

From: [Google Alerts](#)
To: s 22(1)(a)(ii)
Subject: Google Alert - personal data
Date: Wednesday, 22 November 2017 2:04:32 PM



personal data

Daily update · November 22, 2017

NEWS

[Uber reportedly paid hackers \\$100000 to cover up a cyberattack that exposed the **personal data** of ...](#)

Business Insider

Uber paid hackers \$100,000 to cover up a 2016 cyberattack that exposed the **personal data** of 57 million people, including both riders and drivers, ...

[Uber Hid Massive Breach That Affected **Personal Data** of 57 Million Passengers and Drivers for ... - KTLA](#)

[Hackers stole the **personal data** of 57 million Uber passengers and drivers - Los Angeles Times](#)

[Uber Security Breach Exposed **Personal Data** Of 57 Million Customers And Drivers - Jalopnik Full Coverage](#)



Flag as irrelevant

[Uber Says Hackers Stole **Personal Data** Of 57 Million Users](#)

NPR

The company kept the breach secret for more than a year. According to a Bloomberg report, Uber paid the hackers \$100,000 to delete the stolen **data** ...



Flag as irrelevant

[Uber admits year-old hack exposed **personal data** of 57 million riders, drivers](#)

The Advocate

SAN FRANCISCO (AP) — Uber is coming clean about its cover-up of a year-old hacking attack that stole **personal** information about more than 57 ...



Flag as irrelevant

s 22(1)(a)(ii)

s 22(1)(a)(ii)

The **personal data** of Australian Uber users may have been exposed in a massive global breach

Business Insider Australia

And it appears Australian drivers and passengers may have been caught up in the privacy breach, with Uber contacting unspecified local authorities.


☐ ☐ ☐

Flag as irrelevant

s 22(1)(a)(ii)

s 22(1)(a)(ii)

s 22(1)(a)(ii)



From: s 22(1)(a)(ii)
 Subject: South Australia Radio News Update – 2pm / 1pm
 Date: Wednesday, 22 November 2017 3:23:30 PM

**SOUTH AUSTRALIA RADIO NEWS UPDATE
 WEDNESDAY 22 NOVEMBER 2017**

FIVEaa 1395 – 2.01PM

s 22(1)(a)(ii)

**** 2nd story – Managing information security risks/Uber Technologies; University of New South Wales’s Australian Centre for Cyber Security**

Presenter: Uber [has](#) admitted to hiding a massive [breach](#) that exposed the data of 57 million users and drivers around the world. The ride-sharing service paid hackers to delete the data, last year, and keep quiet. It now admits it had a legal obligation in the US to report the privacy breach. The Australian Centre for Cyber Security’s Professor Greg Austin says it’s possible the data is still out there.

Greg Austin: the breach of the driver’s-licence data is probably even more important than the leak of the credit-card information and the details of the users, because, for identity theft, a driver’s licence number’s a far more useful tool than simply the other pieces of information

s 22(1)(a)(ii)

FIVEaa 1395 – 1.04PM

s 22(1)(a)(ii)


**** 3rd story – Managing information security risks/Uber Technologies**

Presenter: Ride-sharing giant Uber is on the defensive following revelations it [covered](#) up the [hacking](#) of the details of millions of customers and drivers. Bill Rehkopf has more.

Bill Rehkopf: Uber – which has come under both regulatory and criminal investigations, in recent months – tried to cover up last year’s hack of over 57 million drivers and customers. Instead, Uber paid those hackers \$100,000 in hush money to keep quiet and delete the stolen data. Uber maintains that, while names, phone numbers and email addresses of its drivers and customers were stolen, there is no evidence that credit-card or other financial

information was hacked. This week, Uber fired its Chief Security Officer and one of his deputies.

s 22(1)(a)(ii)



From: s 22(1)(a)(ii)
 Subject: South Australia Radio News Update – 2pm / 1pm
 Date: Wednesday, 22 November 2017 3:23:35 PM

**SOUTH AUSTRALIA RADIO NEWS UPDATE
 WEDNESDAY 22 NOVEMBER 2017**

FIVEaa 1395 – 2.01PM

s 22(1)(a)(ii)

**** 2nd story – Managing information security risks/Uber Technologies; University of New South Wales's Australian Centre for Cyber Security**

Presenter: Uber [has](#) admitted to hiding a massive [breach](#) that exposed the data of 57 million users and drivers around the world. The ride-sharing service paid hackers to delete the data, last year, and keep quiet. It now admits it had a legal obligation in the US to report the privacy breach. The Australian Centre for Cyber Security's Professor Greg Austin says it's possible the data is still out there.

