COURT OF APPEAL FOR ONTARIO

CITATION: R. v. Hafizi, 2023 ONCA 639
DATE: 20230928
DOCKET: C67423

Fairburn A.C.J.O., Doherty, Feldman, Pepall and Pardu JJ.A.

BETWEEN

His Majesty the King

Respondent

and

Temorshah Hafizi

Appellant

Howard L. Krongold, for the appellant

Lisa Mathews and Allyson Ratsoy, for the respondent

Nader Hassan and Spencer Bass, for the intervener the Canadian Civil Liberties Association

Michael Lacy, Bryan Badali and Sara Little, for the intervener the Criminal Lawyers' Association of Ontario

Jeremy Streeter and Emily Marrocco, for the intervener the Attorney General of Ontario

Heard: February 16, 2023

On appeal from the conviction entered by Justice Charles T. Hackland of the Superior Court of Justice, dated December 4, 2018.

Fairburn A.C.J.O.:

I. OVERVIEW

[1] This is an appeal from conviction for possession of heroin for the purpose of trafficking and uttering a death threat.

[2] The appellant has been tried twice. The first trial ended in an acquittal, followed by a successful Crown appeal. The second trial ended in a conviction, followed by this appeal.

[3] The prosecution's case was strong and rested largely on two sources of information: (1) the appellant's private communications that were intercepted pursuant to a s. 186(1) *Criminal Code* wiretap authorization; and (2) heroin and other drug-related items seized from the appellant's vehicle incident to his arrest: *Criminal Code*, R.S.C. 1985, c. C-46.

[4] The parties have agreed all along that if there had been no interception of the appellant's private communications, then there would have been no arrest and, of course, if there had been no arrest, there would have been no search incident to arrest. Accordingly, both trials focussed upon the decisive issue: were the appellant's private communications obtained in a constitutionally compliant manner?

[5] At the first trial, the trial judge found that there was a s. 8 *Charter* breach because there were deficiencies in the affidavit in support of the application for a s. 186 authorization and excluded all the evidence. After the successful Crown

appeal, the focus at the second trial was on the constitutionality of ss. 185 and 186 of the *Criminal Code*. The appellant argued that this court's interpretation of those provisions in *R. v. Mahal*, 2012 ONCA 673, 113 O.R. (3d) 209, leave to appeal refused, [2012] S.C.C.A. No. 496, has rendered the provisions unconstitutional to the extent that it allows a person's private communications to be intercepted on the basis of reasonable grounds to believe that those interceptions "may assist" (as opposed to "will assist") the investigation. The appellant says that allowing an individual's private communications to be targeted for interception on anything less than what he calls a *Hunter*-compliant "will assist" standard breaches s. 8 of the *Charter*: *Hunter et al. v. Southam Inc.*, [1984] 2. S.C.R. 145. As the second trial judge felt bound by this court's decision in *Mahal*, he dismissed the application for a declaration of unconstitutionality.

[6] The appellant now asks this five-judge panel to find that *Mahal* was wrongly decided. The appellant contends that *Mahal* offends s. 8 of the *Charter* to the extent that it rejects the need for *Hunter*-compliant grounds when it comes to naming specific individuals, places and devices in a wiretap authorization. In the alternative, if we are unprepared to overturn *Mahal* on this point, the appellant asks us to declare ss. 185 and 186 unconstitutional because *Mahal*'s interpretation of the two provisions is said to breach s. 8 of the *Charter*.

[7] The appellant's arguments cannot succeed. As I will explain, *Mahal* is not the first case to say that the *Hunter*-compliant standard of reasonable grounds to

believe that the interception of private communications “will assist” the investigation applies only to the authorization as a whole, and not on an individualized basis. Indeed, on this point, *Mahal* is entirely consistent with prior case law from this court, including *R. v. Finlay and Grellette* (1985), 52 O.R. (2d) 632 (C.A.), leave to appeal refused, [1986] S.C.C.A. No. 46. *Mahal* is also consistent with binding Supreme Court authority, including case law that affirms *Finlay*. Further, even if there was not binding Supreme Court authority, there is good reason for applying the “will assist” standard to the authorization as a whole and a lower standard to particular people, places and devices named in the authorization.

II. PROCEDURAL BACKGROUND

(1) The investigation

[8] The appellant’s son was being investigated for the murder of a man who was stabbed to death outside an Ottawa nightclub.[1] In the context of the murder investigation, the police obtained a s. 186(1) wiretap authorization for a 60-day period (the “first authorization”).

[9] As detailed further below, a wiretap application may be issued under s. 186(1) if the judge is satisfied, based on an application made pursuant to s. 185,

---

[1] His son was ultimately found guilty of second degree murder: *R. v. Hafizi*, 2019 ONCA 2, 373 C.C.C. (3d) 264.

that (1) “it would be in the best interests of the administration of justice to do so”, and (2) investigative necessity has been made out. A s. 185 application must be made by a designated person, supported by an affidavit that contains specified information, including “the names …, if known, of all persons, the interception of whose private communications there are reasonable grounds to believe may assist the investigation of the offence” (emphasis added).

[10] The appellant was named in the first authorization as a person whose communications could be intercepted. The authorization allowed for communications to be intercepted at multiple places, including four related to the appellant: (a) the home he shared with his son; (b) the pizza place that the appellant owned and where he and his son worked; (c) the appellant’s car; and (d) the appellant’s cellular phone. As for the pizza place, the authorization contained a minimization clause, requiring that any interceptions at that location be subject to live audio monitoring or visual surveillance. If a person listed as a “principal known person” in the wiretap authorization was not a party to a communication, then the interception had to be discontinued.

[11] During the first authorization, the police intercepted a conversation between the appellant and his wife that suggested their son was going to leave the country for Afghanistan. The police then discovered that the son had purchased an airline ticket and was about to depart from Canada. Accordingly, he was arrested for murder and detained.

[12] After the son's detention, a second authorization was obtained so that the son's private communications could be intercepted from the custodial facility where he was held. The appellant was also named in the second authorization.

[13] The interception of the appellant's private communications did not just reveal useful information for purposes of the murder investigation. Rather, those interceptions also revealed that the appellant was involved in drug trafficking. In addition, the interceptions captured the appellant making a death threat – that the appellant would "stab [a particular police officer] in his fuckin' neck" the next time the officer came into the appellant's restaurant.

[14] Ultimately, the appellant was convicted of possession of heroin for the purpose of trafficking and uttering a death threat.

(2) The trials

[15] The focal point of both of the appellant's trials was the first wiretap authorization, since the appellant's incriminating conversations were intercepted pursuant to that authorization.

(a) First trial

[16] As noted, the trial judge at the first trial concluded that the appellant's s. 8 *Charter* rights had been breached: 2014 ONSC 3547. That breach was said to be rooted in two things: (a) there were insufficient grounds to support naming the appellant in the authorization; and (b) the affiant had misled the application judge

by deliberately withholding relevant information. Virtually all of the evidence was excluded under s. 24(2) of the *Charter*. Inevitable acquittals followed.

[17] While the appellant had also asked the first trial judge for a declaration that ss. 185 and 186 of the *Criminal Code* were unconstitutional because of the “Court of Appeal[']s interpretation of sections 185 and 186 in *R. v. Mahal*”, the trial judge found it unnecessary to address the request in light of his conclusion on the s. 8 breach.

[18] The Crown appealed the acquittals to this court: 2016 ONCA 933, 343 C.C.C. (3d) 380 (“*Hafizi* ONCA #1”). This court concluded that the trial judge had erred in two ways: (a) by failing to conduct a contextual analysis of the affidavit material, and (b) by failing to properly apply the *Garofoli* standard of review: *R. v. Garofoli*, [1990] 2 S.C.R. 1421, at p. 1452. This court held that a proper application of the *Garofoli* standard of review resulted in only one possible finding: that it was open to the application judge to conclude that there were “reasonable grounds to believe that the interception of the respondent’s private communications might assist in the investigation of a murder in which his son was the prime suspect”: *Hafizi* ONCA #1, at para. 62 (emphasis added). As is clear from this passage (and others), the appeal in *Hafizi* ONCA #1 was resolved in a manner consistent with *Mahal*, on the basis of a “may assist” threshold.

