IMSI catchers -

prison officials / ASAP

Hi,

Approved by ADM with changes - please see Candace's note below.

Thanks, Rula

From: STS ADM Office / Bureau SMA SST (IC)

Sent: October-13-17 12:45 PM
To: STS DGSO / DGOGS SST (IC)

Cc: Gilfillan, Fiona (IC); STS ADM Office / Bureau SMA SST (IC)

Subject: RE: For ADM approval - FW: Media Request: 19(1) / G&M / IMSI catchers - prison officials / ASAP

Good afternoon,

Below is the ADM approved response. Changes tracked.

I don't have the originator, so can you please send back to CMB.

Thanks,

Candace

#### **Proposed Response**

ISED regularly works with public safety and law enforcement agencies, including CSC, regularly to ensure they continue to meet requirements under the *Radiocommunication Act*. Once the OPP concluded the investigation, OPP they shared with ISED that there had been unauthorized use of an device but that this unauthorized use had ceased. ISED's objective behind compliance activities is to establish and maintain regulatory compliance for the benefit of all Canadians. Given that the incident of non-compliance had already been resolved through the course of the investigation by the OPP, ISED concluded that no further action was required.

From: STS DGSO / DGOGS SST (IC) Sent: October-12-17 1:20 PM

To: STS ADM Office / Bureau SMA SST (IC)

Subject: For ADM approval - FW: Media Request: 19(1) / G&M / IMSI catchers - prison officials / ASAP

Good afternoon,

For ADM approval.

Please see the DG approved response below.

Thank you, Simone

From: Fancy, Lynne (IC) Sent: October-12-17 12:31 PM

To: Parsons2, Eric (IC)

Cc: Kennedy, Caroline (IC); STS DGSO / DGOGS SST (IC)

Subject: RE: Media Request: 19(1) G&M / IMSI catchers - prison officials / ASAP

Approved. Thanks.

Lynne

From: Parsons2, Eric (IC) Sent: October-12-17 10:40 AM

To: Fancy, Lynne (IC)

Cc: Kennedy, Caroline (IC); STS DGSO / DGOGS SST (IC)

Subject: RE: Media Request: 19(1) / G&M / IMSI catchers - prison officials / ASAP

Hi Lynne,

Please see proposed answer to all 3 questions. Also attached is the response from CSC for reference. CMB is looking for ADMO approval by 3PM today.

#### **Proposed Response**

ISED works with public safety and law enforcement agencies, including CSC, regularly to ensure they continue to meet requirements under the *Radiocommunication Act*. Once the OPP concluded the investigation, OPP shared with ISED that there had been unauthorized use of an device but that this unauthorized use had ceased. ISED's objective behind compliance activities is to establish and maintain regulatory compliance for the benefit of all Canadians. Given that the incident of non-compliance had already been resolved through the course of the investigation by the OPP, ISED concluded that no further action was required.

Regards, Eric & Caroline

MEDIA: 19(1) , G&M -- 19(1)

TOPIC: IMSI catchers / usage by federal prison officials

REQUEST:

Almost two years ago, federal prison officials fell under criticism and criminal investigation for warrantlessly using an IMSI catcher.

- Q1. I'm wondering whether these same officials ever fell under investigation for contravention of the RadioCommunication Act -- specifically 4(1) and/or 9(1)(b) and/or any analogous clauses.
- Q2. Can ISED say whether it has launched an investigation into this matter? If so, can it say when it was launched?
- Q3. On Aug 2, ISED was explicitly invited by the OPP to do its departmental duty and consider enforcing the law that it is specifically tasked with enforcing. How did ISED respond?

Published | Publié: 2017-10-11 Received | Reçu: 2017-10-11 02:34 (EST) Globe and Mail News, Page: A11

# Security concerns rise as police suspect cell tower 'intercepted' personal data

#### Colin Freeze

Police have determined that a device that functioned as a **cellphone tower** has "likely unlawfully intercepted" private text messages from unsuspecting bystanders.

This pronouncement highlights the growing capabilities of, and legal problems posed by, portable surveillance devices that target **cellphone** data. The findings centre on federal correctional officials who launched a surveillance effort that aimed to locate inmates' contraband phones in an Ontario prison, but which also ended up intercepting several text messages sent by jail guards.

Legal and privacy observers say this determination of unlawfulness likely amounts to the first known police allegation of such a device violating **Canada's** Criminal Code. Yet, no one is poised to face any charges. In August, authorities closed the case after concluding they would be unlikely to win any prosecution, according to a memo obtained by The Globe and Mail.