Greg Austin: the breach of the driver's-licence data is probably even more important than the leak of the credit-card information and the details of the users, because, for identity theft, a driver's licence number's a far more useful tool than simply the other pieces of information

s 22(1)(a)(ii)

FIVEaa 1395 – 1.04PM

s 22(1)(a)(ii)

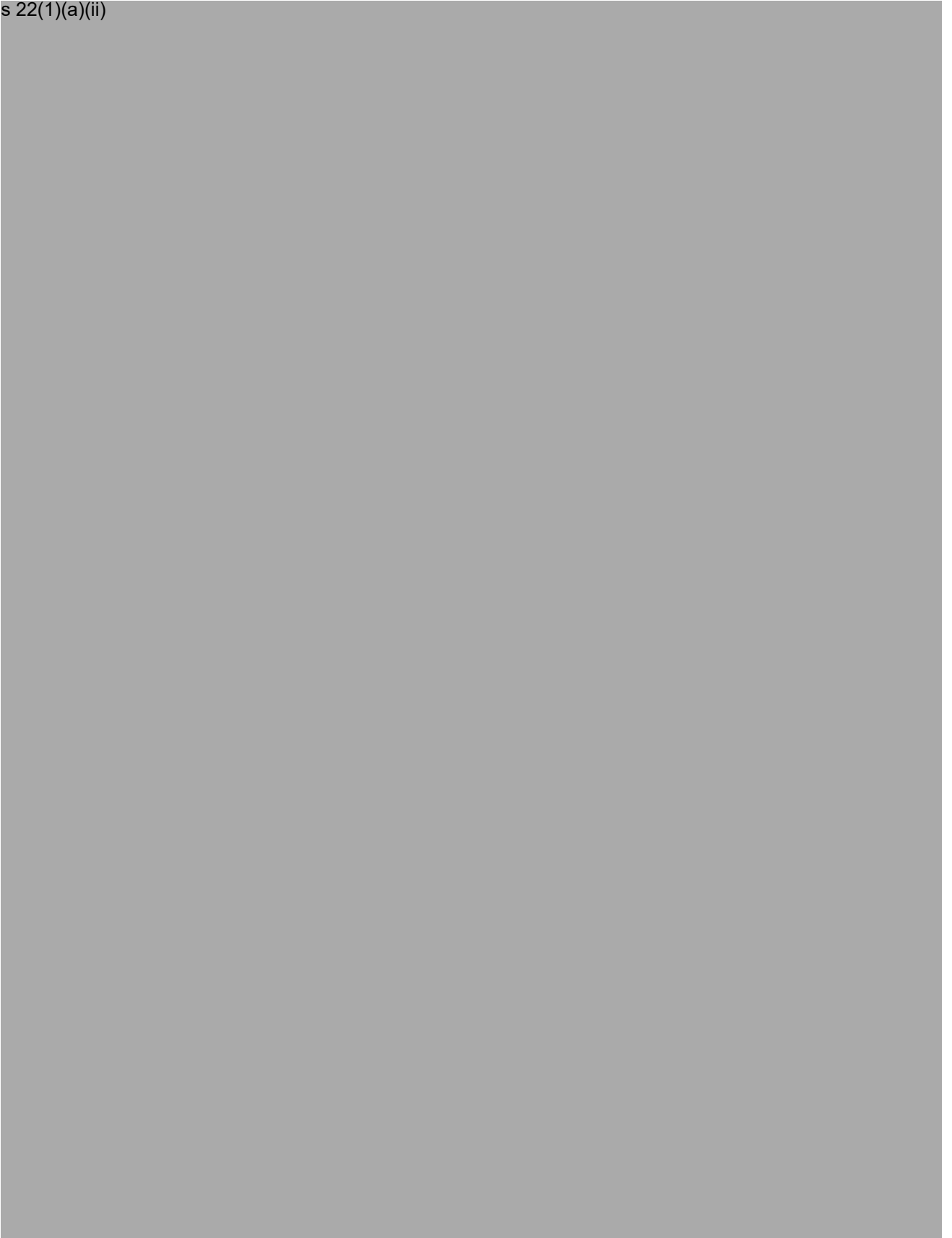
**** 3rd story – Managing information security risks/Uber Technologies**

Presenter: Ride-sharing giant Uber is on the defensive following revelations it [covered](#) up the [hacking](#) of the details of millions of customers and drivers. Bill Rehkopf has more.

Bill Rehkopf: Uber – which has come under both regulatory and criminal investigations, in recent months – tried to cover up last year's hack of over 57 million drivers and customers. Instead, Uber paid those hackers \$100,000 in hush money to keep quiet and delete the stolen data. Uber maintains that, while names, phone numbers and email addresses of its drivers and customers were stolen, there is no evidence that credit-card or other financial

information was hacked. This week, Uber fired its Chief Security Officer and one of his deputies.

s 22(1)(a)(ii)



From: [Google Alerts](#)
To: s 22(1)(a)(ii)
Subject: Google Alert - privacy
Date: Friday, 1 December 2017 10:06:34 AM