[19] Although the appellant continued to advance his constitutional challenge as an alternative position in *Hafizi* ONCA #1, this court declined to decide the issue, noting that it did not have the benefit of reasons from the lower court: *Hafizi* ONCA #1, at paras. 65-66. In the end, the acquittals were set aside, and a new trial was ordered "without prejudice to the right of the [appellant] to renew his constitutional challenge to ss. 185 and 186 of the *Criminal Code* at that time": at paras. 5, 70. That is what he did.

(b) Second trial

[20] At the second trial, the constitutional issue was squarely litigated and decided: 2017 ONSC 5273. The trial judge, at para. 1, described the constitutional challenge as follows:

> By way of pre-trial motion, the applicant seeks a declaration of unconstitutionality in respect of sections 185 and 186 of the *Criminal Code* … 'to the extent that they permit an individual's private communication to be targeted for interception where there are no reasonable grounds to believe that the interception of that person's private communications will afford evidence of an offence'. [Emphasis added.]

[21] The appellant maintained that, before naming a person in an authorization, there must be reasonable grounds to believe that the interception of that specific person's private communications "will assist" (not simply "may assist") the investigation. I will sometimes refer to this position as a call for "individualized grounds". The appellant argued that nothing short of individualized grounds could

meet the minimum constitutional standard required to achieve s. 8 *Charter* compliance. Therefore, the appellant maintained that, to the extent that *Mahal* had interpreted ss. 185 and 186 of the *Criminal Code* as not requiring individualized grounds, it had rendered the provisions inconsistent with s. 8 of the *Charter*.

[22] The second trial judge concluded that the appellant's argument was really just an indirect attack on this court's decision in *Mahal*, a binding appellate decision. Therefore, the application was dismissed, after which the appellant entered an agreed statement of facts that supported the convictions that followed. The appellant now appeals from those convictions, an appeal that is strictly focussed upon the constitutional issue.

III. STATUTORY SCHEME

[23] Before turning to the issues in this case, it is helpful to start by describing the relevant statutory provisions, since understanding how the statutory scheme works is essential to understanding the analysis of the issues to come.

(1) Application for an authorization: s. 185

[24] Section 185 of the *Criminal Code* sets out the criteria that must be addressed in a third-party wiretap application, sometimes also referred to as an "omnibus application". I say "third-party wiretap application" to distinguish a s. 185 application from other forms of Part VI wiretap applications, such as a one-party consent application (s. 184.2) or an emergency wiretap application (s. 188).

[25] The s. 185 application provision specifies who may bring an application, how it should be brought, who may hear it, and the contents of the affidavit that must accompany such an application, including who must be named in the affidavit:

> **185 (1)** An application for an authorization to be given under section 186 shall be made *ex parte* and in writing to a judge of a superior court of criminal jurisdiction or a judge as defined in section 552 and shall be signed by the Attorney General of the province in which the application is made or the Minister of Public Safety and Emergency Preparedness or an agent specially designated in writing for the purposes of this section by
>
> > **(a)** the Minister personally or the Deputy Minister of Public Safety and Emergency Preparedness personally, if the offence under investigation is one in respect of which proceedings, if any, may be instituted at the instance of the Government of Canada and conducted by or on behalf of the Attorney General of Canada, or
> >
> > **(b)** the Attorney General of a province personally or the Deputy Attorney General of a province personally, in any other case,
>
> and shall be accompanied by an affidavit, which may be sworn on the information and belief of a peace officer or public officer deposing to the following matters:
>
> > **(c)** the facts relied on to justify the belief that an authorization should be given together with particulars of the offence,
> >
> > **(d)** the type of private communication proposed to be intercepted,
> >
> > <u>**(e)** the names,</u> addresses and occupations,<u> if known, of all persons, the interception of whose private communications there are reasonable grounds to believe may assist the investigation of the offence</u>, a general description of the nature and location of the place, if known, at which private communications are proposed to be intercepted and a general description of the manner of interception proposed to be used,

> **(f)** the number of instances, if any, on which an application has been made under this section in relation to the offence and a person named in the affidavit pursuant to paragraph (e) and on which the application was withdrawn or no authorization was given, the date on which each application was made and the name of the judge to whom each application was made,
>
> **(g)** the period for which the authorization is requested, and
>
> **(h)** whether other investigative procedures have been tried and have failed or why it appears they are unlikely to succeed or that the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures. [Emphasis added.]

[26] Notably, s. 185(1)(e) specifies the standard for naming a person in the affidavit, namely "reasonable grounds to believe [the interception of the person's private communications] <u>may assist</u> the investigation of the offence" (emphasis added).

(2) The authorization: s. 186

(a) The test for issuing an authorization

[27] Section 186(1) sets out the two overarching criteria that application judges must take into account when considering whether to issue a third-party wiretap authorization:

> **186 (1)** An authorization under this section may be given if the judge to whom the application is made is satisfied
>
> **(a)** that it would be in the best interests of the administration of justice to do so; and
>
> **(b)** that other investigative procedures have been tried and have failed, other investigative procedures are unlikely to

> succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures.

(i) Criteria #1 – Best interests of the administration of justice/ reasonable grounds to believe (s. 186(1)(a))

[28] In *Finlay*, which was the first case to consider the constitutionality of the third-party wiretap provisions, Martin J.A. interpreted the "best interests of the administration of justice" in s. 186(1)(a) as including a *Hunter*-compliant standard. To this end, he said that the phrase "imports at least the requirement that the judge must be satisfied that there [are] reasonable ground[s] to believe that communications concerning the particular offence[2] will be obtained through the interception sought": at p. 656 (emphasis added). As I will explain below, this standard applies to the authorization as a whole.

[29] Before moving on, it is worth making a brief note about terminology. The "best interests of the administration of justice" test in s. 186(1)(a) is sometimes described by the shortform "probable cause". However, I prefer not to use this term. It derives from the Fourth Amendment of the United States Constitution (which protects "[t]he right of the people to be secure … against unreasonable

---

[2] "Offence" is defined in s. 183(1) of the *Criminal Code* for purposes of Part VI as follows: "offence means an offence contrary to, any conspiracy or attempt to commit or being an accessory after the fact in relation to an offence contrary to, or any counselling in relation to an offence contrary to (a) any of the following provisions of this Act, namely …". The provisions that follow are largely considered the most serious offences in the *Criminal Code* and other federal Acts, the point being that third-party wiretap authorizations are not available for just any criminal investigation.

searches and seizures … but upon <u>probable cause</u> …"), not from s. 8 of the *Charter* (which protects against "unreasonable search and seizure"). In my view, the use of the term probable cause can inject confusion into this area of the law.

[30] As a general proposition, a reasonable search and seizure will be one where the needs of law enforcement overtake individual privacy interests, which is the point at which "credibly-based probability replaces suspicion": *Hunter*, at p. 167. The court in *Hunter* pointed to s. 443 (now s. 487) of the *Criminal Code* as a statutory expression of this constitutionally compliant threshold, that being reasonable grounds to believe that there is something in the location of search that <u>will afford</u> evidence with respect to the commission of the offence under investigation: at pp. 167-68.

[31] Undoubtedly, since *Hunter*, there have been numerous decisions that accept the general equivalency between the s. 8 *Charter*-compliant "reasonable grounds to believe" standard noted in *Hunter* and the American "probable cause" standard embedded in the Fourth Amendment: see e.g., *Baron v. Canada*, [1993] 1 S.C.R. 416, at p. 447; *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253, at para. 128, *per* Deschamps J. (dissenting, but not on this point); *R. v. Golub* (1997), 34 O.R. (3d) 743 (C.A.), at p. 759, leave to appeal refused, [1997] S.C.C.A. No. 571; *R. v. Ebanks*, [2007] O.J. No. 2412, at para. 15, rev'd but not on this point, 2009 ONCA 851, 97 O.R. (3d) 721, leave to appeal refused, [2010] S.C.C.A. No. 84; *R. v. Ha*, 2018 ABCA 233, 363 C.C.C. (3d) 523, at para. 59; and *R. v. Law*, 2002

BCCA 594, 171 C.C.C. (3d) 219, at para. 7. Even so, I still prefer to avoid the use of the term "probable cause" in the Canadian s. 8 context because the term "probable" is redundant when it comes to what "reasonable grounds to believe" means under s. 8 of the *Charter.* This is because reasonable grounds to believe imports the concept of credibly-based probability. This is precisely why the Supreme Court noted as early as *Baron*, that the terms "reasonable" and "reasonable and probable" mean exactly the same thing: *Baron*, at p. 447.

