Court File No. C67423

COURT OF APPEAL FOR ONTARIO

B E T W E E N:

HIS MAJESTY THE KING

Respondent

and

TEMORSHAH HAFIZI

Appellant

and

ATTORNEY GENERAL FOR ONTARIO, CANADIAN CIVIL LIBERTIES ASSOCIATION and CRIMINAL LAWYERS' ASSOCIATION

Interveners

FACTUM OF THE INTERVENER, CANADIAN CIVIL LIBERTIES ASSOCIATION

STOCKWOODS LLP
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Nader R. Hasan (54693W)
Tel: 416-593-1668
naderh@stockwoods.ca

Spencer Bass (75881S)
Tel: 416-593-1657
spencerb@stockwoods.ca

Tel: 416-593-7200
Fax: 416-593-9345

Lawyers for the Intervener,
Canadian Civil Liberties Association

TO: **AGP LLP**
Barristers
116 Lisgar Street, Suite 200
Ottawa, Ontario K2P 0C2

Howard L. Krongold (51332N)
Tel: 613-235-9779
Fax: 613-235-8317
howard@agpllp.ca

Lawyers for the Appellant
Temorshah Hafizi

AND TO: **PUBLIC PROSECUTION SERVICE OF CANADA**
160 Elgin St, Suite 1400
Ottawa, ON K2P 2P7

Allyson Ratsoy/James D. Sutton
Tel: 613-941-6656
Fax: 613-957-9043
allyson.ratsoy@ppsc-sppc.gc.ca
james.sutton@ppsc-sppc.gc.ca

Lawyers for the Respondent

AND TO: **MINISTRY OF THE ATTORNEY GENERAL OF ONTARIO**
Crown Law Office (Criminal)
720 Bay Street, 10th Floor
Toronto ON M7A 2S9

Emily Marrocco
Tel: 416-326-4600
Fax: 416-326-4656
emily.marrocco@ontario.ca

Lawyers for the Intervener, Attorney General of Ontario

AND TO: **BRAUTI THORNING LLP**
161 Bay Street
Suite 2900
Toronto ON M5J 2S1

Michael Lacy
Tel: 416-360-2776
Fax: 416-362-8410
mlacy@btlegal.ca

Bryan Badali
Tel: 416-360-2777
Fax: 416-362-8410
bbadali@btlegal.ca

Sara Little
Tel: 416-360-2774
Fax: 416-362-8410
slittle@btlegal.ca

Lawyers for the Intervener, Criminal Lawyers' Association

PART I - OVERVIEW

1. This case raises fundamental issues about the privacy that individuals can reasonably expect in their communications. At issue in this case is the minimum evidentiary standard required for law enforcement to use highly invasive surveillance techniques on individuals who are not the actual target of the investigation but are merely "known persons".

2. The Supreme Court has repeatedly emphasized that new technologies have "the potential, if left unregulated, to annihilate any expectation that our communications will remain private".[1]

3. The Court has also underscored that this risk is heightened when it comes to surveillance techniques authorized by Part VI of the *Criminal Code*. The s. 8 *Charter* jurisprudence and the case law interpreting Part VI have reflected an understanding that the evidentiary threshold required to authorize that particular investigative technique must be proportionate to its invasiveness. One minimum safeguard for Canadians to tolerate significant incursions into individual privacy in the name of law enforcement is a demonstrable justification for those invasive searches on a probability-based standard.

4. However, as a result of this Court's decision in *R. v. Mahal*,[2] a dangerous lacuna has emerged in the case law — one that needs correcting. In *Mahal*, this Court held that a Part VI authorization — long considered one of the most invasive investigative techniques known to our laws — can be expanded to target an additional person if intercepting those communications merely "***may assist***" an investigation. Thus, if there are proper grounds to intercept one person's communications, police can expand their search to target additional persons without reasonable grounds to believe that those added interceptions "***will afford***" evidence of an offence.

---

[1] *R. v. Duarte*, [1990] 1 S.C.R. 30, at p. 44.
[2] 2012 ONCA 673.

5. The "may assist" standard is rudderless and open to fishing expeditions. The *Mahal* standard thus leaves individuals acutely vulnerable to highly invasive surveillance without the important safeguards ordinarily required under s. 8.

6. This concern is not merely academic. The *Mahal* standard has already had a deeply unfair impact on the privacy rights of Ontarians. The lower courts' jurisprudence following *Mahal* demonstrates a willingness to employ this standard to permit invasive searches of the communications of third parties with little actual connection to the offence or target being investigated. This state of affairs undermines the careful balance between privacy protection and law enforcement that our courts have so assiduously fostered over the past forty years.