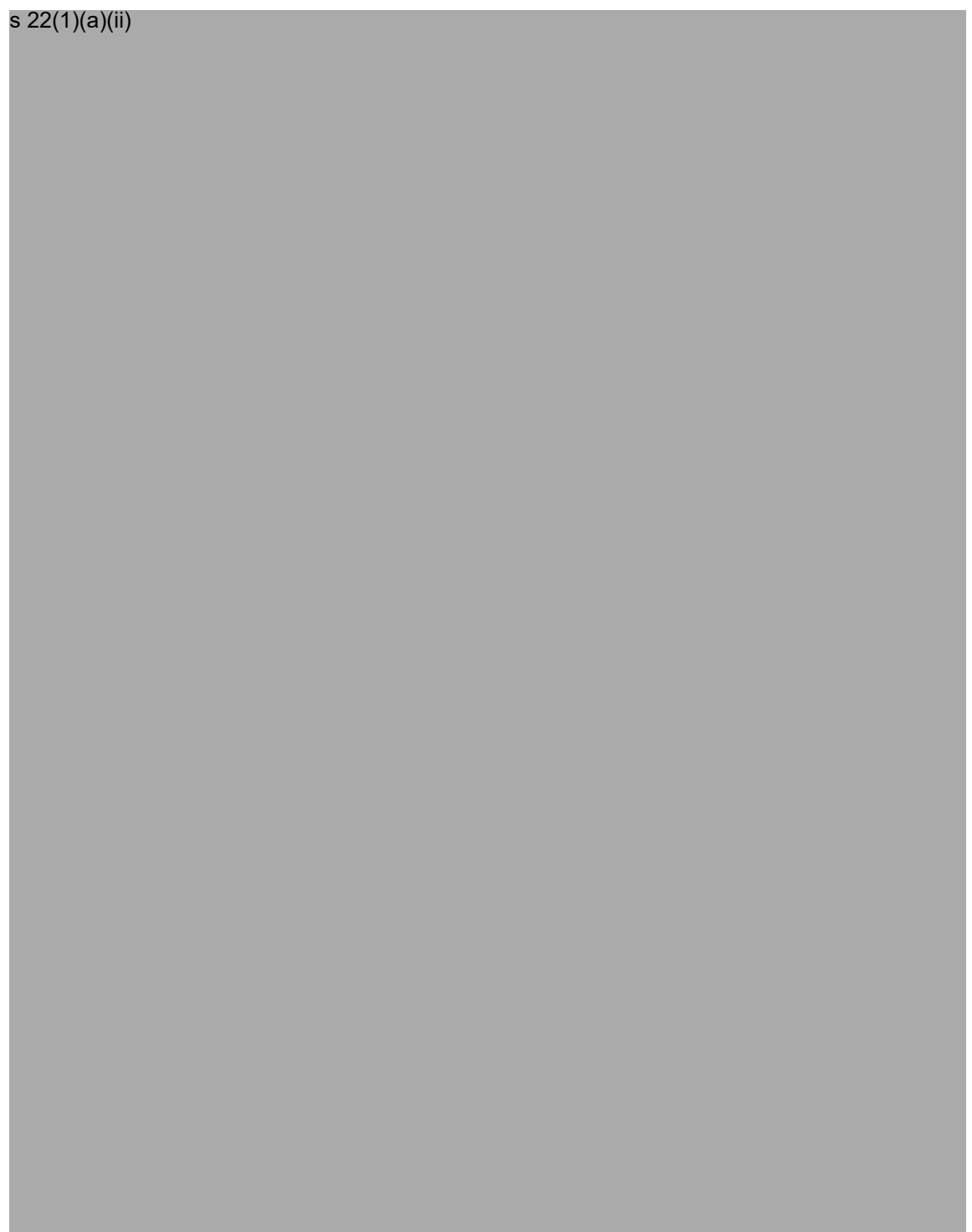


privacy

Daily update · November 30, 2017

NEWS

s 22(1)(a)(ii)



s 22(1)(a)(ii)

EU **Privacy** Regulators Set up Task Force to Liaise on Uber Hack Probes

U.S. News & World Report

BRUSSELS (Reuters) - European Union **privacy** regulators said on Wednesday they had set up a task force to coordinate national investigations into ... Uber has faced a stream of top-level executive departures over issues ranging from sexual harassment to data **privacy** to driver working conditions, ...

