



CIGI-IPSOS GLOBAL SURVEY ON **INTERNET SECURITY AND TRUST**

DARRELL BRICKER, CIGI SENIOR FELLOW

FEN OSLER HAMPSON, CIGI DISTINGUISHED FELLOW
AND DIRECTOR OF THE GLOBAL SECURITY & POLITICS
PROGRAM

© 2016 Ipsos. All rights reserved. Contains Ipsos' Confidential and Proprietary information and may not be disclosed or reproduced without the prior written consent of Ipsos.

Methodology



- This survey was conducted by Ipsos on behalf of the Centre for International Governance Innovation (“CIGI”) between November 20 and December 4, 2015.
- The survey was conducted in 23 countries plus Hong Kong. The countries were: Australia, Brazil, Canada, China, Egypt, France, Germany, Great Britain, Hong Kong, India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, South Africa, South Korea, Sweden, Tunisia, Turkey, the United States. Total sample 24,143 Internet users.
- Twenty of the countries utilized the Ipsos Internet panel system while the other four (Kenya, Nigeria, Pakistan and Tunisia) were conducted by Ipsos Computer-aided Telephone Interviewing (CATI) facilities in each of those countries.
- In the US and Canada respondents were aged 18-64, and 16-64 in all other countries.
- Approximately 1000+ individuals were surveyed in each country and are weighted to match the online population in each country surveyed. The precision of Ipsos online polls is calculated using a credibility interval. In this case, a poll of 1,000 is accurate to +/- 3.5 percentage points. For those surveys conducted by CATI, the margin of error accuracy is +/-3.1.

BRIC = **Brazil, Russia, India, China**
APAC = **Asia Pacific**
LATAM = **Latin America**