[32] As an indication that the word "probable" adds nothing to a s. 8 inquiry, one need look no further than the post-*Hunter* revisions to the *Criminal Code* that largely removed all reference to the word "probable" within what used to be common statutory parlance involving "reasonable and probable grounds to believe."[3] In fact, one of the very statutory provisions we are looking at in this case, s. 185(1)(e) itself, underwent post-*Hunter* revision with the removal of the word probable, changing the phrase from "the interception of whose private communications there are <u>reasonable and probable grounds</u> to believe may assist the investigation of the offence" in then s. 178.12(1)(e) to "the interception of whose

---

[3] See, for example, the change in the last paragraph of the definition of "offence" in Part VI; provisions dealing with taking samples of breath and blood in s. 238(3) (later s. 254, now replaced by ss. 320.27, 320.28 and 320.29); provisions dealing with arrest by any person in s. 449(1)(b) (now s. 494(1)(b) and by a peace officer in s. 450 (now s. 495). Though there does not seem to be a formal amendment making this change, as it occurred during consolidation, the change in wording can be seen by comparing the sections in the 1988 and 1989 versions of E.L. Greenspan, *Martin's Criminal Code* (Aurora: Canada Law Book, 1988-1989), the latter of which incorporates R.S.C. 1985.

private communications there are reasonable grounds to believe may assist the investigation of the offence" in s. 185(1)(e) (emphasis added).

[33] Therefore, four decades into our own *Charter* jurisprudence, and long past the removal of "probable" from our search provisions, I elect to use a Canadian-centric shortform – "reasonable grounds to believe" for the test under s. 186(1)(a).

(ii) **Criteria #2 – Investigative necessity (s. 186(1)(b))**

[34] The "investigative necessity" requirement under s. 186(1)(b) is met where the application judge is satisfied that there are "practically speaking, no other reasonable alternative method[s] of investigation, in the circumstances of the particular criminal inquiry": *R. v. Araujo*, 2000 SCC 65, [2000] 2 S.C.R. 992, at paras. 29, 43 (emphasis in original).[4]

[35] It is a well-accepted principle of law that the investigative necessity component of the s. 186(1) test be considered from the perspective of the investigation as a whole, rather than in relation to each individual, place or device named in the authorization: *Araujo*, at para. 29; *R. v. Tahirkheli* (1998), 130 C.C.C. (3d) 19 (Ont. C.A.), at para. 4; *R. v. Nero*, 2016 ONCA 160, 334 C.C.C. (3d) 148, at para. 120, leave to appeal refused, [2016] S.C.C.A. No. 184; *R. v. Pham*, 2002 BCCA 247, 165 C.C.C. (3d) 97, at paras. 93-94; and *R. v. Beauchamp*, 2015

[4] It is not necessary to show investigative necessity when it comes to terrorism and criminal organization offences: see *Criminal Code*, ss. 185(1.1) and 186(1.1).

ONCA 260, 326 C.C.C. (3d) 280, at paras. 100, 119. As will be seen later in these reasons, the global approach to investigative necessity informed the *Mahal* decision.

(b) Contents of the authorization: s. 186(4)

[36] For purposes of this appeal, it is important to also take note of s. 186(4), which dictates the minimum requirements for what an authorization “shall” include. In particular, s. 186(4)(c) requires the judge to specify the identity of persons, “if known”, whose private communications are to be intercepted, as well as, to the extent possible, the description of “place[s]” where interceptions may take place:

> **(4)** An authorization shall
>
> > **(a)** state the offence in respect of which private communications may be intercepted;
> >
> > **(b)** state the type of private communication that may be intercepted;
> >
> > **(c)** <u>state the identity of the persons, if known, whose private communications are to be intercepted, generally describe the place at which private communications may be intercepted, if a general description of that place can be given, and generally describe the manner of interception that may be used</u>;
> >
> > **(d)** contain such terms and conditions as the judge considers advisable in the public interest; and
> >
> > **(e)** be valid for the period, not exceeding sixty days, set out therein. [Emphasis added.]

[37] Important to this appeal is the interrelationship between s. 185(1)(e) and s. 186(4)(c) of the *Criminal Code*. As already noted, at the third-party wiretap

application stage, s. 185(1)(e) provides a clear statutory test predicated on a “may assist” standard for when the name of a person – “if known” – must be provided in the affidavit in support of the authorization. In contrast, when determining who to name in an authorization, s. 186(4)(c) is entirely silent on any threshold test. As for naming “places” where private communications may be intercepted, neither ss. 185(1)(e) nor 186(4)(c) provide for a statutory test.

(c) Practical approach to authorizations: standard forms

[38] For whatever reason, Parliament did not provide standard forms for wiretap applications, affidavits and authorizations.[5] Accordingly, in the wiretap context, standard forms have developed through best practices over time and are widely used throughout Canada, including in this case. A consolidation of these forms is found in the seminal wiretap text, Robert W. Hubbard, Mabel Lai & Daniel Sheppard, *Wiretapping and Other Electronic Surveillance: Law and Procedure* (Toronto: Thomson Reuters, 2022) (loose-leaf) at Appendix 4-12.

[39] Paragraph 3 of the standard third-party wiretap authorization form sets out the “known persons” whose communications may be intercepted. As circumstances require, paragraph 3 will often be subdivided into up to three groups

---

[5] The absence of statutorily created standard forms for wiretaps under Part VI of the *Criminal Code* stands in direct contrast to the standard forms found in Part XXVIII of the *Criminal Code* for many Part XV search warrants, orders and authorizations.

of persons: (1) “Principal Known Persons” found at 3A; (2) “Other Known Persons” found at 3B; and (3) “Unknown Persons” found at 3C.

[40] Generally speaking, principal known persons are those who are the true targets of the wiretap investigation. Other known persons are those who meet the threshold test for naming a person in a wiretap authorization, but who are more peripheral to the wiretap investigation than the principal known persons. And unknown persons are those who are unknown at the time that the authorization issues, but who will almost invariably be captured communicating at places and over devices where interceptions will take place.

[41] While there is no statutory requirement that known persons be subdivided into principal and other known persons (see *Mahal*, at para. 90), this subdivision can be a practical means by which to organize an authorization depending upon its breadth. Not only does it telegraph who the principal targets of the wiretap authorization are, but it allows for a cleaner interaction between clauses within the authorization, more easily facilitating efforts to minimize the risk to privacy.

[42] For instance, given that the 3A category only includes the known persons who are central to the wiretap authorization, it may be that the interception of communications at certain sensitive locations will be limited to only those individuals who fall within category 3A. The first authorization in this case provides a good example of this type of minimization. Paragraph 6(b)(i) of the first

authorization says that interceptions at the appellant's business place had to be "accompanied by live audio monitoring or visual surveillance" and that intercepting had to be "discontinued once it [was] determined that none of the people in [paragraph] 3(a) [were] a party to the communication."

[43] As for places, paragraph 4 of the standard form third-party wiretap authorization lists all places where the interception of private communications may take place. This paragraph is often subdivided into different types of places, such as residences, vehicles, business places and the like.

[44] Although there is no reference to "devices" in ss. 185 or 186, when communications are to be intercepted while making use of devices, such as mobile devices or telecommunication services, they tend not to be listed as places in paragraph 4.[6] Rather, those devices are often identified under their own section at paragraph 5 of the standard form.

[45] Finally, paragraph 6 of the standard form authorization includes terms and conditions that may be considered "advisable" in the circumstances, pursuant to s. 186(4)(d). These terms and conditions are often referred to as "minimization clauses". I will return to this concept later in these reasons.