[Europe's **Privacy** Regulators Are Ganging Up on Uber](#) - Fortune

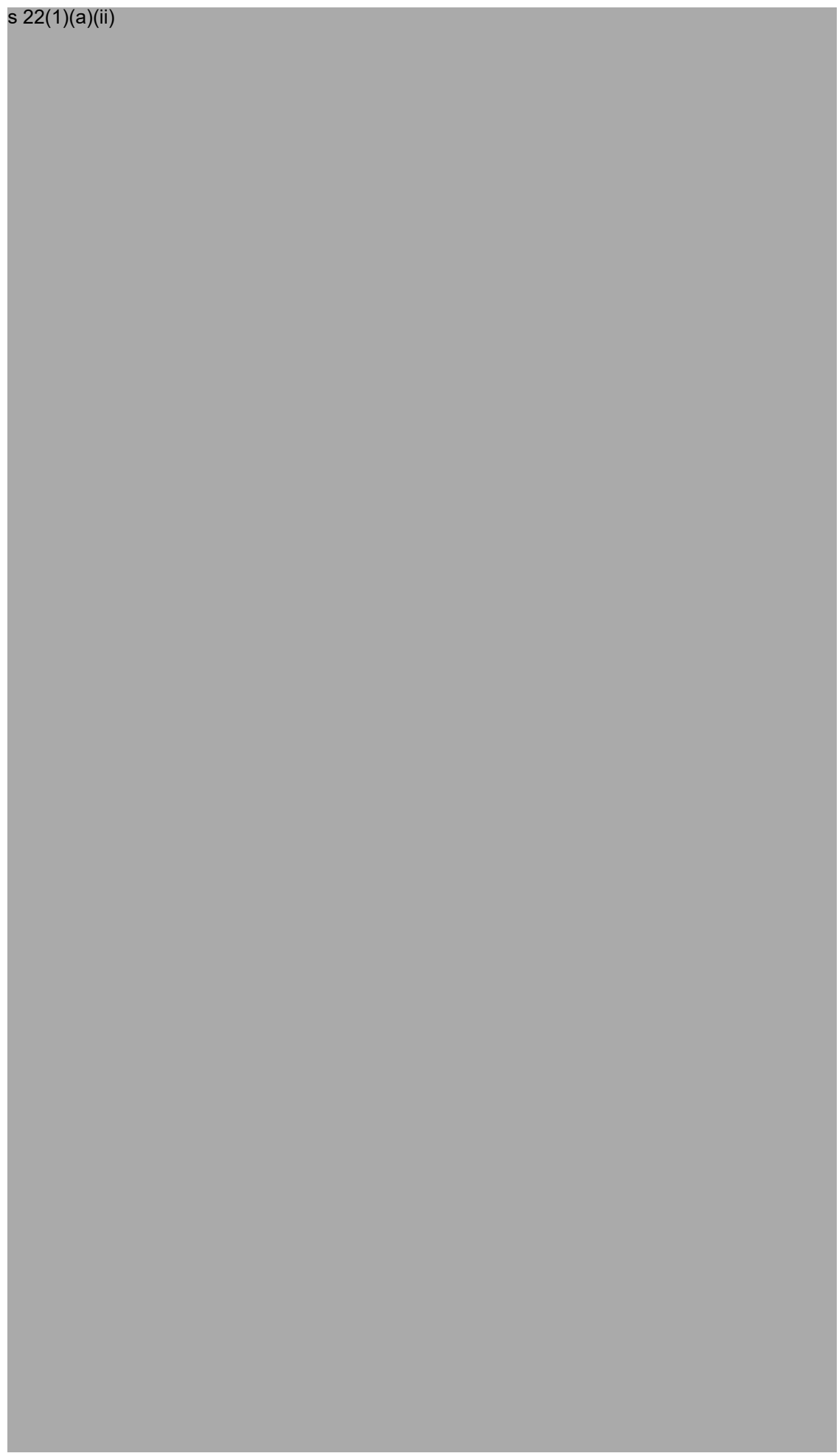
[Class-action lawsuit launched against Uber in Alberta over data **privacy** breach](#) - CBC.ca
[Full Coverage](#)