Content

1

Privacy and Security

2

Behaviour Changes

3

Internet Access

4

**Monitoring and
Censoring by
Government and Police**

5

Hactivists

6

**Keeping Information
Safe and Secure**

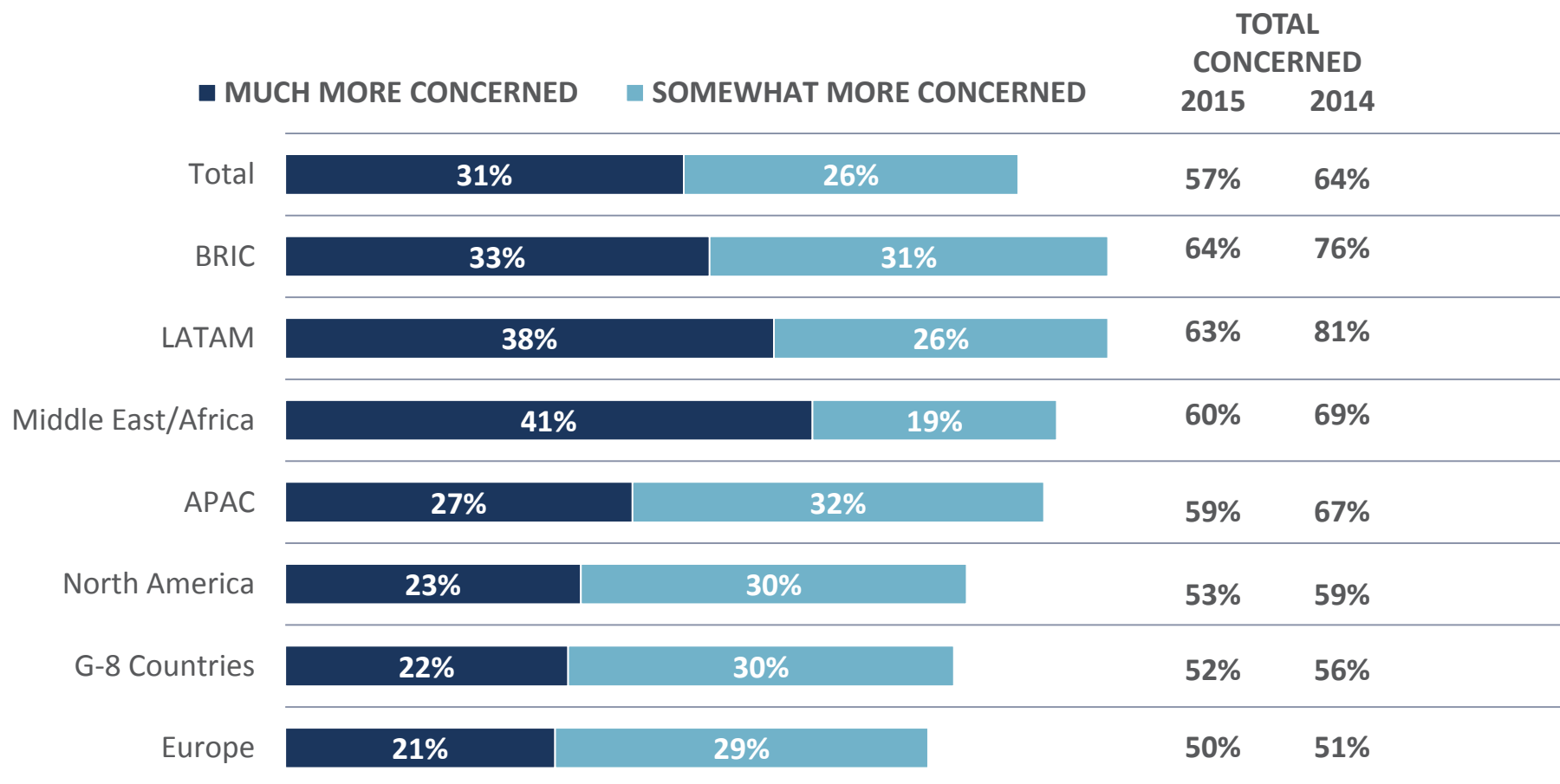