7. Further, the potential impacts of this Court's decision in this case are even more wide-ranging as they relate to police investigative tactics that engage new technological capabilities, such as On-Device Investigative Tools ("ODITs"), which allow police to turn the target's smart phone against them, converting it into a 24/7 listening and viewing spy-cam for police.

PART II - FACTS

8. The CCLA takes no position on the facts of this case.

PART III - ISSUES

9. This appeal is about the constitutional minimum standard for issuing an authorization to intercept private communications of a "known person" under Part VI of the *Criminal Code*. The CCLA submits that the evidentiary standard from *Mahal* violates s. 8 of the *Charter*.

PART IV - ANALYSIS

A. *MAHAL* IS INCONSISTENT WITH SECTION 8'S NORMATIVE FRAMEWORK

10. The *Mahal* standard is inconsistent with the normative framework that the Supreme Court of Canada has established over four decades of *Charter* jurisprudence. Simply put, the *Mahal* standard creates a low, and unconstitutional, evidentiary threshold for a highly invasive search.

(i) Section 8's Protections Are Proportionate to the Invasiveness of the Investigative Technique

11. The Supreme Court has repeatedly stressed that the analysis under s. 8 is a normative one.[3] In accordance with this normative framework, the Court has consistently recognized that the evidentiary standard necessary to satisfy the minimum constitutional requirements under s. 8 must be proportionate to the nature of the proposed privacy invasion involved.

12. In *Hunter v. Southam*, the Supreme Court's seminal pronouncement on the evidentiary threshold for s. 8 of the *Charter*, Dickson J. (as he then was) held that s. 8 required judicial pre-authorization based on "reasonable and probable grounds, established upon oath, to believe that an offence has been committed and that there is evidence to be found at the place of the search".[4] "Reasonable and probable grounds" is a meaningful standard. It refers to the "point where credibility-based probability replaces suspicion."[5] Dickson J. explained that the standard — what would come to be known as the *Hunter v. Southam* standard — "constitutes the minimum standard, consistent with s. 8 of the Charter, for authorizing search and seizure".[6]

13. *Hunter* dealt with the constitutional minimum standards for searches of a place and seizure of items found within that place. Some years later, however, the Supreme Court grappled with the highly intrusive nature of wiretaps. In *R. v. Duarte*, the Court noted that the interception of private communications "has the potential, if left unregulated, to annihilate any expectation that our

---

[3] *R. v. Jarvis*, 2019 SCC 10, at para. 68; *R. v. Spencer*, 2014 SCC 43, at para. 18; *R. v. Tessling*, 2004 SCC 67, at para. 42. See also: *R. v. Dosanjh*, 2022 ONCA 689, at para. 133.
[4] *Hunter et al. v. Southam Inc.*, [1984] 2 S.C.R. 145, at p. 168.
[5] *Hunter*, at 167-168.
[6] *Hunter*, at p. 168.

communications will remain private".[7] Wiretap technologies "affect human relations in the sphere of very close, if not intimate communications, even in the privacy of the home",[8] and "pose heightened privacy concerns beyond those inherent in other searches and seizures".[9]

14. In *Garofoli* and *Duarte*, both decided in 1990, the Supreme Court held that the minimum reasonable-and-probable-grounds standard from *Hunter* applied to wiretap authorizations. In *Garofoli*, Sopinka J. explained that "[s]ince wiretaps are considered to be more intrusive on the privacy of individuals than searches of premises, there is no reason to consider applying lesser minimum requirements to them".[10]

15. In *Duarte*, La Forest J. explained that this constitutional minimum standard "must be taken to afford protection against the arbitrary recording of private communications ***every time we speak*** in the expectation that our words will be heard only by the person or persons to whom we direct our remarks".[11] *Duarte* established that the constitutional standard of judicial pre-authorization based on reasonable grounds to believe that the wiretap will afford evidence of an offence must apply to *all* wiretaps (*i.e.* "every time we speak") — regardless of the subject of the search.