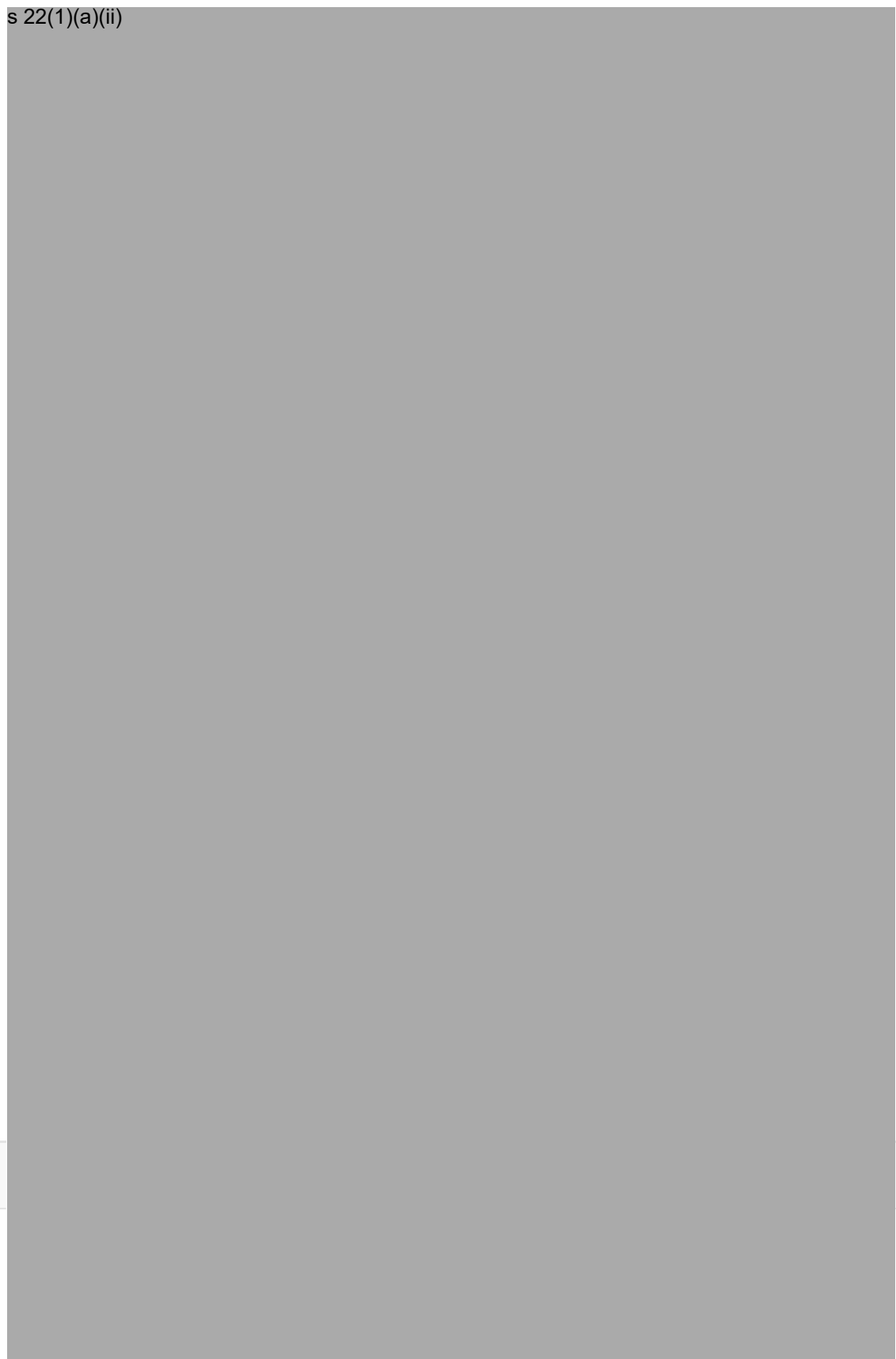
Flag as irrelevant

s 22(1)(a)(ii)

s 22(1)(a)(ii)



s 22(1)(a)(ii)



From: [Google Alerts](#)
To: s 22(1)(a)(ii)
Subject: Google Alert - data breach
Date: Monday, 11 December 2017 10:01:51 AM



data breach

Daily update · December 10, 2017

NEWS

[Uber paid hackers \\$100000 after they stole data on 57 million users](#)

KOCO Oklahoma City

The license numbers of around 600,000 drivers in the United States were included in the **breach**. The company did not alert victims or regulators of the **breach** when it was first discovered. Britain's **data** protection watchdog said the news raised "huge concerns" about Uber's **data** policies and ethics.



Flag as irrelevant

s 22(1)(a)(ii)

s 22(1)(a)(ii)

MY TAKE: What the Uber hack tells us about fresh attack vectors created by the rise of DevOps

Security Boulevard


Dissecting the root cause of Uber's catastrophic **data breach** is a worthwhile exercise. Diving one level deeper into the scenario that led up to the popular ride-hailing service losing personal data for 50 million passengers and seven million drivers shows us why this particular type of hack is likely to recur ...



Flag as irrelevant

s 22(1)(a)(ii)

s 22(1)(a)(ii)



From: [Google Alerts](#)
To: s 22(1)(a)(ii)
Subject: Google Alert - personal information
Date: Saturday, 16 December 2017 2:09:28 PM



personal information

Daily update · December 16, 2017

NEWS

s 22(1)(a)(ii)

[Privacy watchdog: 171K PH users affected by Uber data breach](#)

[Inquirer.net](#)

The **personal information** of 171,000 Filipino Uber drivers and passengers had been compromised in a hack that Uber Technologies Inc. deliberately hid from public knowledge for more than a year, according to the head of the government body looking into the extent and implications of the breach.

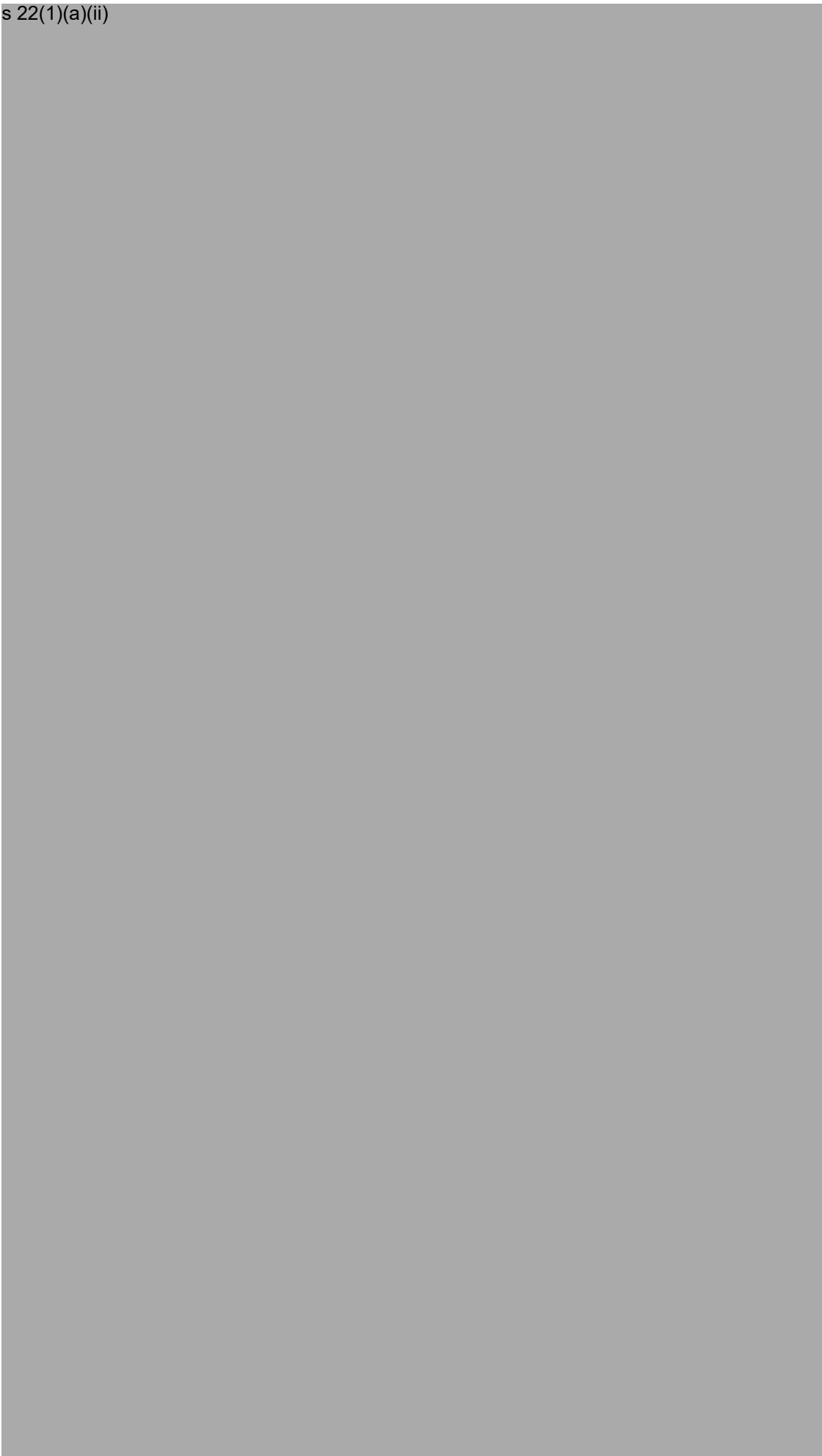
[171000 Filipinos seen affected by hacking of Uber website](#) - [Inquirer.net](#)