7

Conclusion



PRIVACY and SECURITY

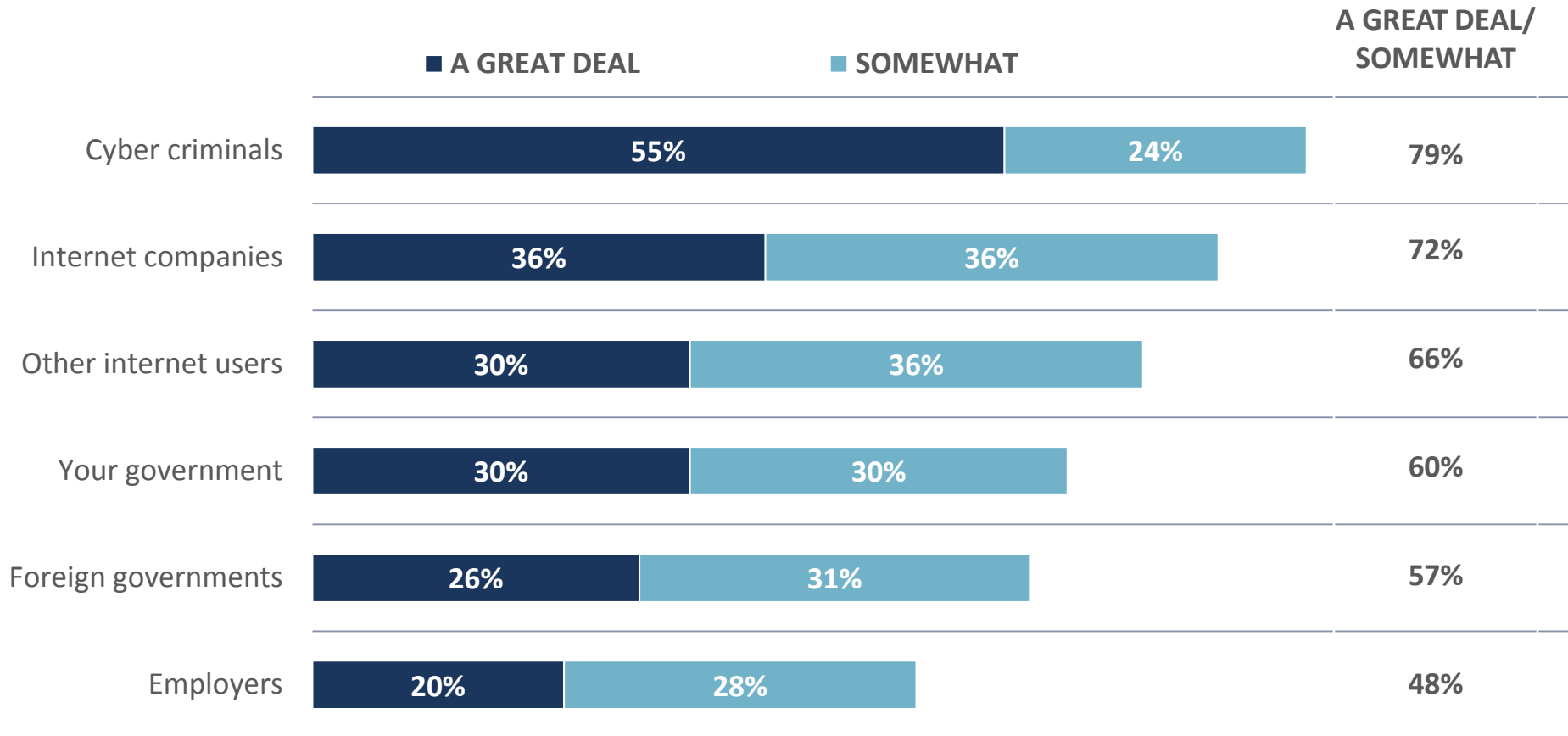
Fewer are concerned about their online privacy in 2015 (57%) compared to 2014; LATAM witnessed the sharpest decrease in concern since last year



