SCC Court Files No.: **35298**

IN THE SUPREME COURT OF CANADA
(ON APPEAL FROM THE COURT OF APPEAL FOR ONTARIO)

BETWEEN:

KEVIN FEARON

APPELLANT
(Appellant)

- and -

HER MAJESTY THE QUEEN

RESPONDENT
(Respondent)

- and -

ATTORNEY GENERAL OF ALBERTA, ATTORNEY GENERAL OF QUEBEC, BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION, CANADIAN ASSOCIATION OF CHIEFS OF POLICE, CANADIAN CIVIL LIBERTIES ASSOCIATION, CRIMINAL LAWYERS' ASSOCIATION, CRIMINAL TRIAL LAWYERS' ASSOCIATION, DIRECTOR OF PUBLIC PROSECUTIONS OF CANADA, AND SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC

INTERVENERS

FACTUM OF THE INTERVENER SAMUELSON-GLUSHKO CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law, CML
57 Louis Pasteur Street
Ottawa, ON, K1N 6N5

Tamir Israel
Tel: (613) 562-5800 ext. 2914
Fax: (613) 562-5417
Email: tisrael@cippic.ca

Counsel for the Intervener

TO: **THE REGISTRAR OF THE SUPREME COURT OF CANADA**

COPY TO:

Sam Goldstein
880 Broadview Avenue
Toronto, ON, M4K 2R1

Sam Goldstein
Shelley Flam

Tel: (416) 927-1211
Fax: (416) 960-4671
Email: sam@samgoldstein.ca

Counsel for the Appellant, Kevin Fearon

Supreme Advocacy LLP
#100-340 Gilmour Street
Ottawa, ON, K2P 0R3

Marie-France Major

Tel: (613) 695-8855 x102
Fax: (613) 695-8855
Email: mfmajor@supremeadvocacy.ca

Agent for the Appellant, Kevin Fearon

AND TO:

Attorney General of Ontario
720 Bay Street, 10th Floor
Toronto, ON, M5G 2K1

Randy Schwartz

Tel: (416) 326-4586
Fax: (416) 326-4656
Email: randy.schwartz@ontario.ca

Counsel for the Respondent, Her Majesty the Queen

Burke-Robertson LLP
Suite 200, 441 MacLaren Street
Ottawa, ON, K2P 2H3

Robert E. Houston, Q.C.

Tel: (613) 236-9665
Fax: (613) 235-4430
Email: rhouston@burkerobertson.com

Agent for the Respondent, Her Majesty the Queen

AND TO:

Attorney General of Alberta
Alberta Justice, Criminal Justice Branch
3rd Floor, Centrium Place, 300
332-6 Avenue S.W.
Calgary, AB, T2P 0B2

Jolaine Antonio

Tel: (403) 297-6005
Fax: (403) 297-3453
Email: jolaine.antonio@gov.ab.ca

Counsel for the Intervener, Attorney General of Alberta

Gowling Lafleur Henderson LLP
2600 - 160 Elgin St
Box 466, Station D
Ottawa, ON, K1P 1C3

Brian A. Crane, Q.C.

Tel: (613) 233-1781
Fax:: (613) 563-9869
Email: brian.crane@gowlings.com

Agent for the Intervener, Attorney General of Alberta

AND TO:

Attorney General of Québec
1200 route de l'Église, 2e étage
Québec, Que., G1V 4M1