[Privacy body looking into Uber's steps to protect user data](#) - [Philippine Star](#)

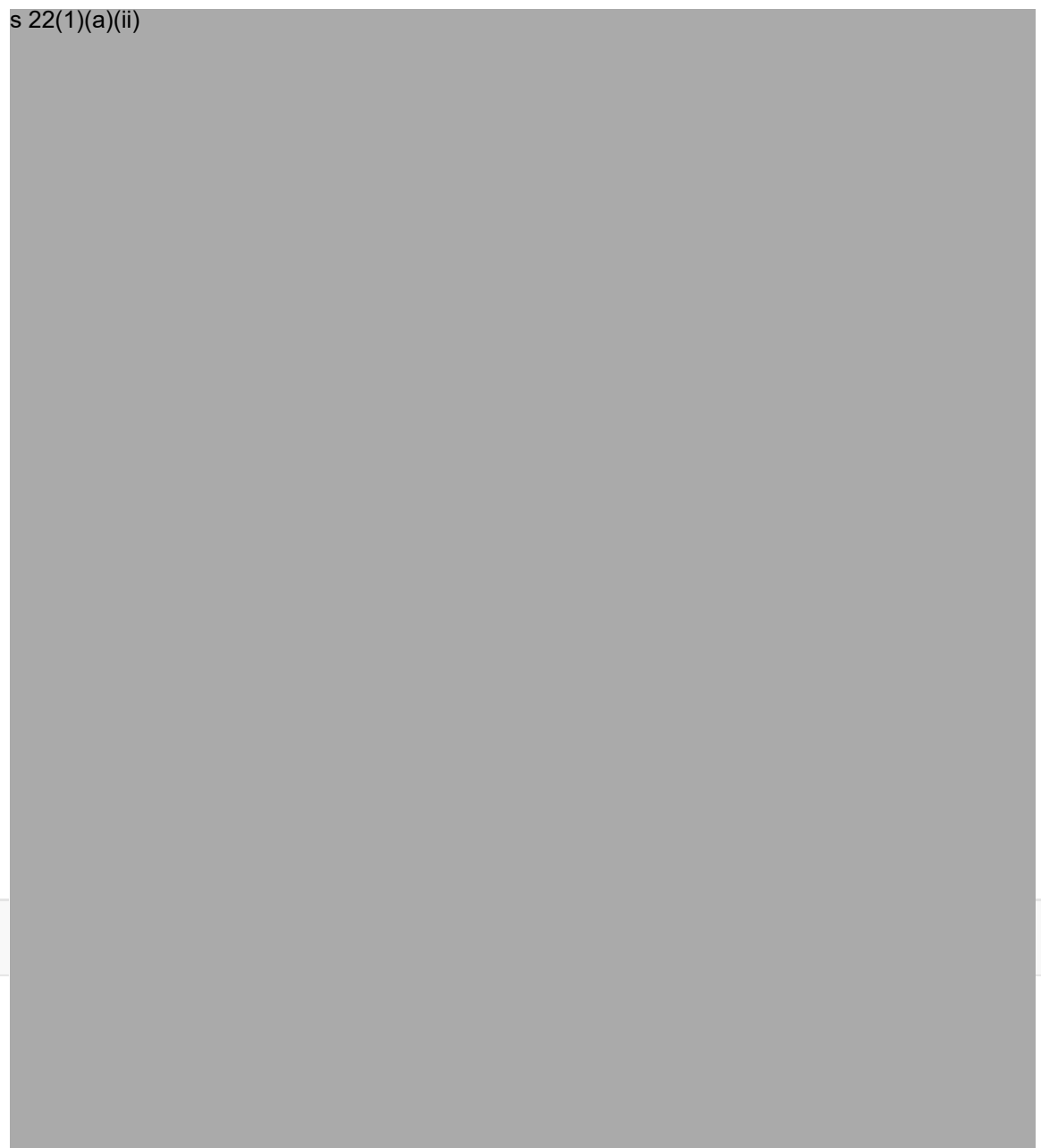
[380000 Uber users hit in Singapore's largest data breach](#) - [The Straits Times](#)
[Full Coverage](#)