---

[6] In *R. c. Hernandez*, [2004] J.Q. No. 11285 (C.A.), at para. 25, leave to appeal refused, [2004] C.S.C.R. No. 572, the court found that it was wrong to associate a cellular telephone device with a place. See also *R. v. Papadopoulos*, [2006] O.J. No. 5404 (S.C.), at para. 35. Accordingly, they are dealt with separately as "devices".

[46] With that necessary statutory context in place, I now turn to the parties' and interveners' positions.

IV. SUBMISSIONS

(1) The appellant, Criminal Lawyers' Association and Canadian Civil Liberties Association

[47] The appellant, Criminal Lawyers' Association ("CLA") and Canadian Civil Liberties Association ("CCLA") all emphasize the risk to privacy that modern wiretapping presents. They maintain that given the wide use of new and improved technologies, people have become increasingly susceptible to state surveillance. In their view, an overly lax test for intercepting an individual's private communications presents a more profound risk to individual privacy than ever before. They say that *Mahal* has created just that risk.

[48] Coming into this appeal, the appellant, CLA and CCLA took primary aim at the part of *Mahal* that says that a person can be named in a wiretap authorization on the basis of reasonable grounds to believe that their private communications "may assist" (as opposed to "will assist") the investigation. They maintain that this standard falls short of the minimum constitutional standard articulated by Dickson J. (as he then was) in *Hunter*, at p. 168: reasonable grounds to believe that "an offence has been committed and that there <u>is evidence</u> to be found at the place of the search" (emphasis added).

[49] In support of the argument that *Mahal* is wrong on this point, the appellant, CLA and CCLA lean heavily upon a single paragraph in this court's decision in *Finlay* where Martin J.A. used "will assist" terminology. They say that *Mahal* and *Finlay* simply cannot be reconciled on this point and that *Finlay* should carry the day.

[50] The focus of the appellant's and CLA's (not CCLA's) argument shifted somewhat at the actual hearing of the appeal. While they still maintain that *Mahal* cannot be reconciled with *Finlay*, and that the "may assist" threshold is too low for naming people in authorizations, they concede that their primary concern is no longer with that part of the *Mahal* decision. This is because they have come to embrace the observation of the Attorney General of Ontario ("Ontario"), also an intervener in this appeal, at para. 3 of its factum, that the mere act of naming someone in an authorization, "dictates nothing about how, where or to what extent that person will be intercepted." Accepting the wisdom of that submission, the appellant and CLA now point to other clauses within a wiretap authorization that they argue are the real problem, specifically those that authorize the places and devices where interceptions may take place.

[51] Therefore, the general focus of the appellant's and CLA's constitutional criticism is now not so much about the test for naming known persons, but about the test for naming places and devices. Accordingly, they have shifted their primary focus away from what *Mahal* said about the test for naming known persons, to

what *Mahal* said about the *Hunter*-compliant standard applying only to the authorization as a whole, and not its individual parts. By necessary implication, the appellant and CLA say that this precludes a “will afford” standard being applied to the naming of specific places and devices in an authorization. They contend that this breaches s. 8 of the *Charter* because authorizing places and devices where interceptions may take place is no different than authorizing searches of locations pursuant to a warrant. In other words, just like each location authorized for search requires individualized reasonable grounds to believe that evidence will be found in that location, so too does each place and device authorized for interception*: R. v. Campbell*, 2011 SCC 32, [2011] 2 S.C.R. 549, at para. 15; *R. v. Vu*, 2013 SCC 60, [2013] 3 S.C.R. 657, at para. 51.

[52] Even though there is now a difference between where the appellant, CLA and CCLA place their focus, in the end, I see the overarching constitutional objection as the same. It really comes down to a very simple proposition. Whether training their lens on naming persons, places or devices, the core constitutional objection is that a person’s private communications can be authorized for interception in the absence of individualized grounds. They ask us to overturn *Mahal* on this point.

[53] If we are not prepared to overturn *Mahal* and say that the naming of known persons, places and devices requires individualized grounds, then we are asked to declare ss. 185 and 186 in breach of s. 8 of the *Charter*.

(2) The respondent and Ontario

[54] The respondent and Ontario do not take issue with what the appellant, CLA and CCLA say *Mahal* says. What they take issue with is the suggestion that *Mahal* creates some sort of constitutional conundrum. It is their position that *Mahal* said nothing new. They maintain that *Mahal* is entirely consistent with *Finlay* and numerous other appellate authorities. The respondent in particular leans heavily on the principles of both horizontal and vertical *stare decisis*, arguing that everything that we are being asked to do has already been decided by both this court and the Supreme Court of Canada, and so this court should decline to change anything.

[55] While both the respondent and Ontario accept that third-party wiretap authorizations often result in the invasion of significant privacy interests, they say that the legislation reflects a carefully designed constitutional compromise, one that has survived constitutional attack over many years and for good reason.

V. ANALYSIS

[56] In answering the constitutional complaint, this court must consider what *Mahal* decided, whether it is consistent with prior authority, and whether this court can and should revisit *Mahal* to fix what the appellant, CLA and CCLA say is the constitutional problem created by that case.

(1) What *Mahal* decided

[57] *Mahal* was also a drug trafficking case. Karamjit Mahal appealed from his conviction for heroin trafficking.

[58] Like the appellant, Mr. Mahal was named in a third-party wiretap authorization and his private communications were intercepted pursuant to the authorization. While Mr. Mahal conceded that he met the “may assist” standard, he objected to being described as a principal known person. He argued that to be named a principal “target” of the investigation (as opposed to an “other” known person), there had to exist reasonable grounds to believe that the interception of his communications would assist in the investigation. He argued that the grounds contained in the affidavit fell short of that standard.

[59] Watt J.A. rejected the suggestion that there is a legal difference between principal known and other known persons. As previously discussed, while categorizing known persons in this way may serve practical purposes, the test for naming people in an authorization is the same, regardless of whether the known persons are subcategorized or not.

[60] Watt J.A. started by describing the “may assist” threshold within s. 185(1)(e) as “modest”: *Mahal*, at paras. 71. Leaning on *R. v. Chesson*, [1988] 2 S.C.R. 148, he explained the test as follows: “[p]rovided investigators know the identity of the person and have reasonable … grounds to believe that the interception of that

person’s private communications may assist the investigation of an offence, that person is a ‘known’ for the purposes of s. 185(1)(e)”: at para. 71.

[61] Moving on to the authorization, Watt J.A. concluded that the test for naming a known person is the same as it is at the affidavit stage. In explaining why that is so, Watt J.A. first reasoned that asymmetry in the tests would make no logical sense. He pointed to the inherent logical flaw that would arise from having a fully compliant affidavit, consistent with the requirements of s. 185(1)(e), fail to satisfy the demands for naming a “known” person under s. 186(4)(c). As Watt J.A. aptly put it, “[t]he illogic of the argument betrays its legitimacy”: at para. 87.

[62] Watt J.A. also recognized that to accede to the appellant’s argument would place an irreconcilable wedge between the application of s. 186(1)(a) (the reasonable grounds to believe test) and s. 186(1)(b) (the investigative necessity test). As he explained, it is well established that the investigative necessity test is to be considered from the perspective of the investigation as a whole, as opposed to on a target-by-target or individual-by-individual basis. He reasoned that it would make no sense to eschew individualized grounds when it came to investigative necessity, but then to require them when it came to the best interests of the administration of justice test. As he noted, this is particularly true given that ss. 186(1)(a) and (b) are connected by a conjunctive “and”: *Mahal*, at para. 88.

[63] Therefore, Watt J.A. concluded that, just like the investigative necessity test in s. 186(1)(b), the best interests of the administration of justice test (or reasonable grounds to believe test) in s. 186(1)(a) is looked at from the perspective of the investigation and responding authorization as a whole: are there reasonable grounds to believe that the authorization as a whole will assist in the investigation of the offence?

(2) *Mahal* changed nothing

[64] In my view, *Mahal* says nothing that has not been said before, either in respect of the threshold test for naming known persons or as it relates to the application of the reasonable grounds standard to the authorization as a whole. As I will explain, *Mahal* is consistent with this court's decision in *Finlay*, and subsequent appellate authority.

