



DISAPPEARING DREAMS?
How cannabis affects sleep **C1**



UP THE
INTENSITY
*Interval training
boosts fitness* **B1**



Past president of the Canadian Association of Chiefs of Police and Commissioner of the Ontario Provincial Police Tom Carrique, right, says police across the country want modifications to Part 2 of Bill C-22 to grant warranted access to encrypted data where big crime is hiding. *SHAUGHN BUTTS*

ENCRYPTION REMAINS STICKING POINT TO BILL C-22

Police chiefs give bill a big thumbs-up,
but want changes to better fight crime

JACKIE CARMICHAEL

EDMONTON Canadian law enforcement leaders are worried Bill C-22 has been defanged, and civil rights advocates say it has gone too far, but the federal government’s bid for “lawful access” to Canadians’ data for crime solving got a big thumbs-up from the Canadian Association of Chiefs of Police last Tuesday.

Immediate past president of the CACP and Commissioner of the Ontario Provincial Police Tom Carrique told Postmedia as the bill heads from the House of Commons to the Senate and its committees for final work in the fall, police across the country still need a couple modifications to Part 2 of Bill C-22 to grant warranted access to encrypted data where big crime is hiding.

The sticking point becomes encrypted data.

Carrique said the federal government has clarified Part 2’s service providers having to build and maintain access to data does not include encrypted data.

“Under a search warrant, we need the ability to get to that encrypted data or we can’t solve homicides. We can’t protect children from sexual exploitation. We cannot disrupt terrorist cells,” Carrique told Postmedia in a sit-down interview during the association’s annual summit and trade show at the Edmonton Convention Centre.

“I think Canadians need to ask themselves, is it acceptable that criminal organizations, drug cartels that are orchestrating homicides in this country are using encrypted technology to orchestrate those hits, prove that they have murdered somebody and then send the money for those transactions? They’re stealing people’s cars, all being orchestrated over encrypted apps. They’re trafficking humans, they’re sharing sex-

ual images of youth. This is all happening through encrypted apps. We are not asking to access encrypted networks. We are asking for, ‘Person A is a criminal, we can convince the court of that, the most serious crime, we’re asking a judge to give us a warrant, which we can get right now, we are judicially authorized, but we can’t break the encryption without the use of a tool, which we have, and we’re simply asking that that tool be explicitly clarified in the Criminal Code for our use and it be protected under the Canada Evidence Act,’” Carrique said.

Tech companies and law-abiding Canadians have nothing to fear, he said.

“We would need to prove before a court that you were involved in serious criminal activity. There are no privacy issues,” Carrique said.

Agencies would still need search warrants and judicial authorization for anything of evidentiary value, Carrique said.

“This is not a surveillance regime. This is not about us having access to information that we should not have,” he said.

SEPARATING GOOD FROM BAD

There’s been a litany of complaints from civil rights groups that the legislation would violate Charter rights against unreasonable search, and that it collects an awful lot of breadcrumbs on absolutely every Canadian because everybody lives in a digital world.

On May 26, Erik Neuenschwander, senior director for user privacy and child safety at Apple, told the House of Commons Standing Committee on Public Safety and National Security he has a team on call, 24-7, to assist law enforcement.

SEE BILL ON **A2**