[Flag as irrelevant](#)

s 22(1)(a)(ii)



s 22(1)(a)(ii)



From: [Google Alerts](#)
To: s 22(1)(a)(ii)
Subject: Google Alert - data breach
Date: Thursday, 28 December 2017 10:04:18 AM

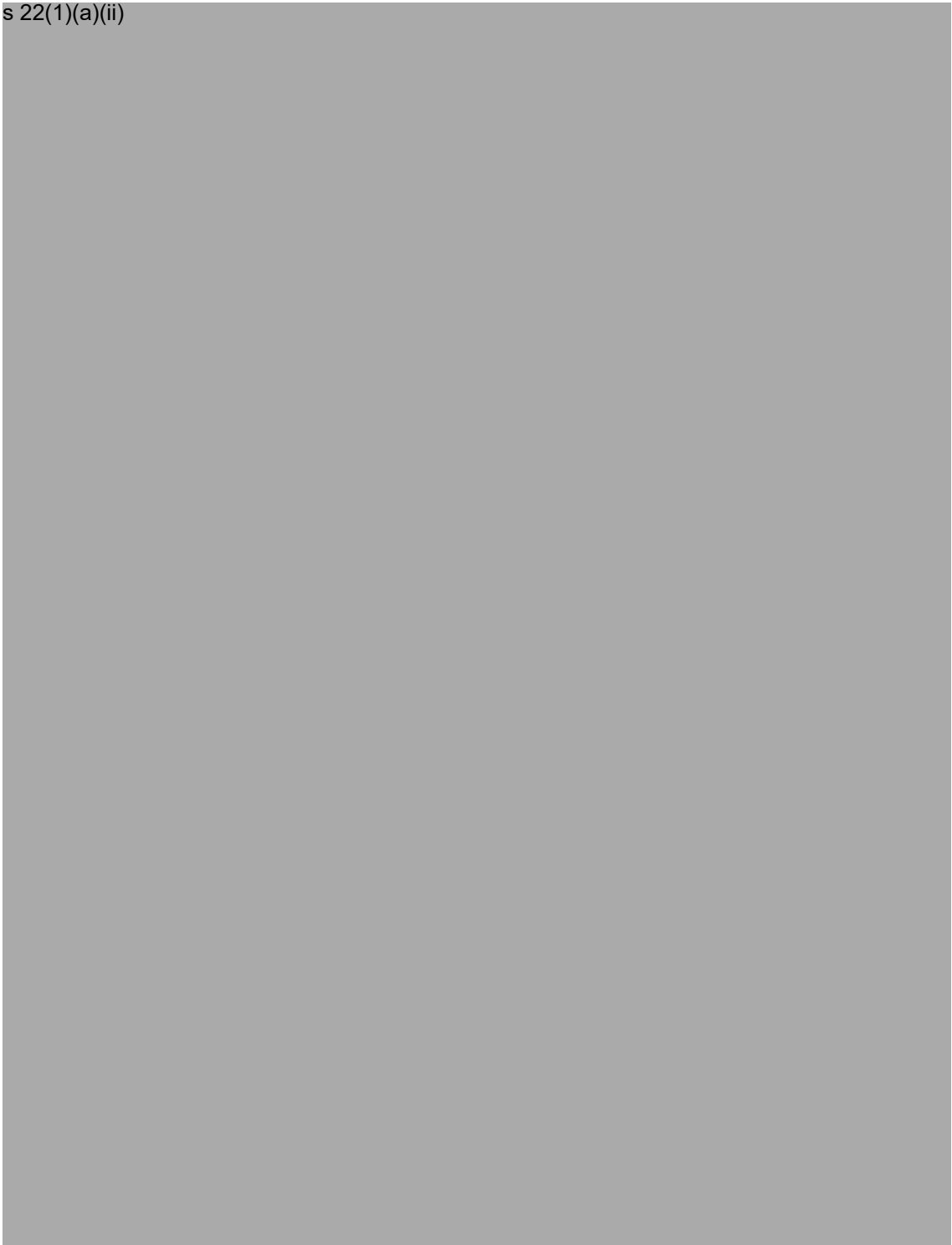


data breach

Daily update · December 27, 2017

NEWS

s 22(1)(a)(ii)



s 22(1)(a)(ii)