16. As reflected in the Supreme Court's jurisprudence, at the heart of Part VI lies the recognition that its investigative techniques are more intrusive than the powers of search and seizure found elsewhere in the *Criminal Code*. As such, its statutory prerequisites were intended to be more stringent. In addition to the *Hunter* probable cause requirement, the issuing judge must also be satisfied that there is no other reasonable alternative method of investigation to achieve the investigative goals in the circumstances.[12]

---

[7] *Duarte*, at p. 44.
[8] *R. v. Araujo*, 2000 SCC 65, at para. 21.
[9] *Wakeling v. United States of America*, 2014 SCC 72, at para. 38.
[10] *R. v. Garofoli*, [1990] 2 S.C.R. 1421, at p. 1444.
[11] *Duarte*, at p. 47 (emphasis added).
[12] *Criminal Code*, s. 186(1)(b).

17. In subsequent years, the Supreme Court has acknowledged that new technologies pose unique challenges for privacy protection. It has consistently sought to ensure that, regardless of the ways in which surveillance is newly enabled by evolving technologies, the necessary, principled balance between individual privacy and state interests required by the *Charter* is upheld. Part of the Court's nuanced and careful response to these challenges has been to consistently hold that stringent standards of judicial pre-authorization apply to searches of computers or other electronic devices,[13] searches of text messages on the recipient's phone,[14] prospective production of future text messages,[15] retrospective production of historical text messages,[16] and production of subscriber information for particular IP addresses.[17] In many cases, the Supreme Court has bolstered existing standards, or put in place new protections, to respond to new technological threats to privacy.[18] In each of these instances, the Court reached its conclusion through a consideration of the invasiveness of the search and the nature of the privacy interests at stake.

18. As these cases demonstrate, the Supreme Court has applied s. 8's normative privacy framework in a teleological progression directed towards maintaining strong privacy protections for individuals despite the evolving digitization and networked nature of our communications. As the invasiveness of investigative techniques have increased because of emerging technologies, the law of constitutionally-protected privacy under s. 8 has had to keep up (even if it sometimes lags a few years behind). Canadians should be able to rest confident that their intimate communications,

---

[13] *R. v. Vu*, 2013 SCC 60, at paras. 48-49.
[14] *R. v. Marakah*, 2017 SCC 59, at para. 50.
[15] *R. v. Telus Communications Co.*, 2013 SCC 16.
[16] *R. v. Jones*, 2017 SCC 60, at para. 59. See also: *R. v. July*, 2020 ONCA 492.
[17] *Spencer*.
[18] See, for example: *Vu*, at paras. 48-49 (separate authorizations required to search electronic devices found in the course of other already authorized searches); *R. v. Fearon*, 2014 SCC 77, at paras. 51, 58, 76-78 (unlike other items found on individuals, the power to search incident to arrest only permits the police to conduct a tailored search of a cell phone).

thoughts, interests, and relationships are secure against state intrusion, absent compelling justification by the state.

(ii) R. v. Mahal *Creates a Lacuna in Privacy Protection*

19. Within the context of this s. 8 framework, *Mahal* stands out as a conspicuous aberration.

20. In *Mahal*, this Court held that the standard to engage in an intercept of the private communications of a "known person" (rather than the principal target) "is a modest one" and investigators are required only to "have reasonable and probable grounds to believe that the interception of that person's private communications may assist the investigation of an offence".[19]

21. As a result, the *Mahal* standard falls below the constitutional minimum described by the Supreme Court in *Hunter* and adopted for wiretaps in *Duarte* and *Garofoli*.

22. Further, it is inconsistent with La Forest J.'s pronouncement in *Duarte* that this constitutional minimum standard must apply on a "uniform basis" to protect against the surreptitious recording of our conversations "every time we speak".[20]

B. LOWER COURTS HAVE APPLIED *MAHAL*'S MODEST STANDARD IN WAYS THAT UNDERMINE PRIVACY

23. A number of cases since this Court's decision in *Mahal* show how the lower courts are employing this "modest" standard to permit invasive searches of the communications of third parties with little actual connection to the offence or target being investigated.

24. For example, in *R. v. Brewster*, Code J., relying on *Mahal*, explained that the test for intercepting the communications of a "known person" is a "low one" and that this standard allows the police to wiretap someone who "may be an entirely innocent third party who is not implicated in the offence under investigation, provided that seizure of the third party's communications may

---

[19] *Mahal*, at para. 71 (emphasis added).
[20] *Duarte*, at p. 47.

somehow further the investigation".[21] The initial wiretap authorization in that case authorized the interception of the communications of *144 known persons*.[22]

25. This is a far cry from *Duarte*'s direction that s. 8 must "afford protection against the arbitrary recording of private communications ***every time we speak***."[23] *Brewster* also highlights one of the deeply unfair ironies of the *Mahal* standard: *innocent third parties*, who may have nothing to do with the offence being investigated, are afforded less privacy protection than the target. Their privacy is sacrificed at the altar of "may somehow further" the investigation.

