Canada's Supreme Court allows warrantless mobile phone search

Colin J. Bennett

February 2015

Canada's Supreme Court allows warrantless mobile phone search

Case affects Canadians' expectations of mobile phone privacy. By **Colin Bennett**.

In a decision that surprised many observers, and disappointed privacy advocates, the Canadian Supreme Court decided in December 2014, that police did not need to get a warrant to search a cellphone when they make an arrest. This 4-3 ruling was directly opposed to the unanimous decision reached by the US Supreme Court in *Riley v. California*, that law enforcement cannot search an arrestee's phone unless they have a warrant.

The facts of the Canadian case (*Kevin Fearon v. HM the Queen*) centered on a jewellery robbery at a Toronto market in 2009, at which the police seized the cell phone of the suspect, searched it without a warrant, and quickly found an incriminating text message and photograph. At issue, was whether Mr. Fearon's Charter rights had been violated. Section 8 of the Canadian Charter of Rights and Freedoms states: "Everyone has the right to be secure against unreasonable search and seizure." Canadian jurisprudence, like the United States, tends to centre on the meaning of "unreasonable" and whether or not the individual might have a "reasonable expectation of privacy" depending on the nature of the information and the context of the search.

At issue, therefore, were exactly the same issues that arose in *Riley v. California* (2014) in the United States. Police have long been able to search a person incident to arrest to establish correct identity and to ensure their safety. But that traditionally meant a search of a wallet, billfold and pockets. The range of information on a modern smartphone could provide a detailed profile of an individual's past and current life. In *Riley*, the US Supreme Court recognised unanimously the difference and therefore insisted that the warrantless search of the digital contents of a smartphone was unconstitutional.

At the trial of Fearon, the judge found that the defendant's rights had not been violated. And at the subsequent appeal the claim was also dismissed on the grounds that the phone was not password protected; the defendant had taken no steps to protect his data, and therefore had no "reasonable expectation of privacy."

The majority opinion of the Canadian Supreme Court, written by Justice Cromwell, concluded that mobile phone searches can aid police officers in identifying risks to public safety, in identifying accomplices, and in locating and preserving evidence. That being said, the judgment insisted that four conditions must be met in order for the search of a cell phone or similar device incidental to arrest to comply with Section 8: The arrest must be lawful; the search must be "truly incidental" and not the object of the arrest, and this condition must be strictly applied; the nature and extent of the search must be tailored to its purpose (limited to areas where evidence is likely to be found, such as text messages, e-mails, and call logs); and Police must record detailed notes about the search, including applications opened and the search duration.

The majority did, however, reject the argument that the absence of password protection on a mobile phone indicates any sort of abandonment of a reasonable expectation of privacy.

The three justice minority on the Canadian court said the majority have given the police "extraordinary power," and recognised the vast range of information that might now be accessible without warrant: "the cell phone acts like a key or portal which can allow the user to access the full treasure trove of records and files that the owner has generated or used on any number of devices. It is not just the device itself and the information it has generated, but the gamut of (often intensely) personal data accessible via the device that gives rise to the significant and unique privacy interests in digital devices. The fact that a suspect may be carrying their house key at the time they are arrested does not justify the police using that key to enter the suspect's home."

The minority went on to argue that the test applied by the majority would essentially allow police officers to conduct searches and then sort out the justification after the fact. Only judicial pre-authorisation through a warrant can provide the effective and impartial balancing of state interests and privacy protection on a case-by-case basis.

The Justice Minister, Peter Mackay, praised the ruling as a pragmatic solution that will aid law enforcement. Other commentators took some comfort in the articulation of a set of safeguards, and in the rejection of the argument that password protection makes any material difference to constitutional privacy expectations.

Others have argued that this decision is at odds with recent jurisprudence and especially with three other Canadian cases: the *R v. Spencer* (2014) decision that requires law enforcement agencies to obtain a warrant prior to accessing subscriber information; *R. v. Cole* (2012) that decided that employees may have a reasonable, though limited, expectation of privacy in their work computer; and *R. v. Vu* (2013) that found that the privacy interests at stake in searches of personal or home computers (including mobile phones) are markedly different because of the quantity and range of information that might be accessible.

So the question for the future is whether the four conditions articulated in *R. v. Fearon* will provide a practical and reasonable guidance for police searches. Will the limitation of the search to information that is truly related to the object of the arrest be a standard that can be enforced in practice? Or will it lead to fishing expeditions? Given the pace of technological development, it is probable that *R. v. Fearon* will not be the last word on the issue.