(a) *Mahal* and *Finlay* are consistent

[65] I start by addressing the suggestion that *Mahal* cannot be reconciled with *Finlay*.

[66] A key issue before the court in *Finlay*, which was decided a year after *Hunter*, was whether the failure to specifically provide a *Hunter*-compliant test for granting a third-party wiretap authorization in what is now s. 186(1)(a) of the *Criminal Code* rendered the statutory scheme unconstitutional. (For ease, I will refer to section numbers that correspond to today's *Criminal Code*.)

[67] In advancing the argument that s. 186 fell constitutionally short of the standard required by s. 8 of the *Charter*, the appellant in *Finlay* pointed to the equivalent legislation in the United States, then s. 2518(3) of Title III of the *Omnibus Crime Control and Safe Streets Act*, 18 U.S.C.A., which had a "probable cause" requirement built in. As s. 186 contained no such requirement, it was said to be deficient.

[68] In addressing that argument, Martin J.A. noted that the proper approach to determining the constitutionality of Part VI was "to consider its provisions and the safeguards … in their entirety" and not to "seize upon individual sections of Part [VI] and to see if those sections, viewed in isolation, contravene the provisions of the *Charter*": at p. 653.

[69] As discussed previously, Martin J.A. rejected the argument that s. 186 was missing a *Hunter*-compliant standard. To the contrary, he concluded that the phrase "best interests of the administration of justice" was, for all intents and purposes, a proxy for *Hunter*: at p. 656.

[70] Martin J.A. explained that while the term "best interests of the administration of justice" is a broad one, incapable of precise definition, it admits of two clearly identifiable elements:

> (a) that the issuing judge be satisfied that "the granting of the authorization will further or advance the objectives of justice"; and

> (b) that the interests of law enforcement and individual personal privacy will be appropriately balanced: *Finlay*, at pp. 654-55.

[71] Drawing on these mutually supportive elements, Martin J.A. concluded that before issuing a third-party wiretap authorization, an application judge must first be satisfied that: (a) there are at least reasonable grounds to believe that a particular offence has been or is being committed,[7] and (b) there are "reasonable ground[s] to believe that communications concerning the particular offence will be obtained through the interception sought": at p. 656. By interpreting s. 186(1)(a) in this manner, and considering it in its full statutory context, Martin J.A. concluded that the statutory scheme was constitutional.

[72] Having already rejected the constitutional challenge, Martin J.A. then went on, at p. 657, in a single paragraph to express some concern over the interception of the private communications of innocent people. It is to this paragraph that the appellant, CLA and CCLA point as proof that *Finlay* and *Mahal* are in conflict. The paragraph, which reads as follows, includes "will assist" language:

> There is, however, one aspect of [Pt. VI] which has given me some concern. It seems clear that, unlike Title III, the private communications of a known person may be the subject of an authorization even though that person is not believed to be involved in the commission of the offence, <u>provided that there are reasonable grounds to believe</u>

[7] Note that since *Finlay*, the jurisprudence has acknowledged that reasonable grounds to believe that an offence "is about to be committed" will also suffice: *R. v. Lucas*, [2009] O.J. No. 2252 (S.C.), at para. 33, aff'd, 2014 ONCA 561, 121 O.R. (3d) 303. See also *R. v. Madrid* (1994), 48 B.C.A.C. 271 (C.A.), at para. 82.

> that the interception of the private communications of that person will assist in the investigation of an offence, e.g., a car rental agency from whom a suspect rents cars to transport drugs. The target of the interception might be entirely innocent but it will assist the police to know when a suspect is renting a car, and he may not use his own telephone to make the necessary arrangements. [Emphasis added.]

[73] The appellant, CLA and CCLA contend that this passage from *Finlay* supports the view that nothing short of individualized reasonable grounds to believe that the interception of a specific individual's private communications "will assist" an investigation can conform to s. 8 requirements. They say that *Mahal* and *Finlay* are in conflict on this point.

[74] While at first blush there appears to be some traction to the argument advanced, when the paragraph is considered in its proper context, the position of the appellant and interveners loses its pull.

[75] I start with the observation that if Martin J.A. had intended to impose an individualized grounds test, he would have done so in more than two passing sentences after already having dismissed the constitutional challenge.

[76] Also, if Martin J.A. had decided that to achieve constitutional compliance it was necessary to have a higher test for naming a person in an authorization than what was required at the application stage, he would have undoubtedly faced that incongruity between application and authorization head-on. This is because, as Watt J.A. noted in *Mahal*, there is a rather obvious logical flaw in the suggestion

that Parliament would set out a threshold test for naming a person in an affidavit in support of an application for a wiretap authorization that would fail to meet the requirements for the authorization.

[77] I have no doubt that Martin J.A., who had earlier in his reasons adverted to the “may assist” threshold in s. 185(1)(e), would have understood the illogic of that position. Had it been his intent to bring this conflict to life, he would have had to have addressed that conflict. Silence on this point speaks volumes.

[78] With that context in mind, I read the passage that the appellant and interveners point to as nothing more than Martin J.A. candidly noting his concern for innocent third parties. I do not read him as attempting to set a constitutional course for naming known persons on a “will assist” standard. He expressed his concern for innocent third parties through the use of a hypothetical. He explains it using “will assist” as plain language, not in reference to the legal standard to be met: after all, if a drug trafficker were to be using a car rental agency to rent cars to transport drugs, it would assist the police to know when that was happening. That is true. Accordingly, I reject the view that *Finlay* requires a “will assist” standard for naming individuals in a wiretap authorization.

[79] As I will now explain, I am bolstered in this conclusion by subsequent authority, since, other than a few lower court decisions along the way,[8] *Finlay* has never been interpreted as the appellant, CLA and CCLA suggest. To the contrary, the Supreme Court of Canada, this court and other appellate courts have affirmed the "may assist" standard for naming individuals in an authorization and have applied the "will assist" standard only to the authorization as a whole.

(3) The Supreme Court of Canada's post-*Finlay* case law

[80] I begin by reviewing a trilogy of cases that undercut the argument put by the appellant and interveners.

(a) *Chesson*

[81] *R. v. Chesson*, [1988] 2 S.C.R. 148, was decided in the wake of *Finlay*. The appellants in that case were jointly charged along with several others with conspiracy to commit robbery and kidnapping.

[82] The appellant, Lorelei Vanweenan, objected to the fact that she had been intercepted under a third-party wiretap authorization in which she had <u>not</u> been named. She claimed that the police had sufficient information to cloak her in "known" status at the time that the authorization was applied for and therefore, she

---

[8] See e.g., *R. v. Chung* (2008), 231 C.C.C. (3d) 484 (Ont. S.C.), at paras. 23-26, *R v. Ahmad*, 2010 ONSC 123, at para. 14; *R. v. Adam*, 2006 BCSC 126, at paras. 10-11, 14; *R. c. Rubin*, 2011 QCCQ 14895, at para. 43; and *R. v. Oliynyk et al.*, 2005 BCSC 1895, at para. 19.

should have been named as a known person. She argued that the failure to do so meant that her private communications should be excluded from evidence at trial.[9]

[83] In engaging with Ms. Vanweenan's argument, the court addressed the threshold test for naming someone in a wiretap authorization. On behalf of the court, McIntyre J. noted that s. 185(1)(e) contains two prerequisites to naming a person in an application, the same ones that Watt J.A. noted in *Mahal*: (a) the person must be known to the police; and (b) there must exist reasonable grounds to believe that the person's private communications <u>may assist</u> the investigation of the offence. McIntyre J. concluded that where these prerequisites are met, the person is a known person and must, therefore, be named in the authorization: p. 164. Accordingly, *Chesson* aligned the statutory test for naming a person at the application stage with the same test for naming them in the authorization.

[84] What can we make of *Chesson* in terms of the issue on this appeal? We are encouraged to largely ignore the decision because *Chesson* is not a constitutional case and so did not confront the issue with which we are faced. While it is true that *Chesson* did not address the constitutional issue, I do not find this fact persuasive in terms of its import to this appeal.