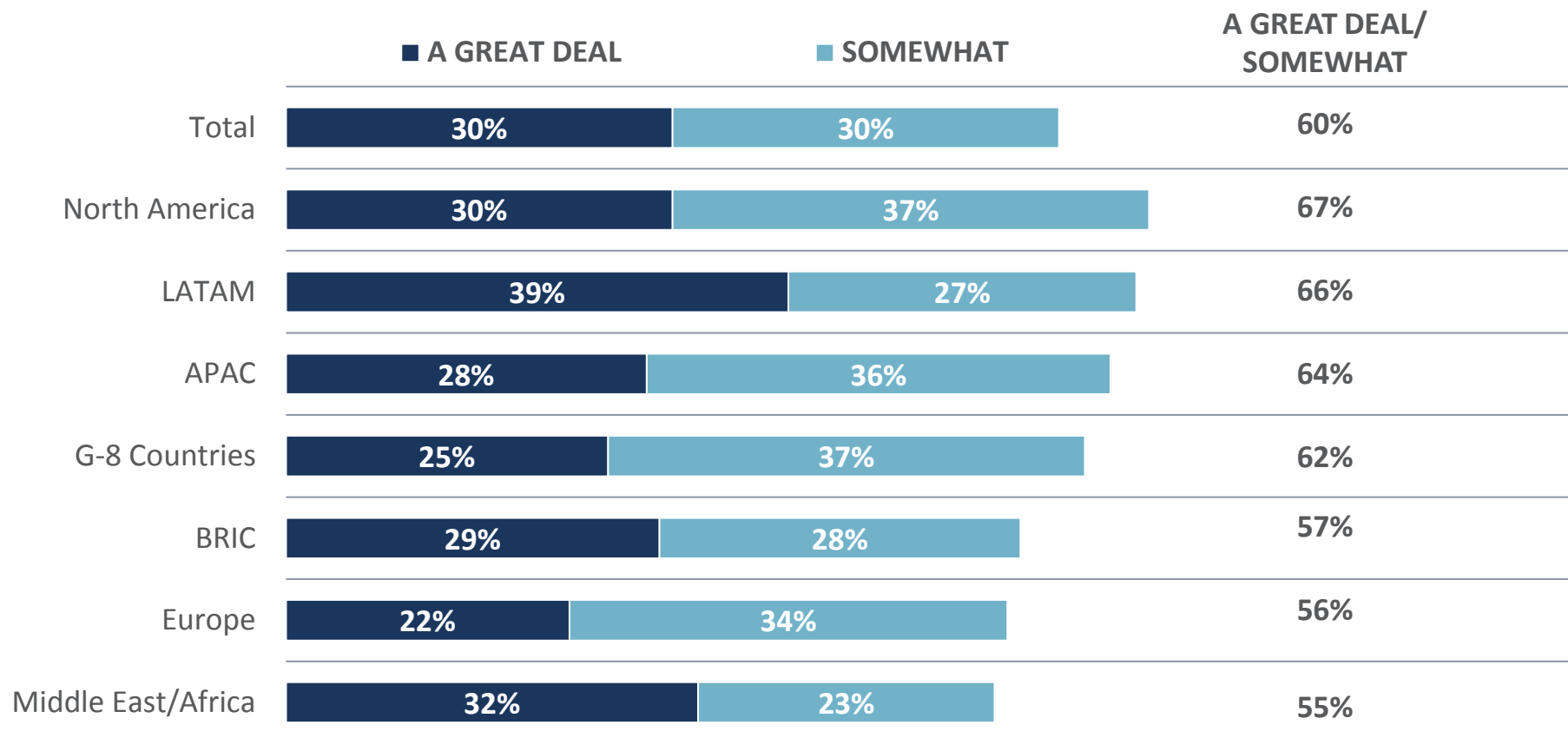
GLOBAL TOTAL



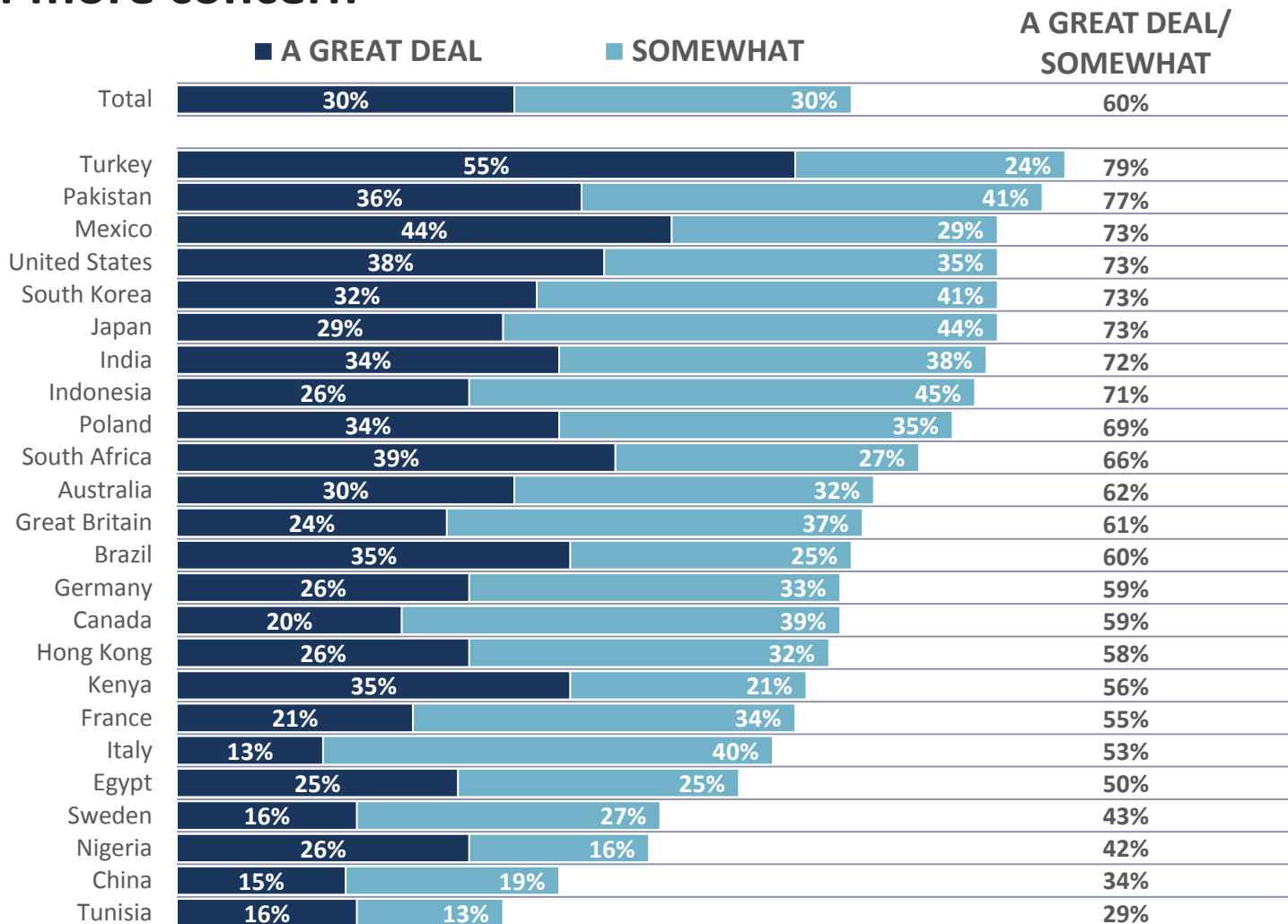
Cyber criminals and internet companies are most likely to contribute to increasing concerns about online privacy