Noël & Associés
111 rue Champlain
Gatineau, Que., J8X 3R1

	Dominique A. Jobin Abdou Thiaw	Pierre Landry
	Tel: (418) 643-1477 ext. 20788 Fax: (418) 644-7030 Email: djobin@justice.gouv.qc.ca	Tel: (819) 771-7393 Fax: (819) 771-5397 Email: p.landry@noelassocies.com
	Counsel for the Intervener, Attorney General of Québec	**Agent for the Intervener, Attorney General of Québec**
AND TO:	**Ruby Shiller Chan Hasan** 11 Prince Arthur Avenue Toronto, ON, M5R 1B2	**Sack Goldblatt Mitchell LLP** #500-30 Metcalfe Street Ottawa, ON, K1P 5L4
	Gerald Chan Nader R. Hasan	Colleen Bauman
	Tel: (416) 964-9664 Fax: (416) 964-8305 Email: gchan@rubyshiller.com	Tel: (613) 235-5327 Fax: (613) 235-3041 Email: cbauman@sgmlaw.com
	Counsel for the Intervener, British Columbia Civil Liberties Association	**Agent for the Intervener, British Columbia Civil Liberties Association**
AND TO:	**City of Vancouver** 453 West 12th Avenue Vancouver, B.C., V5Y 1V4	**Perley-Robertson, Hill & McDougall** #1400-340 Albert Street Ottawa, ON, K1R 0A5
	Bronson Toy Leonard T. Doust, Q.C.	Lynda A. Bordeleau
	Tel: (604) 871-6546 Fax: (604) 873-7445 Email: bronson.toy@vancouver.ca	Tel: (613) 238-2022 Fax: (613) 238-8775 Email: lbordeleau@perlaw.ca
	Counsel for the Intervener, Canadian Association of Chiefs of Police	**Agent for the Intervener, Canadian Association of Chiefs of Police**
AND TO:	**Davies Ward Phillips & Vineberg LLP** 40th Floor, 155 Wellington Street West Toronto, ON, M5V 3J7	**Gowling Lafleur Henderson LLP** 2600-160 Elgin Street, P.O. Box 446, Stn D Ottawa, ON, K1P 1C3
	Matthew Milne-Smith	Henry S. Brown, Q.C.
	Tel: (416) 863-5595 Fax: (416) 863-0871	Tel: (613) 233-1781 Fax: (613) 788-3433

	Email: mmilne-smith@dwpv.com	Email: henry.brown@gowlings.com
	Counsel for the Intervener, Canadian Civil Liberties Association	**Agent for the Intervener, Canadian Civil Liberties Association**
AND TO:	**Ursel Phillips Fellows Hopkinson LLP** 10th Floor, 30 St. Clair Avenue West Toronto, ON, M4V 3A1	**Supreme Advocacy LLP** #100-340 Gilmour Street Ottawa, ON, K2P 0R3
	Susan M. Chapman Jennifer Micallef Kristen Allen	Marie-France Major
	Tel: (416) 969-3061 Fax: (416) 968-0325 Email: schapman@upfhlaw.ca	Tel: (613) 695-8855 x102 Fax: (613) 695-8855 Email: mfmajor@supremeadvocacy.ca
	Counsel for the Intervener, Criminal Lawyers' Association	**Agent for the Intervener, Criminal Lawyers' Association**
AND TO:	**Pringle, Chivers, Sparks Teskey** #300-10150 100 Street NW Edmonton, AB, T5J 0P6	**Gowling Lafleur Henderson LLP** Suite 2600, 160 Elgin Street Ottawa, ON, K1P 1C3
	Dane F. Bullerwell	Jeffrey W. Beedell
	Tel: (780) 424-8866 Fax: (780) 426-1470 Email: dbullerwell@pringlelaw.ca	Tel: (613) 786-0171 Fax: (613) 788-3587 Email: jeff.beedell@gowlings.com
	Counsel for the Intervener, Criminal Trial Lawyers' Association (Alberta)	**Agent for the Intervener, Criminal Trial Lawyers' Association (Alberta)**
AND TO:	**Public Prosecution Service of Canada** P.O. Box 36, Exchange Tower #3400-130 King Street West Toronto, ON, M5X 1K6	**Directeur des poursuites pénales du Canada** 2ième étage, 284 rue Wellington Ottawa, ON, K1A 0H8
	Kevin R. Wilson W. Paul Riley	François Lacasse
	Tel: (416) 973-0026 Fax: (416) 973-8253 Email: kevin.wilson@justice.gc.ca	Tel : (613) 957-4770 Fax : (613) 941-7865 Email: flacasse@ppsc-sppc.gc.ca
	Counsel for the Intervener, Director of Public Prosecutions of Canada	**Agent for the Intervener, Director of Public Prosecutions of Canada**

TABLE OF CONTENTS

PART I – OVERVIEW

1. Mobile devices have greatly increased the amount and nature of personal information that most individuals carry on their person. This has, in effect, dramatically expanded the invasiveness of the historical law enforcement power to search incident to an arrest. In light of the heightened privacy interests inherent in mobile devices, searches of mobile devices can occur only:

    - Where there are reasonable grounds to believe that the contents of a mobile device are immediately necessary to prevent serious harm, to secure law enforcement safety or to prevent the deletion of data on the device, police may search the device incident to arrest; or

    - Where there are reasonable grounds to believe evidence of the underlying offence at issue resides on the mobile device, the device may be seized and judicial authorization for a search of such a device may occur.