The finding by the police probe comes as surveillance gadgets variously known as **Stingrays**, cell-site simulators, or **IMSI catchers** are growing more capable, and spawning fears about whether criminals are now using them to dredge data from the smartphones of the wider public.

Government officials are facing questions about whether they are able to police such activity, or even be trusted to use such devices themselves.

As first reported by The Globe, the Ontario Provincial Police (OPP) in 2015 launched a criminal investigation into the Correctional Service of Canada's (CSC) surveillance activities, and whether they broke Canada's laws against warrantless wiretapping. The internal OPP memo lays out the findings of the investigation.

On Aug. 3, OPP Detective Inspector Gerry Scherer wrote to correctional officials that he was closing the prison-surveillance case with no charges. His memo recaps how the Warkworth Institution, near Peterborough, hired a contractor who had access to powerful **cellphone**-spotting technology as the prison struggled to keep phones out of the hands of inmates. Det. Insp.

Scherer wrote that the contractor's particular device was "capable of intercepting the SMS text messages of any mobile devices operating within its operational range."

Wiretapping laws make it a crime for anyone to intercept private messages without prior judicial permission. Prison authorities never got such approval. Senior CSC officials pulled the plug on the investigation after four months upon learning the machine had intercepted jail guards' communications.

Det. Insp. Scherer's memo says the probe only found evidence that six text messages had been intercepted. No explanation is given as to why the device only sporadically intercepted the texts.

Detectives seized a laptop that had been used by the prison-surveillance team and found records revealing the phone-tracking machine had been switched on "at least" 2,200 times over the four-month period. There was a possibility that "some sessions may have been deleted," Det.

Insp. Scherer wrote, referring to periods of active surveillance.

But the detective also said it looked to him that, for almost all the time it was running, the device captured only data such as **IMSI** numbers. Such unique digital identifiers are associated with every **cellphone** and can be used to help discern a phone's location, but reveal nothing about who is using a phone or what they are saying on it.

Evidence gathered by police suggested the contractor "appears to have acted independently" in terms of any intercepted texts, according to the OPP memo. But police were not able to draw conclusions about whether he could be considered solely responsible for all, or even most, of the unlawful intercepts.

Given this, Det. Insp. Scherer wrote his conclusion: "Should charges in relation to the unlawful interception be laid, there would not be a reasonable prospect of conviction. As a result the OPP will not proceed with the laying of charges at this time."

The OPP confirmed to The Globe on Monday what was communicated in the Aug. 3 memo.

"Criminal charges will not be laid in this matter," Staff Sergeant Carolle Dionne said.

Several **Canadian** legal and privacy experts contacted by The Globe said they knew of no similar cases. However, in the spring, Public Safety Minister Ralph Goodale announced he has tasked federal agents with investigating **IMSI catcher** use in Ottawa. This followed a **CBC** report that found unlawful surveillance was likely taking place in the capital after a reporting team moved through the city with a device supposedly capable of spotting **IMSI catcher** activity.

Meantime, the Office of the Privacy Commissioner of Canada has resumed its own probe into the surveillance at Warkworth Institute. "It had been put on hold as we awaited the completion of a related investigation by the Ontario Provincial Police," spokeswoman **Tobi Cohen** said.

A spokesman for the federal prison authority stressed police never found evidence that any of its own officials engaged in misconduct. "The OPP investigation concluded that a civilian contractor may have unlawfully intercepted a small number of text messages," the Correctional Service of Canada's Avely Serin said.

Previously disclosed material obtained by The Globe shows that the civilian contractor was Peter Steeves, a Quebec-based surveillance specialist who imported a device from Florida and who sold his services for \$10,000. Contacted by The Globe, he said he was just happy to hear the criminal investigation had closed.

BY: COLIN FREEZE AND MATTHEW BRAGA

TORONTO MARCH 24, 2017 Federal prison authorities are under criminal investigation for possible illegal surveillance, The Globe and Mail has learned. The probe centres on Correctional Service Canada's use of a dragnet surveillance device inside a penitentiary.

Fallout from the 2015 surveillance incident, involving a device that CSC officials called a "cellular grabber," has led to a lawsuit from jail guards and a criminal inquiry by the Ontario Provincial Police.

Under the Criminal Code, indiscriminate surveillance campaigns can be deemed crimes that merit prison sentences. Federal security officials do not get blanket exemptions, even if they themselves work to manage prisons.

The case at hand started with a desire to locate prisoners' contraband cellphones, but ended up with a warden apologizing to his own staff for inadvertently spying on them.