[9] At the time, s. 178.16(1) of the *Criminal Code* gave rise to an automatic exclusionary rule when it came to unlawfully intercepted communications pursuant to s. 189(1). That provision was later revoked: *An Act to amend the Criminal Code, the Crown Liability and Proceedings Act and the Radiocommunication Act*, S.C. 1993, c. C-40, s. 10(1). Today, questions of admissibility for unauthorized interceptions are dealt with pursuant to s. 24(2) of the *Charter*.

[85] I start by noting that in the 35 years following *Chesson*, the Supreme Court has never backtracked on the idea that the test for naming a person at the application stage and the test for naming them in the authorization are the same.

[86] I also observe that it is hard to imagine that the *Chesson* court did not at least turn its mind to constitutional principles when explaining when a person not only can be, but has to be, named in an authorization. After all, *Finlay* was the first case in Canada to address the constitutionality of what is now Part VI of the *Criminal Code*. And it had been decided not long before *Chesson* was decided. Surely if the *Chesson* court thought that *Finlay* had imposed a higher "will assist" standard to meet the minimum constitutional requirements of s. 8 of the *Charter*, the court would have at least adverted to the issue. Yet there is not a hint of this in *Chesson* or elsewhere. Again, silence speaks volumes.

[87] In sum, *Mahal* and *Chesson* are consistent.

(b) *Duarte*

[88] *R. v. Duarte*, [1990] 1 S.C.R. 30, is also a case involving drug trafficking and the use of electronic surveillance. In my view, it provides clear support for the *Mahal* observation that s. 186(1)(a) – the best interests of the administration of justice test – operates like the investigative necessity test, applying to the investigation and authorization as a whole and not on an individual-by-individual/place-by-place/device-by-device basis.

[89] The core question to be decided in *Duarte* was whether the constitutional right to be secure against unreasonable search and seizure required police to seek prior judicial authorization before engaging in participant surveillance, meaning where a consenting person is a party to the intercepted communication. In answering that question, La Forest J. expressly adopted Martin J.A.'s observation in *Finlay* that the "best interests of the administration of justice" test in s. 186(1)(a) imports a minimum constitutional requirement that the application judge must be satisfied upon "reasonable … grounds to believe that an offence has been, or is being, committed and that the authorization sought will afford evidence of that offence": at p. 45 (emphasis added). This passage from *Duarte* provides direct support for the *Mahal* statement that the reasonable grounds to believe test is applied to the whole of the authorization (the "authorization sought").

[90] The appellant, CLA and CCLA suggest that there is another passage in *Duarte* that undercuts that global approach. In particular, they point to a passage where La Forest J. posited an individual being able to "call the state to account if he can establish that a given interception was not authorized in accordance with the requisite standard": at p. 46 (emphasis added). I do not read this passage as suggesting that there need be individualized grounds in relation to a person, a place or a device or even a "given interception". To the contrary, I read it as affirming that all interceptions must be made in accordance with the "requisite standard" as a whole: "reasonable … grounds to believe that an offence has been,

or is being, committed and that the authorization sought will afford evidence of that offence”: *Duarte*, at p. 45 (emphasis added).

[91] I would make one further observation. If the *Duarte* court had intended to impose an individualized grounds test for naming known persons, the court would have most certainly had to resolve and, indeed, correct what had been said just a year earlier in *Chesson*. Yet the court was silent on *Chesson* because there was no conflict between the decisions. There was no conflict because, as *Mahal* states, the reasonable grounds to believe standard operates in relation to the authorization as a whole, and not in relation to each named person — or, as applied to the arguments raised by the appellant and CLA, each named place or device.

(c) *Garofoli*

[92] Then along came *Garofoli.* It too was a drug case where the evidence largely came from the interception of private communications pursuant to wiretap authorizations. It addressed two concepts that are supportive of *Mahal*.

[93] First, it adopted *Duarte* (which adopted *Finlay*) in relation to the idea that there need only be reasonable grounds to believe that “the authorization sought will afford evidence of that offence”: at p.1444 (emphasis added), citing *Duarte*, at p. 45. Thus, for a second time in short order, the Supreme Court affirmed the global approach to the reasonable grounds to believe standard — that it applies to the issuance of the authorization as a whole.

[94] Second, *Garofoli* referred to and accepted *Chesson.* Specifically, at p. 1445, the court in *Garofoli* noted that third-party wiretap authorizations can be attacked on multiple bases, including "*Vanweenan* hearing[s]". In describing that type of hearing, the court specifically adopted *Chesson*, saying that it was designed to determine whether the authorization names all known persons "as required by [now ss. 185(1)(e) and 186(4)(c)]." Therefore, *Garofoli*, which at its core was a constitutional case, pushed the legitimacy of *Chesson* forward.

[95] The court has never changed course.

(d) What Supreme Court case law tells us

[96] So, where does this jurisprudential tour leave us? We have *Chesson* imposing a "may assist" threshold for naming a person in an authorization. We also have *Chesson* showing no concern over conflict with *Finlay*. In addition, we have *Duarte* adopting *Finlay* and reinforcing the global approach to the reasonable grounds to believe test for purposes of s. 186(1)(a). And we have *Garofoli* adopting *Duarte*, which adopted *Finlay*, on the same point, as well as *Garofoli* adopting *Chesson.* Therefore, on my reading, *Mahal* is consistent with *Finlay*, *Chesson*, *Duarte* and *Garofoli.* That is a formidable body of jurisprudence.

[97] The appellant points to one other Supreme Court authority that he maintains supports him in pursuit of individualized grounds: *R. v. Thompson*, [1990] 2 S.C.R. 1111. The appellant leans on passages where Sopinka J. suggested that before

the police could intercept a known person at a location to which they “resorted” (as opposed to a place named in the authorization), the police first had to have reasonable grounds to believe that the person would in fact resort to that location: at p. 1139. On this basis, the appellant maintains that *Thompson* supports his claim that naming places and devices in a wiretap authorization, like naming locations of search in a search warrant, require individualized reasonable grounds to believe that evidence will be found at that location.

[98] In my view, *Thompson* is of no assistance to the appellant’s position, as *Thompson* involved an entirely different wiretapping issue than what we are confronted with here.

[99] In third-party wiretap authorizations, there will often be a standard “resort to” clause: see e.g., Hubbard, at Appendix 4-12, para. 4E. Indeed, there was a resort to clause in this case at para. 4(d) of the first authorization. In essence, a resort to clause ensures that if a place or device not listed in the authorization is “resorted to” by a known person (typically a principal known person) while the authorization is in effect, the interceptions of private communications can continue at that resorted to location.

[100] Where Sopinka J. refers in *Thompson* to the need for the police to have reasonable grounds to believe that a known person will resort to the subject location, he is addressing a situation where there is no prior judicial authorization

for the place or device resorted to. One of the constitutional attacks in *Thompson* was that resort to clauses unconstitutionally usurp the judicial function, granting the police the power to decide where interceptions may take place. Ultimately, that constitutional objection was rejected, but on the basis that when this extraordinary, delegated power is exercised by the police, they must have reasonable grounds to believe that that a known person will resort to the place or device in question.

[101] In short, *Thompson* does not invoke a "will assist" test for purposes of actually naming places and devices in an authorization.

(4) Other pre-*Mahal* authority

[102] It also bears mentioning that this court's pre-*Mahal* authority lines up behind my reading of *Finlay* and is also entirely consistent with *Mahal.* I will point to two significant judgments from this court that pre-date *Mahal*.[10]

[103] The first is *R. v. Schreinert* (2002), 159 O.A.C. 174 (C.A.), where Simmons J.A. reinforced that the threshold for naming a "known" party is a "low one", involving reasonable grounds to believe that that the "interception of that party's

---

[10] As for other provincial appellate courts, the New Brunswick Court of Appeal reinforced the *Chesson* "may assist" standard for naming a person in an authorization: *R. v. Doiron*, 2007 NBCA 41, 221 C.C.C. (3d) 97, at paras. 51-53, leave to appeal refused, 333 N.B.R. (2d) 429 (S.C.C.). So too did the Alberta Court of Appeal in *R. v. Abdo* (1988), 93 A.R. 115 (C.A.), at paras. 2, 5, and the British Columbia Court of Appeal in *R. v. Mapara*, 2003 BCCA 131, 180 C.C.C. (3d) 184, at para. 61, aff'd 2005 SCC 32, [2005] 1 S.C.R. 358; 2005 SCC 24, [2005] 1 S.C.R. 384, and *R. v. Mooring*, 1999 BCCA 418, 137 C.C.C. (3d) 324, at paras. 36-37. These are also pre-*Mahal* decisions.

communications *may* assist in the investigation of an offence": at para. 43 (emphasis in original).