    Nothing less will sufficiently protect the important privacy interests implicated by mobile devices.

PART II – POSITION ON APPELLANTS' QUESTIONS

2. The Interverner will address the question of warrantless searches of mobile devices incident to arrest, arguing that section 8 of the *Charter* generally requires prior judicial authorization.

PART III – STATEMENT OF ARGUMENT

3. The interverener proceeds by first establishing the general principles relating to the common law power to search incident to arrest and its constitutional limits. Next we describe the privacy interests inherent in mobile devices. Finally, we turn to the proper scope of a search of a mobile device incident to arrest.

A. THE COMMON LAW POWER TO SEARCH INCIDENT TO ARREST

4. The common law power to search incident to arrest has developed as a general exception to the primary protections afforded by section 8 of the *Charter*. These primary protections, set out by Justice Dickson in *Hunter v. Southam* and summarized by Justice Wilson in *Thomson Newspapers*, are: (a) prior authorization by a neutral and impartial arbiter capable of acting judicially in balancing the interests of the state against those of the individual; (b) reasonable grounds to believe an offence has been committed; (c) reasonable grounds to believe that the contemplated invasion of privacy will yield evidence of that particular offence; and (d) limits on the scope of authorization to

"only documents...strictly relevant to the offence." *Hunter* recognized that these requirements could not apply in all scenarios, but held that "where it is feasible...such authorization is a precondition for a valid search and seizure." Exceptions to this general requirement are to be "exceedingly rare", and are typically only recognized where there is a demonstrable need.

> ***Hunter v. Southam Inc.***, [1984] 2 S.C.R. 145; ***Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)***, [1990] 1 S.C.R. 425, per Wilson, J., dissenting but not on this point, para. 100; ***R. v. Grant***, [1993] 3 S.C.R. 223, paras. 22-24 and 28-29

5. The common law power to search incident to arrest is a broad exception to the general privacy protections set out in *Hunter*. It arises from the fact of arrest and is constitutional if it is 'truly incidental' by its temporal, geographical and purposeful connection to the arrest. The search must therefore be justified by a valid purpose connected with the arrest, which includes: ensuring the safety of law enforcement and the public, the protection of evidence from destruction, and the discovery of evidence of the offence at issue. Law enforcement must have a 'reasonable basis' for invoking a valid purpose, which entails subjective belief in the presence of a valid purpose and an objectively reasonable evidentiary basis for that belief. There must be "some reasonable prospect of securing evidence of the offence." Canadian courts have not clearly articulated the parameters of the 'reasonable basis' standard, merely specifying that it lacks the particularity and specificity that the well-established reasonable belief and reasonable suspicion standards require.

> ***R. v. Caslake***, [1998] 1 S.C.R. 51, per Lamer, C.J., para. 22, per Bastarache, J., in dissent, para. 48; ***R. v. D'Annunzio***, [2010] 224 C.R.R. (2d) 221 (ON SC), paras. 19-20, 23; ***R. v. Khan***, 2013 ONSC 1570, paras. 18-19, 51-53, 62 and 68

6. Lawful arrest does not signal an end to an individual's privacy rights. The common law power to search incident to arrest "does not arise as a result of a reduced expectation of privacy of the arrested individual" but from the "pragmatic and exigent circumstances inherent in the making of an arrest." Courts have recognized that "the treatment meted out by agents of the state to even the least deserving individual will often indicate the treatment that all citizens of the state may ultimately expect." Moreover, the arrested individual remains presumptively innocent and is the object of an adversarial criminal investigation. As such, courts retain an ongoing "responsibility to set boundaries which allow the state to pursue its legitimate interests, while vigorously protecting individuals' right to privacy."