The make and model of the device in question are being withheld from the public, which generally is familiar with such machines by names such as "Stingrays," "cell-site simulators" or "IMSI catchers."

"IMSI catchers are not localized. It would get anything that's in range and won't discriminate," explained Tamir Israel, a lawyer at the Canadian Internet Policy and Public Interest Clinic.

On Monday, The Globe and Mail reported on the <u>RCMP's courtroom bid</u> to keep its use of a similar device secret.

In the winter of 2015, officials at Warkworth Institution, a medium-security prison in Ontario, grew alarmed by prisoner drug overdoses. On Jan. 20, one CSC official sent an internal e-mail, according to federal court documents related to the civil suit, saying "there are phones all over the institution and this is how they are organizing the introduction of contraband."

Officials in Ottawa, records show, put out a request for an outsider who could perform "surveys of radio traffic" to "confirm the presence of cellular phones inside institutions." The winning contractor, according to federal court documents, was a Quebec-based engineer named Peter Steeves, who said he could do the job for \$7,500 in fees, plus \$2,000 in travel expenses.

Contacted Monday by The Globe and Mail, Mr. Steeves said he is no expert in the legalities of interception. "I'm just a guy trying to make a living — I really don't know the law," he said. Asked about the police probe, he said, "I know I have to go for an interview. I have been told it's a criminal investigation."

Access to information records show that last April, a device was shipped to CSC from Florida. Details are mostly being withheld, but it weighed 38 kilograms and its manufacturer was a Britain-based surveillance-machinery firm, Smith Myers.

The "pilot program" at the Warkworth Institution started rolling out in the late spring. By August, CSC officials arranged an internal meeting to review the "cellular grabber to better understand its capacity," according to an e-mail now filed in court. Officials wanted to know "how to force" a phone to communicate its specific location, or how to list phones on a map of the prison.

Before long, CSC officials began asking for even more specifics – such as how to figure out whether phones were sending texts or calls. On Sept. 3, one official asked for the "total activities of cellular devices from inmates, staff ..."

Prison guards learned of the program, and pushed back. "How does this device bend a radio signal ... to eliminate the inclusion of staff areas?" one guard asked in an e-mail to his bosses.

By the end of September, Warkworth's warden, Scott Thompson, sent an apologetic e-mail to all staff, according to access to information records. "Unfortunately, I knew that by trying to intercept what the inmates were doing, I would also be provided information about cellular devices being used in non-inmate areas," his e-mail said. The warden relayed that the device "provides make, phone numbers and sim-card numbers" and, also, "recorded all voice and text conversations."

With that, he assured his jail guards that any of their inadvertently captured communications wouldn't be used against them. "I am sorry if this information causes stress to any of you," he said. Some CSC e-mails contradict the warden, stating explicitly that the device did not capture any conversations beyond three text messages intercepted in a bid used to showcase its capabilities. (On Monday, the contractor, Mr. Steeves, told The Globe that the device "does not capture voice at all.") At the end of October, the Union of Canadian Correctional Officers took their bosses to court. In a lawsuit, they complained their their privacy rights had been violated – and that CSC had spied upon them.

"Look – we're all about getting the contraband out. We're in. If there's technology to do that, we're there," explained Jason Godin, a union vice-president in an interview. "But, God damn it," he said, "... you can't spy on private conversations of staff members."

Mr. Israel suggests that the correctional officials who acquired the device were likely operating in a legal vacuum.

"Because no agency to my mind has openly acknowledged to using these in court, no court has provided guidance as to what the [legal] authorities should be," he said. Some federal officials, he added, "may be under the impression they can just deploy these IMSI catchers without any authorization at all."

CSC officials have recently stopped giving statements to lawyers pursuing the civil suit. According to Federal Court filings, that's because they have become worried to have learned there is now also a criminal probe.

"The Ontario Provincial Police is currently conducting a criminal investigation into the monitoring of cellphones at Warkworth Institution," reads a motion filed earlier this month. Because OPP detectives are now interviewing CSC officials, the latter "have significant concerns about providing affidavits while an investigation is under way."

Spokespersons for the OPP and CSC won't comment on the specifics of the investigation. Correctional officials originally defended their use of the device by saying they had "authority to monitor and intercept communications to ensure the security of institutions." But they have stopped saying this now that they face civil and criminal investigations for alleged unlawful surveillance of jail guards.

Court filed e-mails show that, in the end, CSC seized only three contraband cellphones smuggled into Warkworth.

