August 15, 2017

All the Pieces Matter: Organized Crime, Wiretaps and Section 8 of the *Charter*

By: Erin Sheley

Case Commented On: *R v Amer*, 2017 ABQB 481 (CanLII)

Det. Freamon: "Non-pertinent"? How do you log that non-pertinent?
Det. Pryzbylewski: No drug talk.
Det. Freamon: They use codes that hide their pager and phone numbers. And when someone does use a phone, they don't use names. And if someone does use a name, he's reminded not to. All of that is valuable evidence.
Det. Pryzbylewski: Of what?
Det. Freamon: Conspiracy.
Det. Pryzbylewski: Conspiracy?
Det. Freamon: We're building something here, detective. We're building it from scratch. *All the pieces matter.*

--*The Wire*, Season One, Episode Six

This early scene in HBO's *The Wire*, in which Detective Lester Freamon instructs his rookie colleague Ray Pryzbylewski on how to tag conversations they've overheard on their wiretap of Avon Barksdale's Baltimore drug operation, dramatizes the strategy of long-term police investigations of organized criminal syndicates: "all the pieces matter." Seemingly isolated conversations that, standing alone, reveal no evidence of criminal activity, become part of a general web of information which may eventually prove guilt beyond a reasonable doubt in a court of law. But this form of long-term wiretapping—implicating, as it does, a citizen's right to security from unreasonable searches and seizures under section 8 of the *Charter*—often fits uneasily within the more exacting framework of constitutional case law. In *R v Amer*, the Alberta Court of Queen's Bench had an opportunity to revisit the current state of the law on wiretaps in the wake of a spree of shootings that occurred in Calgary in the summer of 2015.

In this case the Defence (comprised of four accused, Barakat Amer, Baderr Amer, Tarek El-Raffie and Abdul Amer) challenged the validity, execution of, and interpretation of three authorizations for wiretaps granted under Part VI, s 184(2) of the *Criminal Code*, RSC 1985, c C-46. The Calgary Police Service (CPS) believed that eight individuals had been responsible for the four shootings in question, on the basis of evidence gleaned from police surveillance, interviews and communications with confidential informants, computer databases, ballistics analysis and testing, forensic examination of data stored on mobile devices, and records from providers of communications services (at para 45). On the basis of this belief, the CPS applied for and received a wiretap authorization for six cell phones "used by" the four accused which, under s 186 of the *Code*, required a court finding that the authorization "would be in the best

interests of the administration of justice" and that "other investigative procedures have been tried and 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" (at para 49).

The Defence challenged these wiretaps on three grounds:

1. That the authorization was facially invalid insofar as it did not require "live monitoring" of the wiretaps for the purposes of insuring that only named targets, and not third parties, were on the intercepted calls (at para 5).
2. That the CPS failed in their duty of candour to the court in applying for the wiretaps, insofar as they did not draw its attention to the fact that the police proposed to intercept calls without live monitoring and failed to adequately disclose that the evidence did not show that the targets were the dominant users of the device (at para 6).
3. That, when properly interpreted, the authorizations in fact limited authority to intercept cell phones to circumstances where they were being used by a named target (which implicitly required live monitoring for most of the calls) (at para 7).

The Court begins its analysis here with the basic premise articulated in *R v Thompson*, [1990] 2 SCR 111, 1990 CanLII 43 (SCC), holding that electronic surveillance constitutes a search and seizure within the meaning of section 8 of the *Canadian Charter of Rights and Freedoms* (at para 48). The twin requirements for wiretaps under Part VI of the *Code* have, thus, received constitutional gloss by the SCC. In *R v Duarte*, [1990] 1 SCR 30, 1990 CanLII 150 (SCC), it held that the *Code's* "best interests of the administration of justice" requirement "imports as a minimum requirement that the issuing judge must be satisfied that the authorization sought will afford evidence of that offence" (a duty met, in part, by compliance with s 185(1)(e)'s requirement that the application identify "known" targets and the "nature and location of any known places where the interceptions will occur") (at para 49). As to the "investigative necessity" requirement, the Supreme Court has rejected a "last resort" standard in favour of a more malleable test requiring the judge to "look seriously at whether there is, practically speaking, no other reasonable alternative method of investigation" (*R v Araujo*, 2000 SCC 65 (CanLII) at para 35).

Once these requirements are met, however, additional terms and conditions may be required to limit the violation of any individual's privacy interest (at para 52). The question of whether such a limitation—such as the live monitoring urged by the *Amer* Defence—should have been included gets somewhat deferential scrutiny on appeal: "the reviewing judge does not substitute his or her view for that of the authorizing judge" (at para 53).