R. v. Caslake, [1998] 1 S.C.R. 51, paras. 15, 17; ***R. v. Feeney***, [1997] 2 S.C.R. 13, para. 45; ***R. v. Golden***, 2001 SCC 83, paras. 32, 44 and 56; ***R. v. Stillman***, [1997] 1 S.C.R. 607, paras. 46-47; ***R. v. Vye***, 2014 BCSC 93, paras. 50-51

7. Ultimately, assessing the scope of the common law power to search incident to arrest requires "balancing the privacy rights of the arrested person against the duty of the police." In general, the state must demonstrate that "the interference with liberty is necessary given the extent of the risk and the liberty at stake, and no more intrusive to liberty than reasonably necessary to address the risk" if it is to justify a common law search power as consistent with *Charter* values. The proportionate interference with privacy in view of the objectives sought is a factor as is the existence of "less intrusive means of attaining these objectives". Hence, where there is no demonstrable necessity to preserve evidence from destruction or to protect law enforcement, the rationale for a search incident to arrest is attenuated. Where lack of necessity meets heightened privacy interests, the disproportionate impact on constitutionally protected liberties can render a search incident to arrest outside the scope of the common law power or render that power unreasonable. Recently, a number of courts in Canada and the United States have balked at applying the full breadth of the search incident to arrest power to data contained in mobile devices.

R. v. MacDonald, 2014 SCC 3, paras. 66-71, 31, and 36-38; ***R. v. Golub***, [1997] 34 O.R. (3d) 743, (ON CA), paras. 27-29; ***R. v. Caslake***, [1998] 1 S.C.R. 51, para. 15; ***R. v. Golden***, 2001 SCC 83, para. 56; ***Cloutier v. Langlois***, [1990] 1 S.C.R. 158, paras. 58-59; ***R. v. Clayton***, 2007 SCC 32, para. 21; H. Fakhoury, "**Feature: Challenging Cell Phone Searches Incident to Arrest**", (2013) *37 Champion 30*

B. THE PRIVACY INTEREST AT STAKE

8. The quality and diversity of data present on mobile phones raises serious concerns for privacy. Even relatively basic mobile devices today permit individuals to generate and carry a rich, detailed and easily accessible assortment of data about their personal lives with them everywhere they go. This data is qualitatively different what was historically carried by individuals. Such devices have the capacity to generate and store comprehensive conversations in the form of text messages and emails, detailed contact lists and call logs, and still or video image capture. Moreover, as all of these features are combined in one device, individuals do not have the option of selective carriage (selectively bringing the 'business contact book' and 'picture of newborn baby' while leaving the 'personal contact book' and 'invasive photos' at home) as they did historically when packing a briefcase. The

same device generates the data *and* stores it. Finally, it must be noted that feature phones are being rapidly superseded by more sophisticated devices which have all the capacities of modern computers, with the associated privacy implications. The privacy interests of third parties – present in the images, conversations and interactions captured on the mobile device – are also implicated.

9. **Text Messages.** Private communications such as text messages engage a high level of privacy. The interception of such communications without authorization is a criminal offence, and the authorization regime for such interception imposes stringent protections in light of the serious privacy implications entailed. This Court has recognized the increasing prevalence of text messaging as a popular form of communication, describing a text message exchange as "an electronic conversation." Such conversations are captured on mobile devices and exposed to subsequent searches by law enforcement, implicating many of the same interests that are protected by the prohibition on wiretapping. The utility and ease of use associated with text messaging often captures an even richer mosaic of personal life than a telephone call.

> ***R. v. TELUS Communications Co.***, 2013 SCC 16, per Abella, J., paras. 1, 5, 27-28, 30-31and per Moldaver, J., paras. 71-73; ***R. v. Duarte***, [1990] 1 S.C.R. 30, paras. 21 and 47; ***R. v. S.M.***, 2012 ONSC 2949, paras. 22-25; ***R. v. Vye***, 2014 BCSC 93, paras. 6, 50-51

10. **Contact Books and Call Logs.** Mobile devices also contain detailed records of our contacts and associations. Contact books and phone call logs can offer a highly revealing picture of an individual. Most mobile devices contain comprehensive contact lists as well as Caller ID-enabled call logs that will identify most incoming and outgoing calls, as well as the time and duration of the call. This could include, for example, records of calls to suicide or other hotlines, to specialized medical clinics, or to political and religious institutions. Even more basic associations with individuals evoke strong privacy interests, as this Court recognized in *Thomson Newspapers*: "It is for the individual to decide what persons or groups he or she will associate with...One does not have to look far in history to find examples of how the mere possibility of the intervention of the eyes and ears of the state can undermine the security and confidents that are essential to the meaningful exercise of the right to make such choices."