With a report from Laura Stone in Ottawa

## Noel, Sylvain (IC)

From:

Noel, Sylvain (IC)

Sent:

November-06-17 2:42 PM 'Veronika.Friel@rcmp-grc.gc.ca'

To:

Kennedy, Caroline (IC); Todhunter, Travis (IC); Certification Bureau / Bureau

homologation (IC)

Subject:

RE: RCMP Question re: IMSI Catchers

Categories:

Catégorie bleue

Hello,

I am a college of Travis and I carry on the processing of your information request. Thank you for the additional information you have provided. We apologize for the delay in responding.

Radio apparatus distributors in Canada are affected by <u>standards</u> and <u>certification</u>. The preceding hyperlinks will provide you information. We suggest you contact the <u>Certification and Engineering Bureau</u>, should you need additional information.

Regard,

#### Sylvain Noel

Technical Policy Analyst, Spectrum Management Operations Branch Innovation, Science and Economic Development Canada / Government of Canada <a href="mailto:sylvain.noel@ic.gc.ca">sylvain.noel@ic.gc.ca</a> / Tel: 343-291-3588 / TTY: 1-866-694-8389

Analyste de politiques techniques, Direction générale des opérations de la gestion du spectre Innovation, Sciences et Développement économique Canada / Gouvernement du Canada sylvain.noel@ic.gc.ca / Tél: 343-291-3588 / ATS: 1-866-694-8389

From: Veronika Friel [mailto:Veronika.Friel@rcmp-grc.gc.ca]

Sent: Monday, October 02, 2017 12:03 PM

To: Todhunter, Travis (IC)

**Cc:** Kennedy, Caroline (IC); Ryan Horn **Subject:** RE: Licensing questions

Hi Travis.

Thank you for your detailed response.

I feel like I should clarify the situation in which we are seeking answers from ISED. We are specifically dealing with IMSI catchers.

The situation: A private company who is a distributor of various Law Enforcement products in Canada is looking to sell, possess and demonstrate an IMSI device. They mistakenly sent a request to us to obtain a license under s.191 of the CC. but IMSI catchers appear to fall under the RA. RCMP is **ONLY** looking to provide them information on how to proceed with selling their IMSI catchers to Law Enforcement agencies/government entities. What is the process to do that? Who could they contact at ISED?

Please feel free to contact me for further information,
Thank you,
Veronika
Veronika Friel Policy Analyst/Analyste des politiques Technical Investigation Services/Services d'enquêtes techniques Technical Operations/Les opérations techniques Royal Canadian Mounted Police / Gendarmerie Royale du Canada Tel: 613-949-9507 Fax: 613-993-6872 >>> "Todhunter, Travis (IC)" < travis.todhunter@canada.ca> 2017/09/29 3:16 PM >>> Hi Veronika,
Caroline Kennedy asked me to get in touch with you concerning a number of questions that you had sent to us earlier this week. In order to address your questions, there are a number of things we need to first clarify. I will provide these follow-up questions at the bottom of this email.
I'd first like to point out that jammers and IMSI catchers are entirely separate devices that cannot be referred to interchangeably. With this being the case, we would need to know whether you are asking specifically about jammers or about IMSI catchers in order to address your first question, in addition to the other follow-up questions presented below.
With respect to your second question concerning a list of companies with exemptions, please note that the Minister has not issued an exemption order for commercial activities and so no such list exists.
Finally, with regards to your third question on licensing for manufacturers, please note that the <i>Radiocommunication Act</i> does not provide for a scheme to issue licences to manufacturers.
If you have any outstanding questions relating to the manufacture of either IMSI catchers or jammers, we would need to consult with our colleagues in the Engineering Planning and Standards Branch. Please let us know whether this is necessary.
I regret that the answer to your first question is not straightforward. Looking forward to hearing from you soon.
Best,
Travis
Follow-up Questions

1. When referring to a "jammer (IMSI catcher)," are you referring to a jammer or an IMSI-catcher? These two terms are not interchangeable.