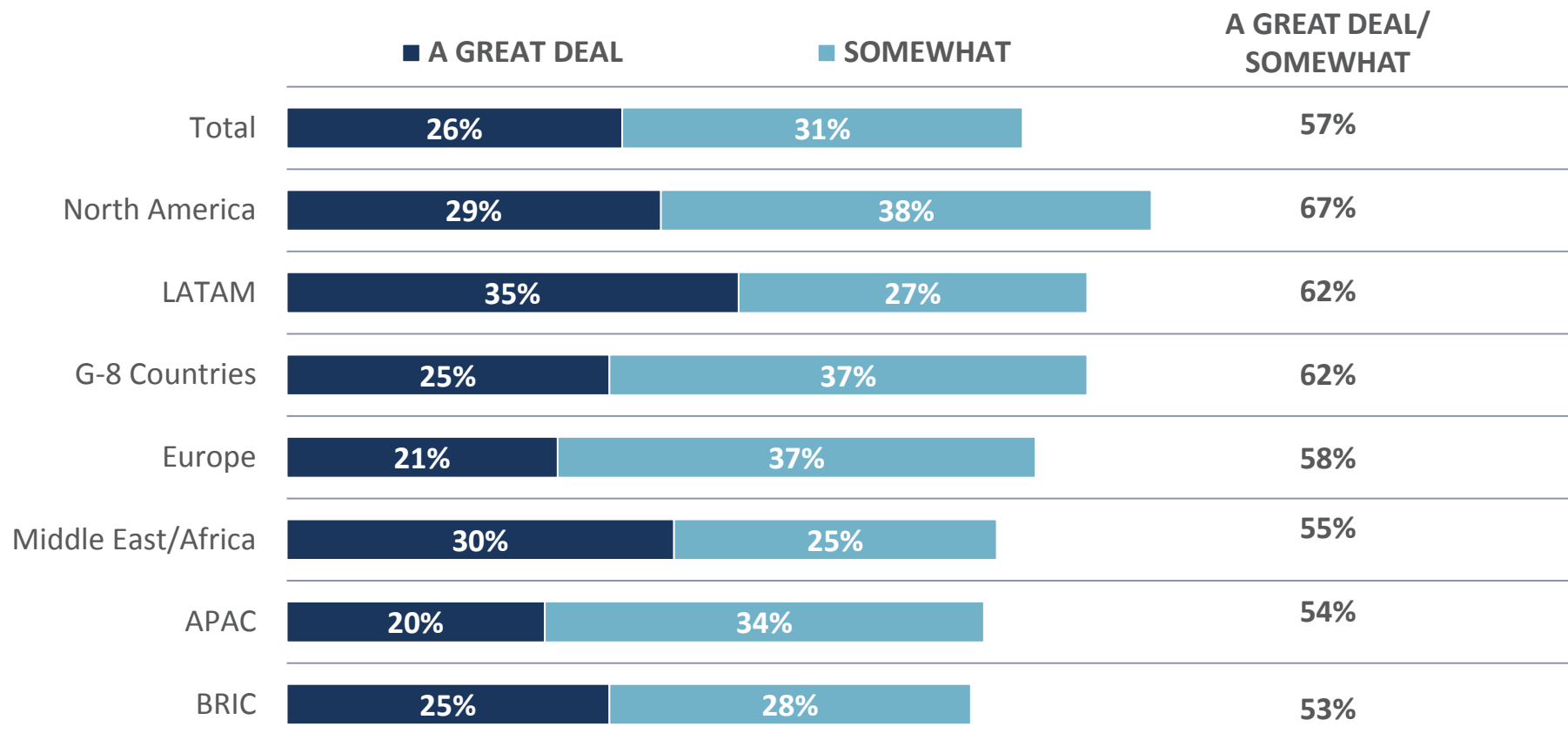
Among those who are more concerned about online privacy, North America, LATAM, APAC, and G-8 countries are more likely to indicate “their government” is the source of more concern



Among those who are more concerned about online privacy, six in ten (60%) indicate “their government” is a source of more concern