> ***R. v. Polius***, [2009] 196 C.R.R. (2d) 288, para. 52; J. Mayer & P. Mutchler, "**MetaPhone: The Sensitivity of Telephone Metadata**", WebPolicy.org, March 12, 2014; ***Amici Curiae* Brief of Experts**

> **in Computer and Data Science**, March 13, 2014, *ACLU v. Clapper*, Case No.: 14-42, (2nd Cir 2014)(U.S.); ***Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)***, [1990] 1 S.C.R. 425, per La Forest, J., concurring, para. 141

11. **Photos & Videos.** Today's mobile devices (including the most basic of mobile phones) are not merely communications tools, but also provide the ubiquitous capacity to capture images in real-time. Individuals have become accustomed to having digital cameras with them at all times, and this has led to social changes in the ways that cameras are used:

> We live in an age in which digital cameras, either standing alone or as a component of other electronic devices such as smartphones, have become ubiquitous. Those cameras allow individuals to record personal, and sometimes, intimate aspects of their lives and those of their family and friends, in a manner that would not have been contemplated in the days when the common way for most people to take photographs was with a camera using film that had to be given to a third-party to develop and print. Today, for some people, a digital camera may serve as an electronic journal or diary.

The types of images captured with and stored on mobile devices are not only revealing of daily life, but can be extremely intimate and sensitive in nature. Many of these images would not have been captured historically or, if captured, would be stored far from prying eyes at home. In addition, mobile devices allow for image and video *sharing* of images and video with other individuals, creating further incentives to capture and retain a rich assortment of images on mobile devices. Searches of mobile devices conducted incident to arrest have already come across such sensitive and embarrassing images and videos, and can expect to do so with greater frequency in the future.

> ***R. v. Caron***, 2011 BCCA 56, para. 60; ***R. v. Vye***, 2014 BCSC 93, paras. 6 and 51; ***R. v. Adeshina***, 2013 SKQB 414, para. 34; ***R. v. D'Annunzio***, [2010] 224 C.R.R. (2d) 221 (ON SC), paras. 4-5; J. Bailey & M. Hanna, "**The Gendered Dimensions of Secting: Assessing the Applicability of Canada's Child Pornography Provision"**, (2011) 23 *Can J. W. & L.* 405

12. **Computer-like Features.** Even the most basic mobile devices exhibit several features that this Court has identified as raising distinct privacy issues. Basic storage capacity permits text, video and call logging information to be retained indefinitely and, by default, it is. Mobile devices retain (and permit forensic recovery of) temporary activity such as draft text messages and manually deleted content. Ancillary information, such as the time, duration and destination of all calls, is automatically generated by the device. The device can access remote content such as voice mail, often without the need to input a password. Moreover, mobile phones are rapidly becoming what are effectively miniature computers. In 2012, 52% of all mobile devices used were already smartphones, tablets or other advanced mobile

devices. Canadians are increasingly utilizing these devices to listen to music, read online news, watch television, access social networks, browse the Internet and send/receive Email. Additionally, mobile devices increasingly permit individuals to access data from their home computers or even to monitor activities within their homes through remote access to webcams and other security features.

> ***R. v. Vu***, 2013 SCC 60, paras. 41-44; ***R. v. Polius***, [2009] 196 C.R.R. (2d) 288, para. 53; ***R. v. Vye***, 2014 BCSC 93, para. 5(d); ***R. v. Fearon***, 2013 ONCA 106, para. 16; Canadian Radio-television & Telecommunications Commission, ***Communications Monitoring Report***, September 2013, p. ii and Figure 6.2.18; ***U.S. v. Wurie***, 728 F.3d 1, (1st Cir, 2013), pp. *8-9

C. SEARCHING CELL PHONES INCIDENT TO ARREST

13. In the absence of exigent circumstances, the common law power cannot extend to the seizure of a mobile device incident to arrest. The reasonable basis standard for searches incident to arrest does not provide adequate protection for the heightened privacy interests at issue in mobile devices. The lack of prior authorization is neither necessary, nor sufficient to ensuring searches of mobile devices are conducted in a targeted, minimally intrusive and proportionate manner.