- 2. When referring to private companies making inquiries, are you referring to a manufacturer of jammers and/or IMSI-catchers?
- 3. When referring to s. 191 of the Criminal Code and the assignment of Special and Regular Licenses to private companies in order for them to possess, sale or purchase intercept communication devices pursuant to this provision, are you looking to provide an exemption under subsection 191(2) of the Criminal Code or are you looking to either provide an exemption or authorization, as the case may be, under the Radiocommunication Act?
- a. If so, and if ISED were to provide either an exemption or authorization, as the case may be, would this enable you to provide an exemption under paragraph 191(2)(b) of the Criminal Code?
- b. If you aren't looking to provide an exemption or authorization under the *Radiocommunication Act*, are you simply looking to forward requests for an exemption or authorization, as the case may be, directly to ISED?
- 4. In reading s. 191 of the *Criminal Code*, it seems that it covers devices whose primary purpose is to surreptitiously intercept private communications. If you are contemplating jammers and not IMSI-catchers, would the jamming functionality fall within the definition of interception of private communications under the *Criminal Code*?
- 5. What is the purpose of s. 191 of the *Criminal Code* in relation to ISED? Is it that your authorization under this provision is contingent upon ISED providing an exemption or authorization, as the case may be, under the *Radiocommunication Act* and corresponding Regulations?
- 6. In question 3, you referred to "a licence." Can you please clarify? Are you looking to provide an exemption to sell jammers? How does a licence differ from an exemption that you mentioned in question 1?

From: Veronika Friel < Veronika. Friel@rcmp-grc.gc.ca>

Sent: Tuesday, September 26, 2017 8:59 AM

To: Kennedy, Caroline (IC)

Cc: Ryan Horn

Subject: Licensing questions

Good day Caroline,

I was given your contact information from Troy Glassel at the RCMP. I am the RCMP analyst currently responsible for assigning Special and Regular Licenses to private companies in order for them to possess, sale

or purchase intercept communication devices (electro-magnetic, acoustic, mechanical or other device), under the 191 of the CC.

I have a few questions that would need your expertise. Please see below.

- 1) In order to approve their applications for a license, the private companies sends us a list of their devices in order for us to do a background check on them. If we realize that one of their devices constitute a "jammer" (IMSI catcher), we will refuse their request to sell, possess or demonstrate this type of device. Therefore, I would like to propose to them that it is possible to obtain an exemption to "install, use, possess, manufacture or import a jammer" without violating the jammer prohibitions in the RA (Under the amended RA, a new prohibition was added under s. 4(4), which states, "No person shall install, use, possess, manufacture, import, distribute, lease, offer for sale or sell a jammer"). How would they go about to obtaining such an exemption? Would you be the contact person to give them such information?
- 2) Would ISED have a list of companies that already have this type of exemption? Would RCMP be able to acquire this list for future reference when private companies requests licenses?
- 3) Do private companies need to obtain a license before manufacturing their device? or is it only when the device is built that they would need one?

Thank you for your time,

Veronika

#### Veronika Friel

Policy Analyst/Analyste des politiques
Technical Investigation Services/Services d'enquêtes techniques
Technical Operations/Les opérations techniques
Royal Canadian Mounted Police / Gendarmerie Royale du Canada
Tel: 613-949-9507

Fax: 613-949-9507

#### Noel, Sylvain (IC)

From:

Kennedy, Caroline (IC)

Sent:

November-30-17 6:19 PM

To:

Noel, Sylvain (IC); Thiessen, Joanne (IC); Todhunter, Travis (IC); Agi, Ojo (IC)

Cc:

Corbin, Marc (IC); Parsons2, Eric (IC)

Subject:

Fw: Federal Court decision wrt IMSI-Grabber // Federal Court decisions released on IMSI

and BII matters

Follow Up Flag:

Follow up

Flag Status:

Completed

Interesting read!

From: Jensen, Amy (IC) <amy.jensen@canada.ca> Sent: Thursday, November 30, 2017 3:58 PM

To: Kennedy, Caroline (IC)

Subject: FW: Federal Court decision wrt IMSI-Grabber // Federal Court decisions released on IMSI and BII matters

From: Nolan, Stephen (IC) Sent: November-29-17 10:14 AM

To: Jensen, Amy (IC); Fleming, Philip (IC)

Subject: Fw: Federal Court decision wrt IMSI-Grabber // Federal Court decisions released on IMSI and BII matters

Fyi

From: Robichaud, Guy (IC) < <u>guy.robichaud@canada.ca</u>>

Sent: Wednesday, November 29, 2017 10:04 AM

To: Nolan, Stephen (IC)

Subject: TR: Federal Court decision wrt IMSI-Grabber // Federal Court decisions released on IMSI and BII matters

FYI - related news article

# TELECOMMUNICATIONS / TÉLÉCOMMUNICATIONS

#### CSIS legally captures phone data: ruling

Canada's domestic spy service has been capturing the phone-identifying data of terrorism suspects for years without judicial knowledge or oversight, according to a ruling released Tuesday. But the Canadian Security Intelligence Service's warrantless use of data-capturing devices is legal and proper in most instances, the ruling says, as long as the agency restricts what it does with captured information. The decision from Federal Court Chief Justice Paul Crampton relates to CSIS warrant applications for an "Islamist terrorism" investigation, although the identities of the target individuals are being withheld. It amounts to the most detailed ruling to date by any Canadian court on government agents' use of devices known as IMSI catchers, "Stingrays," or "cell-site simulator" (CSS) technology.