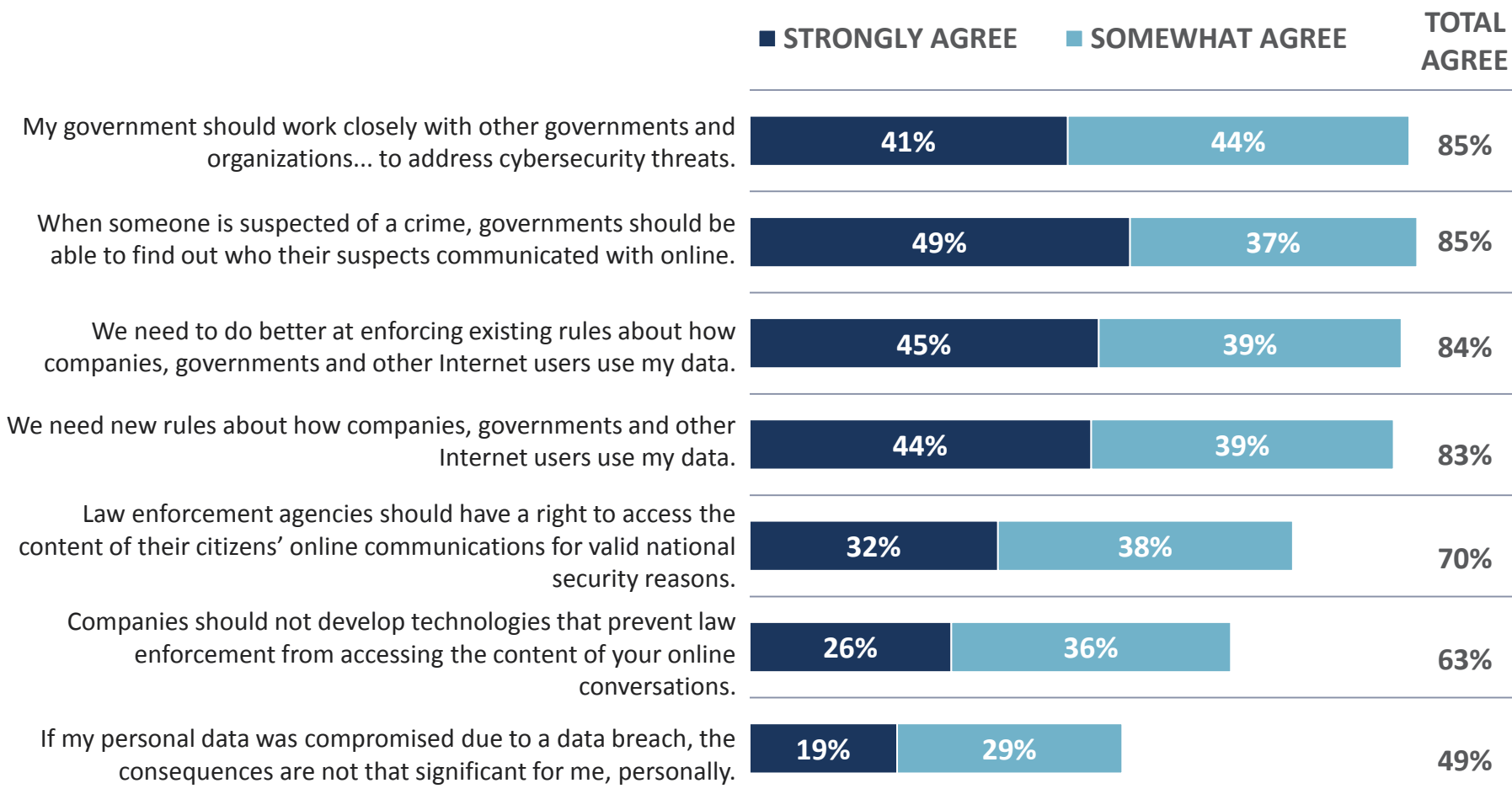


Among those who are more concerned about online privacy, North America, LATAM, and G-8 countries are more likely to indicate “foreign governments” is a source of more concern