AUTHOR

Professor Colin Bennett, Department of Political Science, University of Victoria, British Columbia, Canada.

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

EDPS aims to be proactive and focus on external relations

New European Data Protection Supervisor (EDPS), Giovanni Buttarelli, promises an active dialogue with regulators, industry and civil society plus some new initiatives. **Laura Linkomies** reports.

"My goal is for the European Union to speak with one voice on data protection," Giovanni Buttarelli said in an interview with *PL&B* at the end of January. "This is a historical moment for data protection because of the surveillance debate, the new security threats, the ongoing data protection reform, and the transatlantic dialogue. After more than 22 years of experience in data protection, I now have a unique opportunity to be in this privileged

Continued on p.3

Hong Kong DPA sets sights on cross-border data transfers

The Privacy Commissioner issues guidance and encourages companies to follow it whether or not transfer rules are implemented by the government. **Paul Lanois** reports.

On 29 December 2014, the Hong Kong Office of the Privacy Commissioner for Personal Data (the Privacy Commissioner) published guidance on personal data protection in cross-border data transfers (the Guidance Note). This Guidance Note was released in light of the Privacy Commissioner's call earlier in 2014 for "a renewed

Continued on p.4

Issue 133 **February 2015**

GLOBAL ANALYSIS OF DATA PRIVACY LAWS AND BILLS

NEWS

ANALYSIS

MANAGEMENT

INTERNATIONAL report

ISSUE NO 133 **FEBRUARY 2015**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

SUB EDITOR
Tom Cooper

REPORT SUBSCRIPTIONS
Glenn Daif-Burns
glenn.daif-burns@privacylaws.com

CONTRIBUTORS
Paul Lanois
Attorney, admitted to the New York and Paris Bars
Robert Bond
Charles Russell Speechlys LLP, UK
Colin Bennett
University of Victoria, British Columbia, Canada
Ian Cunliffe
CPA Australia
Christine Bryant
Solicitor, Australia
Chris Connolly
Galexia, Australia
Nigel Waters
Pacific Privacy Consulting, Australia

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

Is privacy investment on the rise?

Some commentators say that large companies have started to act as if the EU DP Regulation was already in force – and bodies such as the European Data Protection Supervisor (EDPS) are making preparations to be 'ready from day one' as the new EDPS Giovanni Buttarelli told me last month (p.1). In the US, TRUSTe research shows that 30% of organisations budgeted more than $1 million for privacy in 2014. So organisations understand that compliance is still less costly than data breaches.

The new EU DP regulation would bring about new compliance costs, even if it relies on the accountability principle (p.35). One large cost area is international transfers, whether it be drafting BCRs or other arrangements. The easiest solution would be to find common ground between EU BCRs and APEC CBPRs (p.11) but the EU is not yet satisfied that the two systems offer similar protections, although commonalities exist. Also, watch out for the Hong Kong Commissioner's new interpretation on international transfers (p.1).

So why is there delay with the EU DP Regulation? The Commission's proposal was always very ambitious. We are still waiting for the Council to agree a common position and the negotiations have become very political – Germany, France and the UK are holding up the negotiations, for different reasons. If agreement can be found by June, it is hoped that the trilogue will be conducted by the end of 2015 (p.9). In the meantime, the Council of Europe is progressing with Convention 108 reform that includes assessments of candidate countries (p.7) and follow-up checks on Member States which have signed and ratified the convention.

See p.18 for the most comprehensive tables ever on global privacy laws and bills. While Europe was the first to regulate, with Sweden's Data Act of 1973, most new laws are now enacted elsewhere (p.14). Australia has new privacy principles but they may not aid compliance (p.30) and Canada's Supreme Court has issued a controversial ruling on searching mobile phones in the context of an arrest of a person (p.29).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 100+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
You will be sent the PDF version of the new issue on the day of publication. You will also be able to access the issue via the website. You may choose to receive one printed copy of each Report.

3. E-Mail Updates
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Chief Privacy Officer, BT Retail, UK**"

Subscription Fees

Single User Access

International Edition **£500 + VAT***

UK Edition **£400 + VAT***

UK & International Combined Edition **£800 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-4 or 5-25 users – see website for details.

Subscription Discounts

Special charity and academic rate:
50% discount on all prices. Use HPSUB when subscribing.

Number of years:
2 (10% discount) or 3 (15% discount) year subscriptions.

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.
www.privacylaws.com/UK