G&M

De: Robichaud, Guy (IC)

Envoyé: 28 novembre 2017 11:12

À: Nolan, Stephen (IC)

Objet: TR: Federal Court decision wrt IMSI-Grabber // Federal Court decisions released on IMSI and BII matters

Good morning Stephen,

You will find the decisions at the following links:

http://cas-cdc-www02.cas-satj.gc.ca/rss/CONF-2-17%20-%20Public%20Judgment%20and%20Reasons%20ENG.pdf

http://cas-cdc-www02.cas-satj.gc.ca/rss/CONF-3-17%20-%20Public%20Judgment%20and%20Reasons%20ENG.pdf

A summary was also issued by the Court at: <a href="http://cas-cdc-www02.cas-satj.gc.ca/rss/Media%20Bulletin%20nov-28-2018%20FINAL%20">http://cas-cdc-www02.cas-satj.gc.ca/rss/Media%20Bulletin%20nov-28-2018%20FINAL%20</a>(web%20English).pdf

Thank you,

Guy Robichaud

Legal Counsel, ISED Legal Innovation, Sciences and Economic Development Canada / Government of Canada guy.robichaud@canada.ca / Tel: 343-291-2244 / TTY: 1-866-694-8389

Avocat, Services juridiques d'ISDE Innovations, Sciences et Développement économique Canada / Governement du Canada guy.robichaud@canada.ca / Tél: 343-291-2244 / ATS: 1-866-694-8389

De: Robichaud, Guy (IC)

Envoyé: 27 novembre 2017 10:13

A: Nolan, Stephen (IC)

Objet: Federal Court decision wrt IMSI-Grabber

Bonjour Stephen,

ATI, nous anticipons que la décision de la Cour fédérale sur les émulateurs de station de base (« IMSI-Grabbing »), dont nous avons déjà discuté, sera probablement rendue publique aujourd'hui.

Je vous informerai, lorsque j'aurai reçu confirmation que la décision a effectivement été rendue, et le lien à la décision de la Cour lorsque je l'aurai.

Guy Robichaud

Legal Counsel, ISED Legal Innovation, Science and Economic Development Canada / Government of Canada guy.robichaud@canada.ca / Tel: 343-291-2244 / TTY: 1-866-694-8389

Avocat, Services juridiques d'ISDE Innovations, Sciences et Développement économique Canada / Governement du Canada guy.robichaud@canada.ca / Tél: 343-291-2244 / ATS: 1-866-694-8389

Solicitor-Client Privilege - Not to be circulated

#### Secret professionnel de l'avocat - Ne pas distribuer

This message, and the documents attached hereto, are intended only for the addressee and may contain privileged or confidential information, including information subject to solicitor-client privilege. Any unauthorized disclosure may be unlawful and is strictly prohibited. If you have received this message in error, please notify us immediately. Please then delete the original message and the documents attached thereto. Thank you.

Le présent message et les documents qui y sont joints sont destinés exclusivement au destinataire indiqué et leur teneur peut être confidentielle ou privilégiée. Il est strictement interdit à quiconque d'en prendre connaissance, de les utiliser ou de les divulger. Si vous recevez le present message par erreur, veuillez nous en aviser immédiatement et le détruire, ainsi que les documents qui y sont joints. Merci.

#### **AGENDA**

# Discussion – WPS ability to meet terms and conditions of the Authorization:

- 1. Organization who is being authorized (which section)?
- 2. Training framework
- **3.** Policies and procedures to limit the reach of the device (and minimize interference to the extent possible)
- 4. Storage and security
- 5. Any procedures or tests completed to comply with Safety Code 6

ANNEX A DRAFT

# Public Safety Radiocommunication Requirements

## **KEY MESSAGES**

#### **GENERAL**

- Police and other similar entities in Canada use a diverse range of radiocommunication tools in criminal investigations and other activities related to public safety and national security.
- Innovation, Science and Economic Development (ISED) Canada continues to work with these entities to ensure their use of radio tools complies with the Radiocommunication Act.
- These requirements are designed to ensure the safe use of radio devices in Canada and to minimize interference with other legitimate radiocommunications.