In arguing that live monitoring should have been required by the authorization, the Defence relies heavily on *Thompson* which held that an unreasonable search had occurred due to a wiretap with insufficient limiting conditions (at para 55). That case, however, involved the continuous recording of public payphones based on evidence (nearly identical to the facts involved in the scene from *The Wire*) that they were near the location one of the targets of that investigation was staying and that the targets made wide use of payphones for their communications (at para 55). To support the claim that the cell phones in this case implicated heightened privacy interests of third parties analogous to public payphones, the Defence argued that: (1) privacy interests associated with cell phones deserve special recognition; (2) there is an

elevated concern for third parties in cases with no live monitoring; and (3) the evidence did not support the conclusion that the actual targets were the "dominant users" of the tapped phones (at para 56).

The Court rejects each of these three claims in turn, relying on a combination of existing precedent and practicality. First, it notes that the only case law indicating a heightened privacy interest in cell phones relates to police searches of cell phone data, not to the interception of calls, and that intercepting a cell phone call does not lead, counter to the Defence's suggestion, to more knowledge of a target's physical location than if it were a landline (at paras 47-48). Second, it finds that any requirement of live monitoring would often be logistically ineffective: "relevance of a conversation cannot necessarily be determined at the beginning of a call, or even at its end until all other information is gathered in an investigation" (at para 60). While the Court does not discuss this at length, it seems potentially relevant to its analysis not only that live monitoring would be ineffective for these reasons, but also impractical: in setting up the facts of the case it notes that during the time of the investigation the CPS's wire room was intercepting twenty to twenty-four calls at any given time (between the instant investigation and two others that were ongoing); according to the testimony of one of the investigating officers, had live monitoring been implemented twenty monitors would have been required and the sheer volume of calls would have tied them up for months (at para 18).

As to the third claim, that the evidence failed to establish that the targets themselves were the dominant users of the phones, the Court analyzes the facts and finds the nature of the defendants' illegal operations dispositive on the question of privacy. Relying on the testimony of police experts, the Court points to the very large number of calls and the fact that phones in the drug business are often answered by multiple people who might receive orders (at para 64). These facts provide "an explanation for why the volume of calls is so high and why persons other than targets of the homicide investigation used cellphones" (at para 65). In coming to this conclusion, it is worth noting that the Court states that "the point is not that drug traffickers have no privacy rights," citing *R v Spencer*, 2014 SCC 43 (CanLII) for the proposition that the privacy interest does not depend on whether it shelters legal or illegal activity (at para 65). It correctly contrasts the instant case with *Thompson*, noting that this was hardly an indiscriminate "fishing expedition" in public payphones but a search at least tailored to the targets' drug associates (at para 65). But it is hard to understand how the logic of this distinction does not exactly compel the conclusion that drug traffickers do, in fact, have no, or at least fewer, privacy rights.

In any case, the Court ends its analysis on the question of facial invalidity by noting that the facts of other cases could, in fact require a live monitoring restriction to be *Charter*-compliant (at para 67). It concludes, however, that the instant case does not rise to such a level. The Court also makes relatively short work of the Defence's other two principal arguments. Reviewing the evidence submitted by the CPS as part of its request for authorization the Court concludes that it "did not suggest anything other than a reasonable basis for belief that the specified cell phones were regularly used by the targets" (at para 75) and that the application did in fact include a live monitoring requirement in certain locations such as custodial places so it alerted the authorizing judges to the possibility of a wider live monitoring requirement. Thus, there was no breach of the duty of candour by the CPS. As to the argument that the authorization did, in fact, implicitly require live monitoring, the Court points to the plain text of the authorization which includes as "persons whose communications may be intercepted" the category "unknown persons" (at para 90).

With respect to the one lingering question raised by this case concerning the privacy rights of drug dealers, perhaps it would have been better for the Court to have simply articulated the implicit missing piece in its analysis. Like the phone calls between Barksdale dealers in *The Wire*, the day-to-day dealings of a drug syndicate are inextricably interwoven with the murders and aggravated assaults that result from them. All the pieces matter. It might, therefore, be more transparent and law-like for courts to simply articulate a standard that says doing business with members of a known criminal conspiracy results in a lowered expectation of privacy on those occasions, rather than sweeping that reality under the rug. (Indeed the existing law already relaxes the requirements for wiretap authorization in cases involving criminal organization offences, where the police need not meet the "investigative necessity" requirement). Until then, however, all of the pieces of an individual police investigation will matter—for constitutional purposes—as much as the pieces of the conspiracy it tracks.

This post may be cited as: Erin Sheley "All the Pieces Matter: Organized Crime, Wiretaps and Section 8 of the *Charter*" (15 August, 2017), online: ABlawg, http://ablawg.ca/wp-content/uploads/2017/08/Blog_ES_Amer.pdf