[104] The second is *R. v. Nugent* (2005), 193 C.C.C. (3d) 191 (Ont. C.A.), where Doherty J.A. reinforced the same thing, saying that the trial judge had erred by imposing too high a threshold when considering whether Phillip Nugent should have been named in the authorization. Instead of looking to whether Mr. Nugent was a party to the alleged offence, the trial judge "should have considered whether that information provided reasonable grounds to conclude that the interception of Nugent's communications <u>could assist</u> in the investigation": at para. 9 (emphasis added).

(d) There is no basis to revisit *Mahal*

(i) Stare decisis

[105] As has been shown, *Mahal* said nothing new. It is entirely consistent with prior authority, including prior Supreme Court authority. Thus, effectively, we are not only being asked to overturn multiple decisions of this court, including *Mahal*, but we are also being asked to depart from Supreme Court authority. In these circumstances, I need only address vertical *stare decisis*.

[106] It is not open to this court to depart from Supreme Court authority except in exceptional circumstances. The Supreme Court explained those exceptions in

Canada (Attorney General) v. Bedford, 2013 SCC 72, [2013] 3 S.C.R. 1101, at para. 42:

> In my view, a trial judge can consider and decide arguments based on *Charter* provisions that were not raised in the earlier case; this constitutes a new legal issue. Similarly, the matter may be revisited if new legal issues are raised as a consequence of significant developments in the law, or if there is a change in the circumstances or evidence that fundamentally shifts the parameters of the debate.

[107] Those exceptions do not apply in this case. No new *Charter* provisions are raised in this case. There have not been significant changes in the law: *Hunter* is still good law and *Finlay*, which applies *Hunter*, has stood the test of time, having been given the stamp of approval by the Supreme Court of Canada. While the appellants, CLA and CCLA argue that this court should respond to an increase in the use of electronic communications and the new technologies available to intercept such communications, I do not see those changes as supporting the change in the law that they seek.

[108] As I will explain, the law as it has stood since 1985, and as articulated in *Mahal*, continues to make constitutional and practical sense. Therefore, I would not overturn *Mahal*. Nor would I find ss. 185 or 186 unconstitutional because of how *Mahal* has interpreted them.

(ii) The third-party wiretap scheme continues to strike the appropriate balance

[109] To determine whether an appropriate constitutional balance has been struck for purposes of s. 8 of the *Charter*, one cannot consider only one aspect of the statutory scheme. Rather, the proper approach is to consider the provisions and safeguards in their full context: *Araujo*, at para. 26; *Finlay*, at p. 653; see also *Wakeling v. United States of America*, 2014 SCC 72, [2014] 3 S.C.R. 549, at para. 67. Two important aspects of that context are the rigorous statutory safeguards unique to the third-party wiretap scheme and the distinct, prospective nature of third-party wiretap authorizations themselves. It is also important to understand, with the benefit of a practical lens, why the standard for naming a person, place or device has evolved as it has.

Rigorous safeguards

[110] For many decades now there has been a concern about the use of intrusive surveillance technologies and their impact on citizens' privacy: *R. v. Jones*, 2017 SCC 60, [2017] 2 S.C.R. 696, at para. 73, citing *Duarte*, at pp. 43-44. There is an understandable fear that if law enforcement is equipped with sophisticated, modern surveillance technologies and the use of those technologies is left uncontrolled, there exists a real potential to "annihilate privacy": *Jones*, at para. 74, quoting *R. v. Wong*, [1990] 3 S.C.R. 36, at p. 47.

[111] In the course of acknowledging these concerns, the courts have repeatedly recognized the strength of Part VI of the *Criminal Code* when it comes to protecting privacy. The fact is that Part VI does not leave things “uncontrolled.” To the contrary, as recognized in *Jones*, there exist “heightened safeguards” in Part VI, all of which are imposed to address the “dangers created by prospective authorizations”. Those safeguards lead to what has been described as an application process for third-party wiretap authorizations that is “the most exacting pre-trial investigative proceeding known to our criminal law’”: *Jones*, at para. 74. citing S.C. Hutchinson et al., *Search and Seizure Law in Canada* (loose-leaf), vol. 1, at p. 4-37. See also: *R. v. Telus Communications*, 2013 SCC 16, [2013] 2 S.C.R. 3, at paras. 71-73.

[112] Some of the safeguards have already been mentioned in these reasons. However, it is worth reviewing the broad array of safeguards to ensure an accurate picture of the context within which to consider the constitutional complaint in this case is brought. These safeguards include:

1) **Who may issue an authorization**: A third-party wiretap authorization can only be granted by a Superior Court judge or a s. 552 judge, which stands in direct contrast to most other search-related provisions in the *Criminal Code* (s. 185(1)). As explained in *Araujo*, at para. 29, “the authorizing judge stands as the guardian of the law and of the constitutional principles protecting privacy interests”.

2) **Who may bring an application for authorization**: Unlike other search provisions, applications may only be

brought by specifically designated agents, typically Crown counsel, who must be designated in writing by either their respective Attorney or Deputy Attorney General (generally those matters prosecuted by the province) or the Minister or Deputy Minister of Public Safety and Emergency Preparedness (generally those matters prosecuted by the federal Crown) (s. 185(1)(a) and (b)).

3) **Stringent threshold for granting an authorization**: As discussed, before an authorization is granted, the application judge must be satisfied that it is in the best interests of the administration of justice and that, subject to few exceptions, there must be investigative necessity (ss. 186(1)(a) and (b), (1.1)).

4) **Authorizations limited to specified offences**: Unlike other search provisions, authorizations are limited to the investigation of "offences" specifically enumerated under s. 183, which are generally considered to be the most serious offences in the *Criminal Code* and a few other Acts (ss. 183, 186(4)(a)).

5) **Disclosure of prior applications**: Unlike other search provisions, any prior application must be disclosed in the affidavit in support of the authorization (s. 185(1)(f)).

6) **Imposition of terms and conditions**: Unlike other search provisions, the application judge considering the application has the express statutory power to limit the sphere of the authorization, including its extent and the manner of its execution, through terms and conditions the judge considers advisable in the public interest (s. 186(4)(d)). As explained in *Araujo*, at para. 29, the crafting of appropriate terms and conditions is an important part of the application judge's role:

> The judge should not view himself or herself as a mere rubber stamp, but should take a close look at the material submitted by the applicant. He or she should not be reluctant to ask questions from the applicant, to discuss or to require more information or to

> narrow down the authorization requested if it seems too wide or too vague. The authorizing judge should grant the authorization only as far as need is demonstrated by the material submitted by the applicant.

While imposing terms and conditions is not statutorily mandated, the failure to impose appropriate terms and conditions may result in a finding of a s. 8 *Charter* breach: see e.g., *Thompson*, at p. 1145.

7) **Protection of privileged information:** Unlike other search provisions, solicitor-client communications are expressly protected in different ways and all information that would have been protected by privilege, but for an interception, remains privileged and inadmissible as evidence without the consent of the person who enjoys the privilege (ss. 186(2), 189(6)).

8) **Notice of intention to adduce intercepted communication into evidence**: Reasonable notice must be provided before an intercepted private communication can be admitted into evidence at trial (s. 189(5)(a)).

9) **Offence to knowingly intercept**: The knowing interception of a private communication in certain delineated ways constitutes an indictable offence unless done in accordance with a saving provision, which includes interceptions done in accordance with an authorization (s. 184(1) and (2)).

10) **Offence to disclose intercepted communications**: It is an offence to disclose a private communication intercepted under an authorization except in accordance with certain statutory exceptions (ss. 193 (1) – (3), 193.1 (1)-(2)).