#### RCMP AUTHORIZATION

- ISED has authorized the RCMP to use radio devices, referred to as mobile device identifiers or more commonly, "IMSI catchers" or Stingrays, designed to capture device identifier data on commercial mobile networks.
- ISED recognizes that these kinds of radio devices are important tools for public safety communities.
- This authorization limits the RCMP to capture device identification data of individual mobile devices.
- This authorization does not exempt the RCMP from the requirement to obtain judicial warrants when using these devices in criminal investigations.
- ISED inspectors may exercise their authorities under the Radiocommunication Act at
  any time to verify compliance with the terms and conditions of this authorization.

#### **Public Safety Radiocommunication Requirements**

- ISED intends to authorize the RCMP to use radio devices that capture mobile user device
  identifiers. These devices are called by many names including International Mobile Subscriber
  Identity (IMSI) catchers, Mobile Device Identifiers (MDIs) and cell-site simulators, as well as
  StingRays, a commercial brand name.
- Under the *Radiocommunication Act*, these radio devices must be authorized by ISED before they can be used in Canada.

#### BACKGROUND

- In July 2016, ISED received a letter from the RCMP seeking to ensure its use of these devices complies with the *Radiocommunication Act*. The letter noted the RCMP uses these devices only in a manner fully consistent with other federal laws and judicial oversight requirements.
- These devices can capture International Mobile Equipment Identity (IMEI) and International
  Mobile Subscriber Identity (IMSI) numbers, the unique identifiers of cell phones being used in an
  area. The devices capture basic information from nearby cellphones and other connected
  devices, such as pagers and smart tablets. Police use this information as part of criminal
  investigations.
- The devices being used by the RCMP are not capable of intercepting the content of private communications such as voice calls, text messages and e-mail. They are capable only of capturing identifier information.
- The Radiocommunication Regulations allow the interception and use of radiocommunications
  for purposes related to law enforcement and public safety. However, under the
  Radiocommunication Act, radio devices, such as these, must be authorized by ISED for use in
  Canada. An authorization is required for any such radio device, whether it is receive-only or
  send-and-receive.

#### CONSIDERATIONS

These devices are not jammers, which fully obstruct or impede wireless communications in an
area. Therefore, while the RCMP's use of jammers is exempt from prohibitions in the Act under
the Ministerial Exemption Order, their use of these identifier devices is not.

- ISED has prepared a special authorization that will permit the RCMP to use these devices in Canada.
- This authorization includes conditions the RCMP must meet to ensure the safe operation of these devices and minimize interference with other legitimate radiocommunications.
- This authorization does not permit the RCMP to use these devices to intercept private communications.
- The RCMP is not exempt from requirements to obtain judicial warrants when using these devices in criminal investigations, unless an emergency situation exists, e.g. AMBER Alert.
- The RCMP is engaging wireless telecommunication service providers in Canada through the Canadian Association of Chiefs of Police on the use of these devices.

#### **NEXT STEPS**

- The special authorization will be signed by the Director General, Spectrum Management
  Operations Branch (DGSO), and transmitted to the RCMP. It will expire five years from the day it
  is signed.
- ISED does not publish special authorizations. In anticipation of media enquiries on this subject,
   SITT has prepared key messages for possible media enquiries.
- Additional police forces across Canada may in the future request similar authorizations for the
  use of these devices. ISED will subject each request to similar due diligence processes before
  determining whether to issue an authorization.

#### **Ontario Provincial Police Radiocommunication Requirements**

- ISED intends to authorize the Ontario Provincial Police (OPP) to use radio devices that capture
  mobile device identifiers such as International Mobile Equipment Identity (IMEI) and
  International Mobile Subscriber Identity (IMSI) numbers, the unique identifiers of cell phones
  being used in an area. These devices are called by many names including IMSI catchers, Mobile
  Device Identifiers (MDIs) and cell-site simulators, as well as StingRays, a commercial brand
  name.
- Under the *Radiocommunication Act*, these radio devices must be authorized by ISED before they can be used in Canada.
- ISED has previously issued a similar authorization to the RCMP for these types of devices.