EXIGENT CIRCUMSTANCES

14. Where there are reasonable grounds to believe that the contents of a mobile device are immediately necessary to prevent serious harm, law enforcement should be permitted to seize and search that device incident to arrest in order to alleviate such harm. This is reasonable and in keeping with the general statutory and constitutional standards. It is also necessary, as the exigent nature of the threat in question will often make it impractical to seek or obtain a warrant. While a mobile device will rarely pose an imminent threat to law enforcement, there could be scenarios where the circumstances of arrest give rise to a tangible threat and the information on an arrestee's mobile device could help to assuage or prevent this threat. As in other contexts, a 'safety search' of a mobile device can be justified in instances where there are reasonable grounds to believe such an imminent threat exists.

> ***R. v. Tse***, 2012 SCC 16, paras. 32-33; ***Respondent's Memorandum of Fact and Law***, January 31, 2014, paras. 55-56; ***R. v. MacDonald***, 2014 SCC 3, paras. 41-43

15. Similarly, where there are reasonable grounds to believe in the existence of a tangible risk that evidence on a mobile device might be destroyed, police should be permitted to take measured steps to preserve

the evidence incident to arrest. This cannot be a 'generalized' risk, applied to all mobile devices, as that would amount to a "blanket exception". It should be noted that the presence of such a risk would be rare, as powering down a device or removing its battery (at least until officers return to the station) will typically address any risk of remote deletion of evidence hosted on the device itself. Where there is reason to believe that powering down a device is insufficient, measured steps can be taken, such as the temporary imaging of the device or the placement of the device in a "Faraday enclosure" – a "relatively inexpensive device formed by conducting material that shields the interior from external electromagnetic radiation." Finally, much like with computers, there is "the capacity to recover deleted information" (*Polius*; *Vye*). However, the content of the device should not be viewed or analyzed until a warrant has been sought and issued unless these measures are demonstrably ineffective.

> ***R. v. Grant***, [1993] 3 S.C.R. 223, paras. 29-31; ***R. v. Polius***, [2009] O.J. No. 3074, para. 53; ***R. v. Vye***, 2014 BCSC 93, para. 5(d); ***R. v. Vu***, 2013 SCC 60, para. 49; ***U.S. v. Wurie***, 728 F.3d 1, (1st Cir, 2013), certiorari granted, 134 S.Ct. 999 (Supreme Court, 2014)(U.S.), pp. *11; H. Fakhoury, "**Feature: Challenging Cell Phone Searches Incident to Arrest**", (2013) *37 Champion 30*, p. 34

NON-EXIGENT EVIDENTIARY SEARCHES

16. **Reasonable Grounds to Believe:** In the Non-exigent evidentiary searches must be premised on reasonable grounds to believe. The current 'reasonable basis' standard is too low to offer adequate protection for the heightened privacy rights housed in mobile devices. The ubiquitous use of mobile devices and the diversity of data commonly held on such devices will mean that, much like a home, there will almost *always* be a reasonable basis for believing that searching the device may yield evidence of the offence in question. A commonly advanced justification for searching mobile devices incident to arrest is an officer's experience that alleged criminals use mobile devices to communicate. Similarly, officers commonly advance the justification that alleged criminals take incriminating photographs with their mobile devices. A consistent application of the 'reasonable basis' standard would permit searches in most instances, even in the absence of any *specific* grounds to justify intrusion of a specific mobile device, simply because suspected criminals (like all individuals) use mobile devices in all aspects of life.

> ***R. v. Khan***, 2013 ONSC 1570, paras. 18-19, 51-53, 62 and 68 ("he decided to do so because in his experience, such devices often contain text messages or photographs of drugs which might provide evidence of trafficking in narcotics."); ***R. v. Caron***, 2011 BCCA 56, paras. 7-9 and 16 ("In my experience...people involved in crime have photographed themselves or the crime as a keepsake...there may be photographs of his speedometer showing a high rate of speed."); ***R. v.***

> ***D'Annunzio***, [2010] 224 C.R.R. (2d) 221 (ON SC), paras. 4-6, 20-21, 23 ("...she thought there could be photos or videos that could possibly 'be evidence of the sexual assault or other inappropriate sexual behaviour.'"); ***R. v. Fearon***, 2010 ONCJ 645, paras. 26 and 44 ("...the cell phone might have text messages or last calls that would indicate persons they communicated with shortly after the robbery...Also...people take photographs of things they steal...")