11) **Public reporting**: The Minister of Public Safety and Emergency Preparedness “shall”, as soon as possible at the end of each year, publish a report that references certain information related to the use of electronic

surveillance, including the number of third-party authorizations, as well as certain information about the content of those authorizations (s. 195(1)-(5)).

12) **Notice to those who have been intercepted**: Written notice must be provided to those who have been the "object" of a third-party wiretap authorization (s. 196(1)-(5) and s. 196.1(1)).

[113] As this list of safeguards reveals, the statutory scheme governing third-party wiretap authorizations offers the most robust set of protections for any search-related scheme in the *Criminal Code*.

[114] An authorization cannot even issue until the judge is satisfied that the investigation into a serious criminal offence has for all intents and purposes stalled and that there exist reasonable grounds to believe that the authorization as a whole will assist in the investigation of that offence. Only then does the scalpel come out to craft the contents of the authorization.

[115] Adding to the strength of privacy protections is the fact that: applications have been taken out of the hands of police officers and placed into the hands of specially designated lawyers; applications have been taken out of the hands of all but superior court judges; intercepted communications are automatically shrouded in protection from disclosure except where strict statutory provisions are met; privilege cannot be pierced by an interception; and much more. Taken together, these protections reflect an exquisite balance that defines the concept of reasonableness under s. 8 of the *Charter*: a balance between protecting the very

legitimate interest in protecting privacy, with the also very legitimate interest in protecting the safety and security of the community through the suppression of crime: *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at para. 17; *Hunter*, at pp. 159-60; and *R. v. Edwards*, [1996] 2 S.C.R. 128, at para. 30.[11]

The unique nature of third-party wiretap authorizations

[116] Another important contextual factor informing why *Mahal* (and the cases from which it evolves) makes sense is the unique nature of third-party wiretap authorizations.

[117] The fact is that there are "substantial differences" between third-party wiretap authorizations and search warrants: *Finlay*, at p. 648. For the most part, search warrants are single-entry authorizations that permit a location to be searched for a particular, pre-defined thing that is already in existence. The value of that pre-existing thing to the investigation is easy to articulate because it already exists or at least is reasonably believed to exist.

[118] In contrast, third-party wiretap authorizations are entirely prospective in nature, anticipating conversations and communications that have not yet occurred,

---

[11] In response to the appellant, CLA and CCLA's concerns about the risks posed to privacy interests with greater technological abilities, I would also point out that technological advances can also hinder police investigations by making it easier to evade surveillance. The rise in encryption is a good example. Over 70% of communications lawfully intercepted by the RCMP use some form of encryption: Pam Dheri and Dave Cobey, "Lawful Access & Encryption in Canada: A Policy Framework Proposal" (2020) 68 C.L.Q. 430, at p. 436. The point is that technological improvements cut both ways.

and so their content remains to be seen in the future, as does the determination of the investigative value of those communications. As Martin J.A. explained in *Finlay*, at p. 648, quoting from C.S. Fishman, *Wiretapping and Eavesdropping* (1978), at pp. 6-11, this results in unknowns:

> The interception may occur at any time during the period specified in the authorization. It will often be the case that the listener will not be able to determine whether the intercepted conversation constitutes the evidence sought until after he has heard it in its entirety in the context of other conversations similarly overheard.

[119] Therefore, wiretaps are necessarily future-looking and somewhat provisional by nature. Section 185(1)(e) is the only place where the "may assist" standard for a search provision appears in the *Criminal Code* because it is the only section dealing with prospective interceptions. What happens into the future will depend on many uncertain moving parts, often including the ability of the police to covertly encourage communications. Pepall J.A. captured this well in *R. v. July*, 2020 ONCA 492, 152 O.R. (3d) 1, when she said, at para. 64:

> Wiretaps are sweeping in their reach and target future communications based on an investigative theory that conversations relevant to an offence will take place. With a wiretap, the words sought for capture do not exist at the time the authorization is granted. They may never exist. The wiretap may fail to disclose anything of relevance to any offence under investigation. By their nature, the subject-matter sought — communications about an offence — is speculative[.] [Citation omitted.]

[120] I agree. And it is the forward-looking, somewhat uncertain nature of what might come to be in the future that invites the “may assist” standard.

The may assist standard does not operate on suspicion

[121] It is also important to address the suggestion that has been made in some of the submissions in this case that the test for naming a known person – reasonable grounds to believe that the interception of their communications may assist the investigation – operates on a standard of suspicion. It does not. Indeed, to suggest that the test operates on a suspicion threshold is to read the words “reasonable grounds to believe” out of the test.

[122] The jurisprudence has made clear that “reasonable grounds to believe” and “reasonable grounds to suspect” are entirely different threshold tests, the former operating on the level of credibly-based probability and the latter operating on the level of reasonable possibilities: *Hunter*, at p. 167; *R. v. Chehil*, 2013 SCC 49, [2013] 3 S.C.R. 220, at para. 27; *R. v. A.M.*, 2008 SCC 19, [2008] 1 S.C.R. 569, at paras. 77-80; and *R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456, at para. 75.

[123] The test for naming a known person is rooted in credibly-based probability that future communications may assist the investigation. The “may assist” component is simply a nod to the fact that the nature of the thing that may assist cannot be known at the time of the application.

[124] This is why, as Doherty J.A. described in *Nugent*, at para. 9, the authorizing judge must focus upon whether the affidavit provides a “sufficient link” between the named target and the offences charged or others involved in the investigation to conclude whether the interception of their communications could assist in the investigation of the offences. See also *R. v. Brown*, 2019 ONSC 5615, at paras. 63, 66; *R. v. Brammall*, 2019 ONSC 7334, at para. 75; and *R. v. Montgomery*, 2016 BCCA 379, 341 C.C.C. (3d) 147, at paras. 81, 91. I adopt that terminology as a nice summary of the threshold test for naming a known person.

[125] While neither ss. 185(1)(e) or 186(4)(c) contain a statutory threshold test for the naming of a “place at which private communications [of named persons] may be intercepted”, the “where” is simply determined by the strength of connection between the named person (who has already met the threshold test for a known person) and the place or device where that person’s communications may take place. Ontario suggests that the test is really the same as for naming a known person, only modified to meet the circumstances: reasonable grounds to believe that the known person’s communications may be intercepted at the place or on the device named. I agree.

The importance of third-party wiretaps as an investigative tool

[126] The final contextual factor that I would highlight in terms of why the law has developed as it has and should not be disrupted, is that third-party wiretap authorizations are an important investigative tool of essentially last resort in the midst

of very serious criminal conduct. Doing as Martin J.A. did in *Finlay*, as the Supreme Court did in *Chesson*, *Duarte* and *Garofoli*, and as this court has done in *Schreinert*, *Nugent* and *Mahal*, all set against the backdrop of such a robust statutory scheme, has ensured the right constitutional balance.

[127] An example helps illustrate the point as to why the current standard for naming known persons, places and devices in an authorization makes practical sense, and how, conversely a “will assist” standard on an individualized basis could unduly hamper police investigations. Imagine that a child is abducted, and the family awaits a ransom call. While the police have reasonable grounds to believe a call <u>will</u> come through, it <u>may</u> come through to any one of a number of family members at any number of places or on any number of different devices. Doing as the appellant, CLA and CCLA request, and applying a “will assist” standard to each person, place and device would undermine the use of a s. 186 authorization as an investigative technique in that situation. This is precisely why, as Watt J.A. reinforced in *Mahal*, the reasonable grounds to believe standard applies to the investigation and authorization as a whole and not to its individual parts.

[128] I agree.

VI. CONCLUSION

[129] In conclusion, *Mahal* said nothing new. It is consistent with *Finlay* and other decisions of this court. It followed binding Supreme Court authority. And it makes practical sense and conforms with s. 8 of the *Charter*.

DISPOSITION

[130] For these reasons, I would dismiss the appeal.

J.M.F.

Released: September 28, 2023

Fairburn ACJO

I agree Doherty JA

I agree K. Feldman J.A.

I agree. S.E. Pepall JA

I agree G. Pardu J.A.