#### **BACKGROUND**

- In February 2017, ISED received a letter from the OPP seeking to ensure its use of these devices
  complies with the Radiocommunication Act. The letter noted the OPP uses these devices only in
  a manner fully consistent with other laws and judicial oversight requirements.
- Further to this letter, ISED officials met with employees of the OPP Technical Support Branch in March 2017, where it was shown that:
  - These devices can capture only IMEI and IMSI numbers. The devices capture basic information from nearby cellphones and other connected devices, such as pagers and smart tablets. Police use this information as part of criminal investigations.
  - o The devices being used by the OPP are not capable of intercepting the content of private communications such as voice calls, text messages and e-mail. They are capable only of capturing identifier information.
- The Radiocommunication Regulations allow the interception and use of radiocommunications for purposes related to law enforcement and public safety. However, under the Radiocommunication Act, radio devices, such as these, must be authorized by ISED for use in Canada. An authorization is required for any such radio device, whether it is receive-only or send-and-receive.

#### CONSIDERATIONS

- ISED has prepared a special authorization that will permit the OPP to use these devices.
- This authorization, similar to that which was issued to the RCMP, includes conditions the OPP must meet to ensure the safe operation of these devices and minimize interference with other

legitimate radiocommunications.

- This authorization does not permit the OPP to use these devices to intercept private communications.
- The OPP is not exempt from requirements to obtain judicial warrants when using these devices in criminal investigations, unless an emergency situation exists, e.g. AMBER Alert.

#### **NEXT STEPS**

- The special authorization will be signed by the Director General, Spectrum Management
  Operations Branch (DGSO), and transmitted to the OPP. It will expire five years from the day it
  is signed.
- ISED does not publish special authorizations. In anticipation of media enquiries on this subject, SITT in coordination with CMB will prepapre key messages for possible media enquiries.
- As mentioned previously, additional police forces across Canada may in the future request similar authorizations for the use of similar devices. ISED will subject each request to similar due diligence processes before determining whether to issue an authorization.

DRAFT

Mr. J.E. (John) Tod Chief Superintendent Bureau Commander Investigation & Support Bureau Ontario Provincial Police 77 Memorial Avenue Orillia, Ontario L3V 7V3

Dear Mr. Tod,

Thank you for your letter of February 17, 2017, seeking our assistance on the use of mobile device identifier (MDI) technology in accordance with the requirements of the *Radiocommunication Act*.

ISED appreciates the importance of ensuring the OPP has at its disposal the necessary tools, including those involving radiocommunications, to conduct its mandate and ensure the safety and security of Ontarians. As such, I have asked Amy Jensen, A/Manager, Spectrum Regulatory Policy, to work with your officials to review the OPP's requirements in order to assess the required course of action.

We look forward to working with you and your Investigation & Support Bureau colleagues.

Sincerely,

Corinne Charette
Senior Assistant Deputy Minister
Spectrum, Information Technologies and Telecommunications

c.c. Amy Jensen, A/Manager, Spectrum Regulatory Policy, Spectrum, Information Technologies and Telecommunications 613-291-4807 or amy.jensen@canada.ca.

# Items to check with applicants for IMSI catcher special authorizations

- System overview diagram;
  - o Especially: Is there a jamming capability as part of the system?
- · Key technical parameters:
  - o Equipment make(s) and model(s)
  - o RF Output Power (dBm)
  - o Antenna gain (dBi)
  - o Type of traffic that will be carried
  - Frequency band(s)
  - o RF Bandwidth (MHz)
- Minimal but sufficient information on how your operations will meet one or many paragraph(s)
   of subsection 54(2) of the <u>Radiocommunication Regulations</u>, restated as follows:
  - preserving or protecting any property, or the prevention of serious harm to any person,
     including the bringing of emergency assistance to any person;
  - o giving evidence in any criminal or civil proceeding;
  - o for the purpose of the investigation or prosecution of an alleged contravention of any law of Canada or a province or in the interests of the administration of justice; or
  - o for the purposes of international affairs or national defence or security.
- Broad outline of the training management with regard to installing, operating and possessing the radio apparatus in question;
- Broad outline of your approach with regard to localizing, confining or restricting interference and obstruction to radiocommunication;
- Broad outline of your storing and transporting management with regard to the radio apparatus
   in question; and

EDRMS #794767

- Your approach with regard to Safety Code 6 compliance (<u>Limits of Human Exposure to</u>
   Radiofrequency Electromagnetic Energy in the Frequency Range from 3 kHz to 300 GHz).
  - It should be noted that the installation and operation of the radio apparatus in question will have to comply with Safety Code 6 at all times, including the consideration of combined effects of nearby installations within the local radio environment.
  - o Technical reference: <u>GL-01 Guidelines for the Measurement of Radio Frequency</u> <u>Fields at Frequencies From 3 kHz to 300 GHz.</u>