Here's how Uber could have prevented that massive **security breach**

Verdict

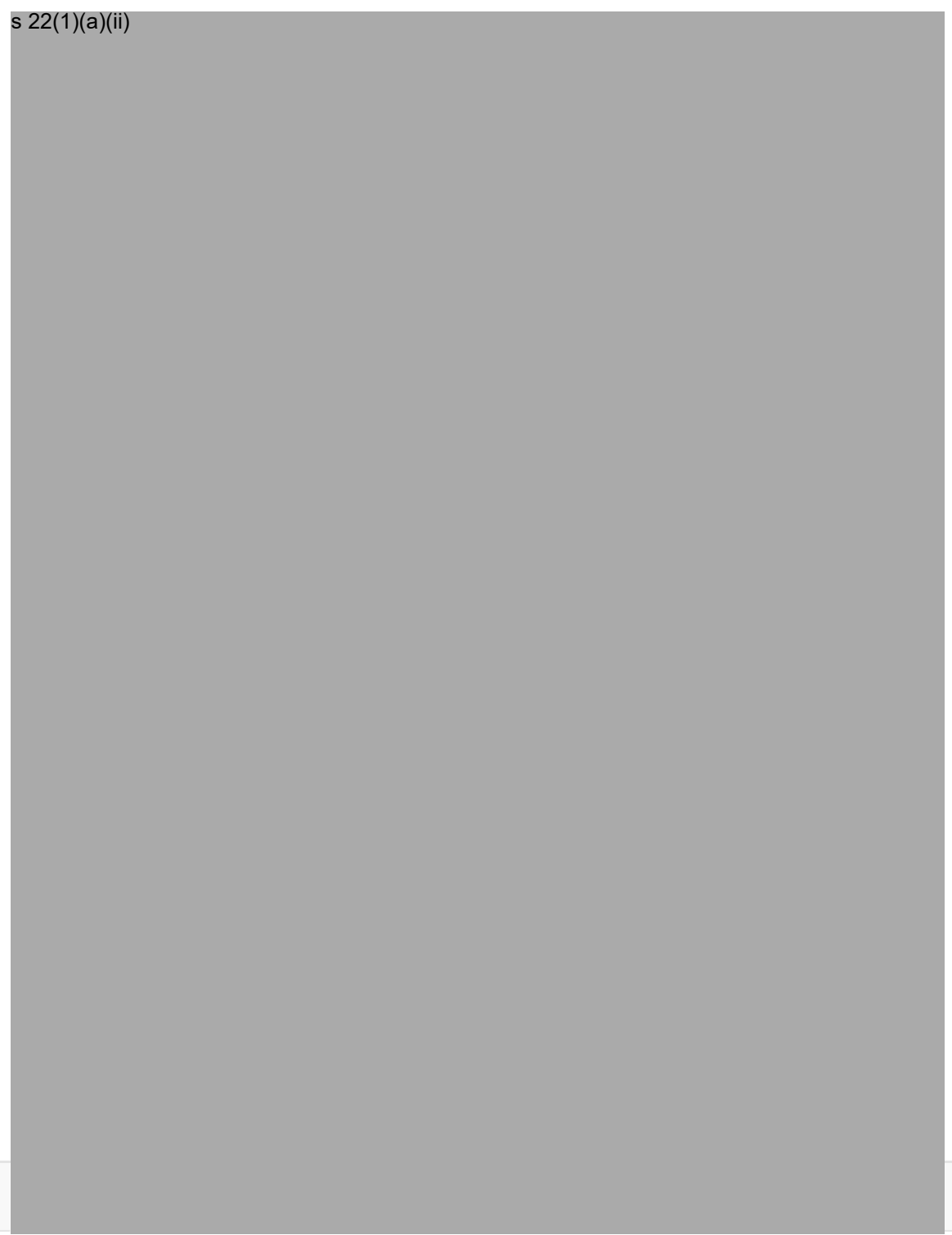
Companies using the public cloud get better security than if they store data themselves thanks to economies of scale — but Uber's massive **data breach** shows there's still a lot to do. Ride-sharing firm Uber suffered a **data breach** in October 2016 that exposed the personal data of 57m customers and ...




Flag as irrelevant

s 22(1)(a)(ii)

s 22(1)(a)(ii)




s 22(1)(a)(ii)



From: [OAIC](#)
To: [PMC Privacy](#)
Subject: Information Matters: Our Uber privacy determination, save the date for International Access to Information Day and more
Date: Friday, 30 July 2021 10:51:36 AM


s 22(1)(a)(ii)



Welcome to our July edition of Information Matters.

In this newsletter, read about our [Uber privacy determination](#), s 22(1)(a)(ii)

s 22(1)(a)(ii)



Uber determination finds privacy breach

Australian Information Commissioner and Privacy Commissioner Angelene Falk has found Uber Technologies, Inc. and Uber B.V. interfered with the privacy of an estimated 1.2 million Australians.

Commissioner Falk found the Uber companies failed to appropriately protect the personal data of Australian customers and drivers, which was accessed in a cyber attack in October and November 2016.

The determination finds the Uber companies breached the *Privacy Act 1988* by not taking reasonable steps to protect Australians' personal information from unauthorised access and destroy or de-identify the data as required. They also failed to take reasonable steps to implement practices, procedures and systems to ensure compliance with the Australian Privacy Principles.

"This determination makes my view of global corporations' responsibilities under Australian privacy law clear," Commissioner Falk said.

"Australians need assurance that they are protected by the Privacy Act when they provide personal information to a company, even if it is transferred overseas within the corporate group."

[Read more](#)

s 22(1)(a)(ii)