26. In *Brewster*, the court ultimately held that the authorization to intercept the communications of a third party as a "known person" based on the tip of an untested confidential informant — which it admitted would not satisfy the *Hunter* standard — and information about his association with gang members or associates met the low *Mahal* standard.[24] This Court dismissed the appeal because it was bound by the *Mahal* decision.[25]

27. *R. v. Durban*[26] also illustrates how *Mahal* is being used to create an expansive dragnet. *Durban* originated from an investigation into a conspiracy to export ecstasy and cocaine, orchestrated by an airport employee named Joe Lee. The police obtained an authorization to intercept Lee's calls. At the time, the defendant, Jem Durban, was not known to police.[27]

28. Over the next few months, the police intercepted many calls between Lee and Durban and saw the two men meeting. The police then obtained a second authorization that included Durban as a "known person," even though there was "no evidence whatsoever of Mr. Durban supplying

---

[21] *R. v. Brewster*, 2016 ONSC 4133, at para. 133. See also: *R. v. Wafer*, 2021 ONCJ 618, at para. 47.
[22] *R. v. Yu*, 2019 ONCA 942, at para. 3.
[23] *Duarte*, at p. 47 (emphasis added).
[24] *Brewster*, at para. 136.
[25] *Yu*, at para. 161.
[26] 2012 ONSC 6939.
[27] *Durban*, at para. 52.

drugs into the airport for the benefit of Mr. Lee's criminal network, or anybody else's criminal network for that matter".[28]

29. As a result of this second authorization, the police intercepted Durban's calls with third parties and learned that he had imported heroin; he was arrested and charged.

30. Ultimately, the court held that the intercepts leading to Durban's arrest and charges were properly authorized, despite being "issued in relation to a wholly separate police investigation" against a distinct target and they were "wholly unrelated to Joe Lee or the conspiracy that was involved in the police investigation in which both authorizations were issued".[29] While Molloy J. stated that it "may not be possible to say that there are reasonable and probable grounds to believe that intercepting [Durban's] communications 'would' yield evidence of the crime under investigation", she was bound by *Mahal*, which was released shortly before her decision.[30] As a result, she dismissed the s. 8 challenge.

31. Thus, lower courts have relied on *Mahal*'s "may assist" standard in a way that permits the police to intercept vast amounts of private communications of third parties that have very little, if anything, to do with the actual offence being investigated, merely because they communicate with someone who happens to be connected with the principal target.

32. Further, in *Du Carmur v. Cole*, Akhtar J. explained that, in order to name someone as a "known person", it is not necessary to know "precisely how the [subject's] intercepted communications might assist in the investigation, but merely consider that they may assist in the investigation".[31] He went on to state that, as long as the *Mahal* standard was met, "there was no requirement to demonstrate the plaintiff's direct involvement in the listed offences".[32]

---

[28] *Durban*, at paras. 2, 59.
[29] *Durban*, at paras. 1-3.
[30] *Durban*, at para. 68.
[31] *Du Carmur*, at para. 75.
[32] *Du Carmur*, at para. 79.

33. These cases show how the "modest" *Mahal* standard operates in investigations and in s. 8 *Charter* challenges. While the rest of s. 8 marches towards a teleological progression of effective constitutional protections that are both principled and proportionate, the *Mahal* gap means that we remain vulnerable to highly intrusive searches on a low evidentiary standard.

C. *MAHAL* WILL PERMIT EVEN GREATER PRIVACY INVASIONS WITH NEW TECHNOLOGIES

34. While this case is about a conventional wiretap, the *Mahal* standard applies to all Part VI authorisations respecting "known persons". This is particularly concerning in this age of rapid technological expansion, as the State continues to find new ways to invade privacy. As Moldaver J. wrote in *TELUS*, which involved a question of statutory interpretation of Part VI, "[t]he task of adapting laws that were a product of the 1970s to a world of smartphones and social networks is a challenging and profoundly important one."[33]

35. The development of new investigative tactics risks making the already-invasive Part VI authorization even more intrusive. For example, the RCMP are seeking (and obtaining) Part VI authorizations for ODITs, which permit the police to engage in a more invasive search than law enforcement has ever been able to do before.[34]

36. These ODITs are spyware that can be remotely installed on a target's computer or mobile device and allow law enforcement to collect electronic evidence, including texts, emails, photos, videos, and financial records.[35] Once installed, law enforcement can review all of the contacts, access a person's cloud account, track their location, and even remotely turn on the device's camera or microphone to turn it into a real-time viewing and listening device.[36] There is even a

---

[33] *Telus*, at para. 53.