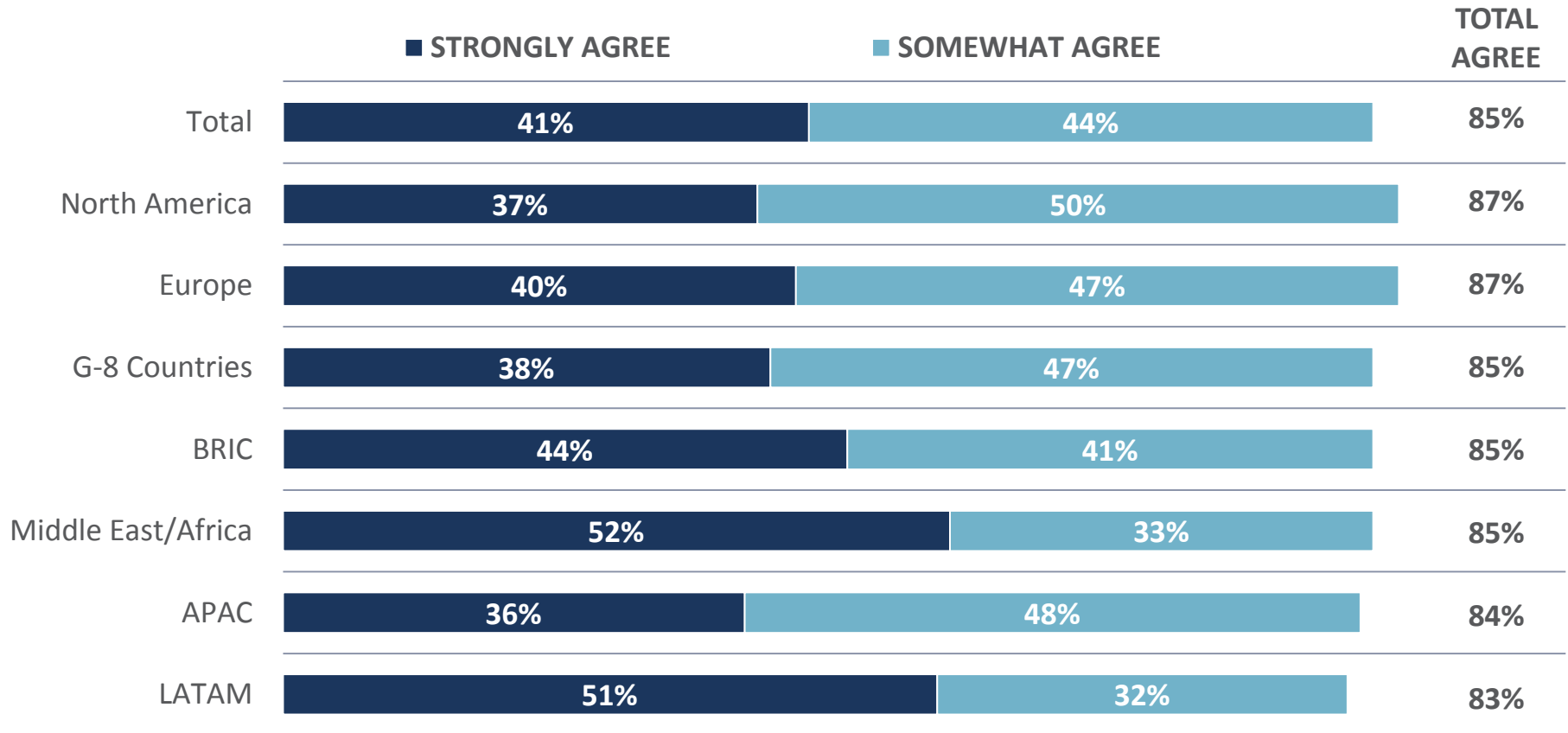


GLOBAL TOTAL

Vast majority agree that government should be able to investigate online communications of someone who is suspected of a crime



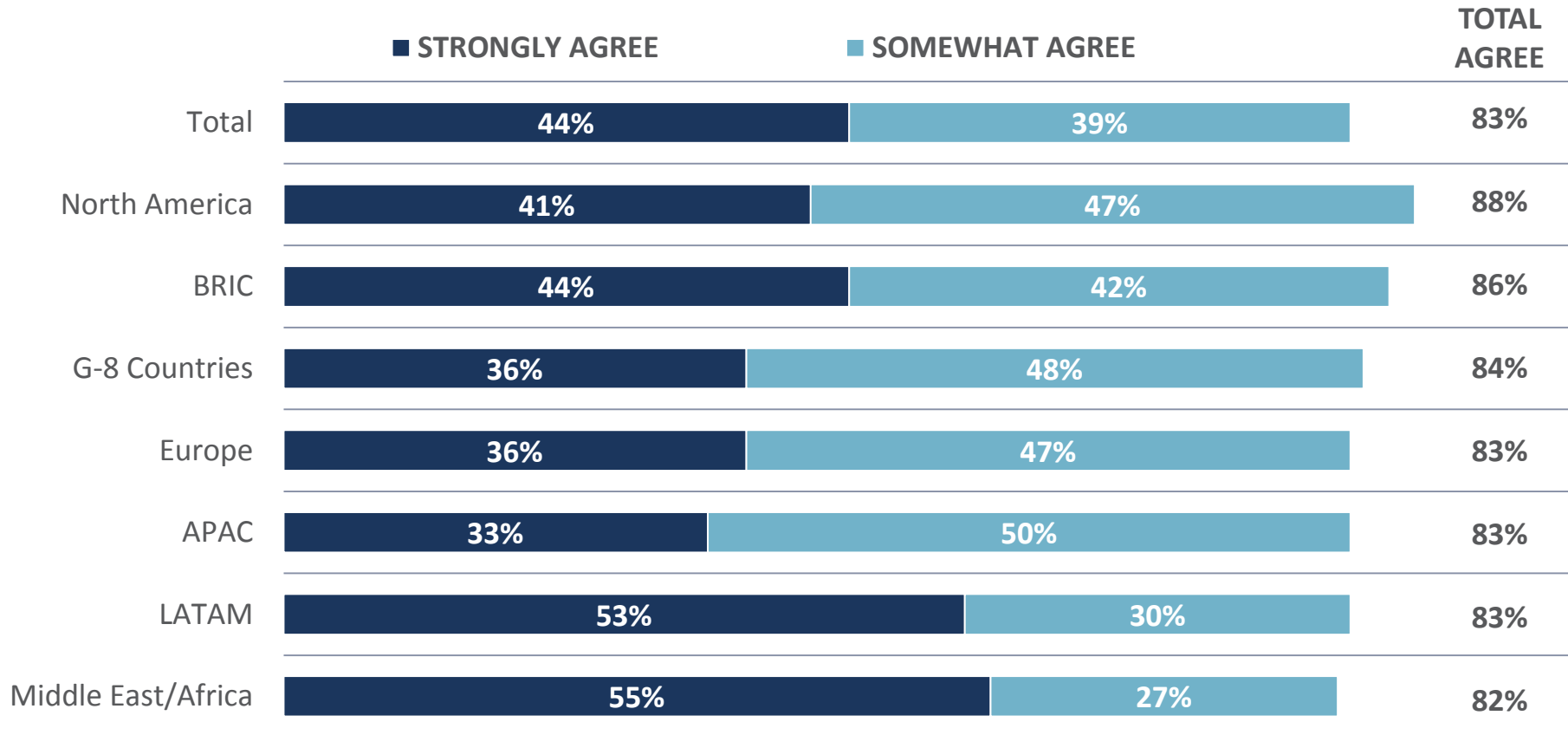
All country groups generally agree their government should work closely with other governments and organizations to address cyber security threats



Q10. To what extent do you agree or disagree with the following statements: [My government should work closely with other governments to address cybersecurity threats. My government should work closely with other organizations, including companies, civil society, academics, and technologists, to address cybersecurity threats.]