17. Permitting the generalized 'reasonable basis' standard to govern searches of mobile devices will mean, in effect, that officers may search mobile devices in most situations. Much like a home, people treat their phones as a secure repository for a range of often sensitive information that they would not otherwise have on their person at all times. Much like a home or a wiretap, there will almost always be a general prospect that evidence of an offence will be discoverable on a mobile device. This is because, much like a home or real-time communications, mobile devices are implicated in all aspects of our lives. We do not, however, permit law enforcement to search the home of every arrestee. The "mere possibility" that evidence may exist on a mobile device "is not sufficient to justify" its search in light of the heightened privacy interests involved (*Golden*). Only a standard that requires individualized, specific and objectionably discernable facts can ensure that mobile devices are invaded in a proportionate and reasonably necessary manner. Much like searches of computers incident to a warrant, evidentiary searches of mobile devices must therefore be premised on independent reasonable grounds to believe that the search will yield evidence of the offence in question.

> ***R. v. Feeney***, [1997] 2 S.C.R. 13, para. 160; ***R. v. Golub***, [1997] 34 O.R. (3d) 743, (ON CA), paras. 36-37, 40; ***R. v. Jones***, 2011 ONCA 632, paras. 47-48; ***R. v. Fearon***, 2010 ONCJ 645, para. 47; ***R. v. Vu***, 2013 SCC 60, paras. 47-48; ***R. v. Khan***, 2013 ONSC 1570, paras. 53, 58 and 62; ***R. v. Caron***, 2011 BCCA 56, para. 60; ***R. v. D'Annunzio***, [2010] 224 C.R.R. (2d) 221 (ON SC); ***R. v. Vye***, 2014 BCSC 93, para. 6; ***R. v. Golden***, 2001 SCC 83, paras. 94, 98; ***R. v. MacDonald***, 2014 SCC 3, para. 36 and 41

18. **Prior Judicial Authorization:** Much as with evidentiary searches of the home, non-exigent evidentiary searches of the data in mobile devices is in a "different place" and requires prior judicial authorization (*Jones*). There is good reason to require distinct and prior judicial authorization for the data on a mobile device. At the time of arrest, the decision to search is often based on "information which is often less than exact or complete" and conditions where "[j]udicial reflection is not a luxury that the officer can afford." This does not permit for the careful and judicious weighing and deliberation that is necessary in order to effectively limit a search of a mobile device. Moreover such a search cannot be conducted in a targeted manner incident to arrest. This is because mere access to a

mobile device places significant amounts of data in 'plain view'. In addition, while search protocols and other data-specific search limitations are not at this time a constitutional imperative in each and every search of a data receptacle, prior judicial authorization will permit courts to determine on a case by case basis whether such limitations are necessary to render a search of a given mobile device 'reasonable'. Overall, to enable minimal intrusion on private data, searches of mobile devices must be carried out under controlled conditions, with the use of "necessary software, technology and expertise", after serious and judicious consideration of the particulars at issue.

> ***R. v. Golub***, [1997] 34 O.R. (3d) 743, (ON CA), para. 18; ***R. v. Jones***, 2011 ONCA 632, paras. 47-50; ***R. v. Liew***, 2012 ONSC 1826, paras. 137-138; ***R. v. Vu***, 2013 SCC 60, para. 62; ***R. v. D'Annunzio***, [2010] 224 C.R.R. (2d) 221 (ON SC), para. 26; ***R. v. Polius***, [2009] 196 C.R.R. (2d) 288, para. 57

19. Permitting even cursory searches incident to arrest will impact heavily on the heightened privacy interests inherent in mobile devices. A 'thumbing through' of a mobile device can easily reveal highly sensitive and embarrassing images or interactions (*Polius; Khan; Vye*). It can reveal political, religious or other preferences through contact listings or call logs or text-based exchanges. In light of small screen sizes and limited controls, information on mobile devices is necessarily optimized for quick and easy accessibility. Even the most cursory search of the data on a mobile device at the scene of arrest – intended to confirm ownership of the device and nothing more – has included combing through photographs and private communications on the device (*Manley*). This Court recently held that even cursorily pushing an apartment door "slightly further open" in order "to get a better view" was invasive as such an act "had the potential to reveal to the officers...any number of things...as they could now see more of the interior of the unit." A 'cursory' or casual thumbing through of the data on a mobile device "does not lessen the gravity of [the] intrusion" and has equal potential to reveal (*Caron*; *Khan*). Prior authorization is therefore required for any search of the data held in a mobile device.