[34] "Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues", Report of the Standing Committee on Access to Information, Privacy and Ethics, 44th Parliament, 1st Session, November 2022, pp 21-22.

[35] *Reference re Sections 12 and 21 of the Canadian Security Intelligence Service Act*, 2019 FC 141, at para. 2 ("*CSIS Reference*").

[36] *In re Warrant to Search a Target Computer at Premises*, 2013 WL 1729765, at 755 (S.D. Tex.).

real possibility that law enforcement could incorrectly remotely install an ODIT on a device that belongs to an innocent third party, rather than the intended target.[37]

37. If police were able to obtain authorizations to intercept a target's private communications by installing an ODIT, and if they were able to do this by merely satisfying *Mahal*'s "may afford" standard, s. 8's protections would be hollow.

38. Future cases will provide opportunities for full consideration of the constitutional standards for ODIT authorizations. However, this discussion of emerging interception technologies highlights what is truly at stake in this decision, not just today, but in the future. For now, the Court should take this opportunity to bring Part VI jurisprudence in Ontario back into line with well established, existing constitutional standards and Supreme Court jurisprudence.

PART V - ORDER REQUESTED

39. The CCLA takes no position on the disposition of the appeal.

ALL OF WHICH IS RESPECTFULLY SUBMITTED this 23rd day of December 2022.

Nader R. Hasan / Spencer Bass

[37] *CSIS Reference*, at para. 24.

SCHEDULE "A"

LIST OF AUTHORITIES

TAB	CASES
1	*R. v. Duarte*, [1990] 1 S.C.R. 30
2	*R. v. Jarvis*, 2019 SCC 10
3	*R. v. Spencer*, 2014 SCC 43
4	*R. v. Tessling*, 2004 SCC 67
5	*R. v. Dosanjh*, 2022 ONCA 689
6	*Hunter et al. v. Southam Inc.*, [1984] 2 S.C.R. 145
7	*R. v. Araujo*, 2000 SCC 65
8	*Wakeling v. United States of America*, 2014 SCC 72
9	*R. v. Garofoli*, [1990] 2 S.C.R. 1421
10	*R. v. Vu*, 2013 SCC 60
11	*R. v. Marakah*, 2017 SCC 59
12	*R. v. Telus Communications Co.*, 2013 SCC 16
13	*R. v. Jones*, 2017 SCC 60
14	*R. v. July*, 2020 ONCA 492
15	*R. v. Fearon*, 2014 SCC 77
16	*R. v. Brewster*, 2016 ONSC 4133
17	*R. v. Wafer*, 2021 ONCJ 618
18	*R. v. Yu*, 2019 ONCA 942
19	*R. v. Durban*, 2012 ONSC 6939
20	*Reference re Sections 12 and 21 of the Canadian Security Intelligence Service Act*, 2019 FC 141, at para. 2 ("*CSIS Reference*").

21	*In re Warrant to Search a Target Computer at Premises*, 2013 WL 1729765
	SECONDARY SOURCES
22	"Device Investigative Tools Used by the Royal Canadian Mounted Police and Related Issues", *Report of the Standing Committee on Access to Information, Privacy and Ethics*, 44th Parliament, 1st Session, November 2022, pp 21-22

SCHEDULE “B”

TEXT OF STATUTES, REGULATIONS & BY-LAWS

None

TEMORSHAH HAFIZI et al.	and	HIS MAJESTY THE KING	Court File No. C67423
Applicants (Appellants)		Respondent (Respondent in Appeal)	

COURT OF APPEAL FOR ONTARIO

Proceeding commenced at TORONTO

FACTUM OF THE INTERVENER, CANADIAN CIVIL LIBERTIES ASSOCIATION

STOCKWOODS LLP
Barristers
Toronto-Dominion Centre
TD North Tower, Box 140
77 King Street West, Suite 4130
Toronto ON M5K 1H1

Nader R. Hasan (54693W)
Tel: 416-593-1668
naderh@stockwoods.ca

Spencer Bass (75881S)
Tel: 416-593-1657
spencerb@stockwoods.ca

Tel: 416-593-7200

Lawyers for the Intervener
Canadian Civil Liberties Association

Email for parties served:
Howard L. Krongold: howard@agpllp.ca