> ***R. v. Khan***, 2013 ONSC 1570, paras. 18-20 and 58; ***R. v. Fearon***, 2013 ONCA 106, paras. 14-15; ***R. v. Liew***, 2012 ONSC 1826, para. 15; ***R. v. Manley***, 2011 ONCA 128, paras. 37-38; ***R. v. Hiscoe***, 2013 NSCA 48, paras. 5-7; ***R. v. MacDonald***, 2014 SCC 3, para. 42; ***R. v. Caron***, 2011 BCCA 56, para. 61; ***R. v. Vye***, 2014 BCSC 93; ***R. v. Polius***, [2009] 196 C.R.R. (2d) 288, para. 57, para. 20

20. Not any and all examinations of a device will fall outside the common law power and, hence, be unconstitutional. It is possible to gain cursory information about a mobile device without rummaging through its data. For example, in *Wurie*, (U.S. 1st Circuit, currently under appeal), the

arrestee's outward-facing caller ID screen indicated repeated calls from a number identified as 'my house' in plain site. Other courts have recognized reasonable ways of gaining information about a device without accessing the data held therein (*Burchell*; *Little*). In addition, the mobile device itself will typically display a serial number and other device and even subscriber identifiers on the exterior of the device that can be used to determine device ownership, for example.

> ***R. v. Burchell***, 2011 ONSC 6236, paras. 48-49; ***R. v. Little***, [2009] O.J. No. 3278, (ON SC), paras. 143-147, 149; ***U.S. v. Wurie***, 728 F.3d 1 (1st Cir., 2013)(U.S.), p. *2

21. A mobile device can also be properly seized incident to arrest, at which point there will "exist...less intrusive means of attaining" the data contained therein (*Cloutier; MacDonald*). In the absence of exigent circumstances, this data is secure once the device is seized. The data is more secure than physical evidence, which can be hidden on (or in) the arrestee (*Golden*), in the arrestee's immediate surrounding area or in a container on the arrestee's person (*Smallwood*). Law enforcement need to be able to assess whether the arrestee hid evidence in the 'lead up' to arrest but evidence cannot be 'stashed' in a mobile device. Balancing the high likelihood that irrelevant and extremely private information will be revealed with the lack of any immediate law enforcement need renders any *ex post* judicial analysis of the propriety of a search "most unsatisfactory" (*Hiscoe*). We therefore respectfully submit that, in the absence of exigent circumstances, any search of data contained within a mobile device be premised on prior judicial authorization. This approach will have the additional benefit of permitting the judiciary to play an ongoing *a priori* role in determining the proper scope of access in light of the "ever-quickening pace of change" that characterizes mobile device capacities.

> ***Smallwood v. State***, 113 So. 3d 724 (Fla Sup Ct, 2013)(U.S.), pp. *735-738; ***Cloutier v. Langlois***, [1990] 1 S.C.R. 158, para. 58; ***R. v. MacDonald***, 2014 SCC 3, paras. 36-37; ***R. v. Hiscoe***, 2013 NSCA 48, para. 69-70; ***R. v. Golden***, 2001 SCC 83, paras. 32, 44 and 56

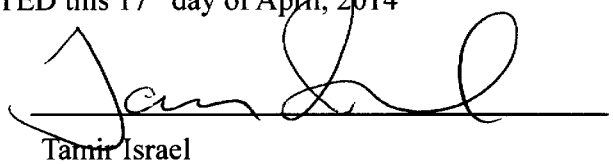
PART IV – COSTS

22. The intervener will not seek costs and asks that no costs be awarded against it.

PART V – ORDER SOUGHT

23. The intervener does not seek oral argument, but respectfully requests that its written submissions will be taken into account in resolving the issues raised by this appeal.

ALL OF WHICH IS RESPECTFULLY SUBMITTED this 17th day of April, 2014



Tamir Israel

Samuelson Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)
University of Ottawa, Faculty of Law, CML
57 Louis Pasteur Street
Ottawa, ON, K1N 6N5

Tel: (613) 562-5800 ext. 2914
Fax: (613) 562-5417
Email: tisrael@cippic.ca

Counsel for the Intervener, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC)

PART VI – TABLE OF AUTHORITIES