Base: All Respondents No Offline Countries (n=20,137)

North America and BRIC are more likely to agree there needs to be new rules about how companies, governments, and other internet users use personal data



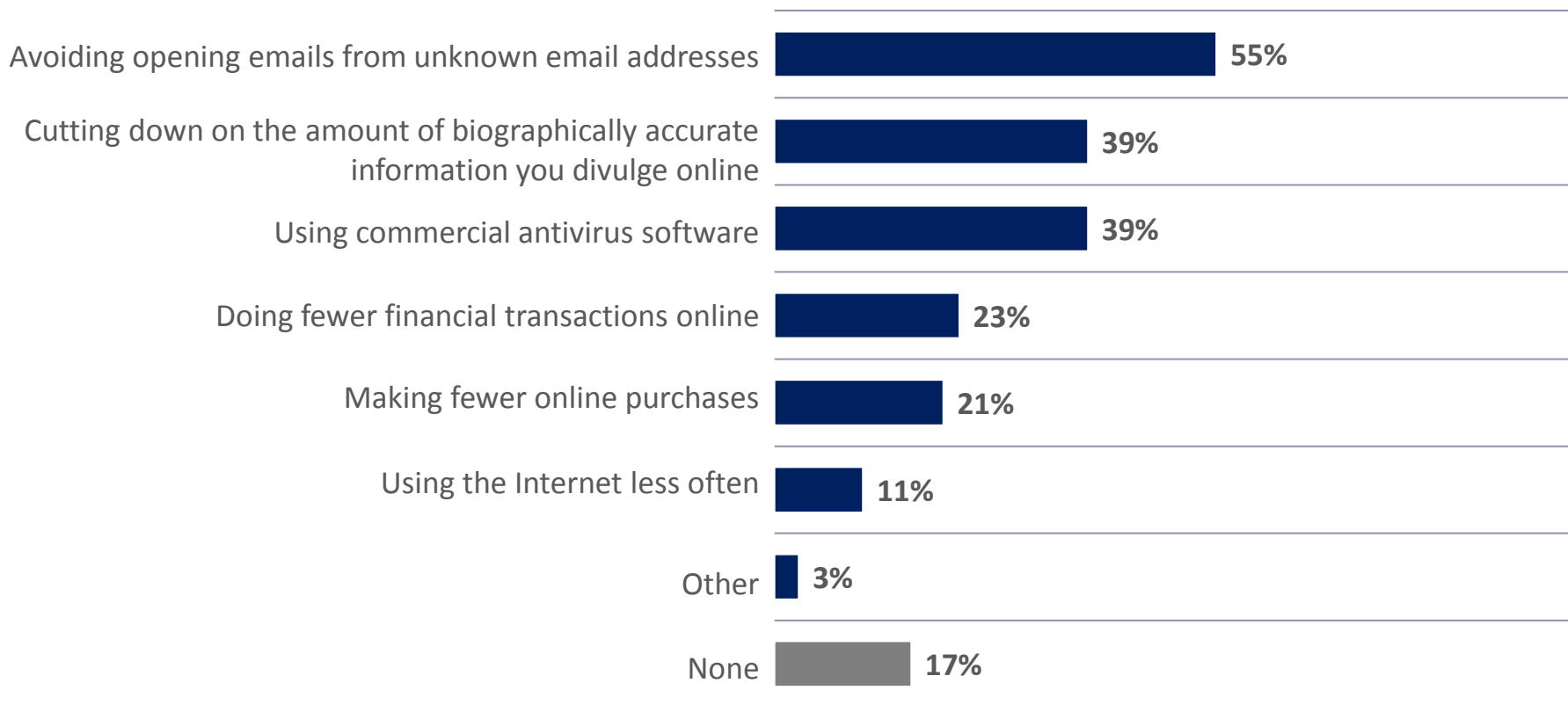
Q10. To what extent do you agree or disagree with the following statements: [My government should work closely with other governments to address cybersecurity threats. My government should work closely with other organizations, including companies, civil society, academics, and technologists, to address cybersecurity threats.]

Base: All Respondents No Offline Countries (n=20,137)

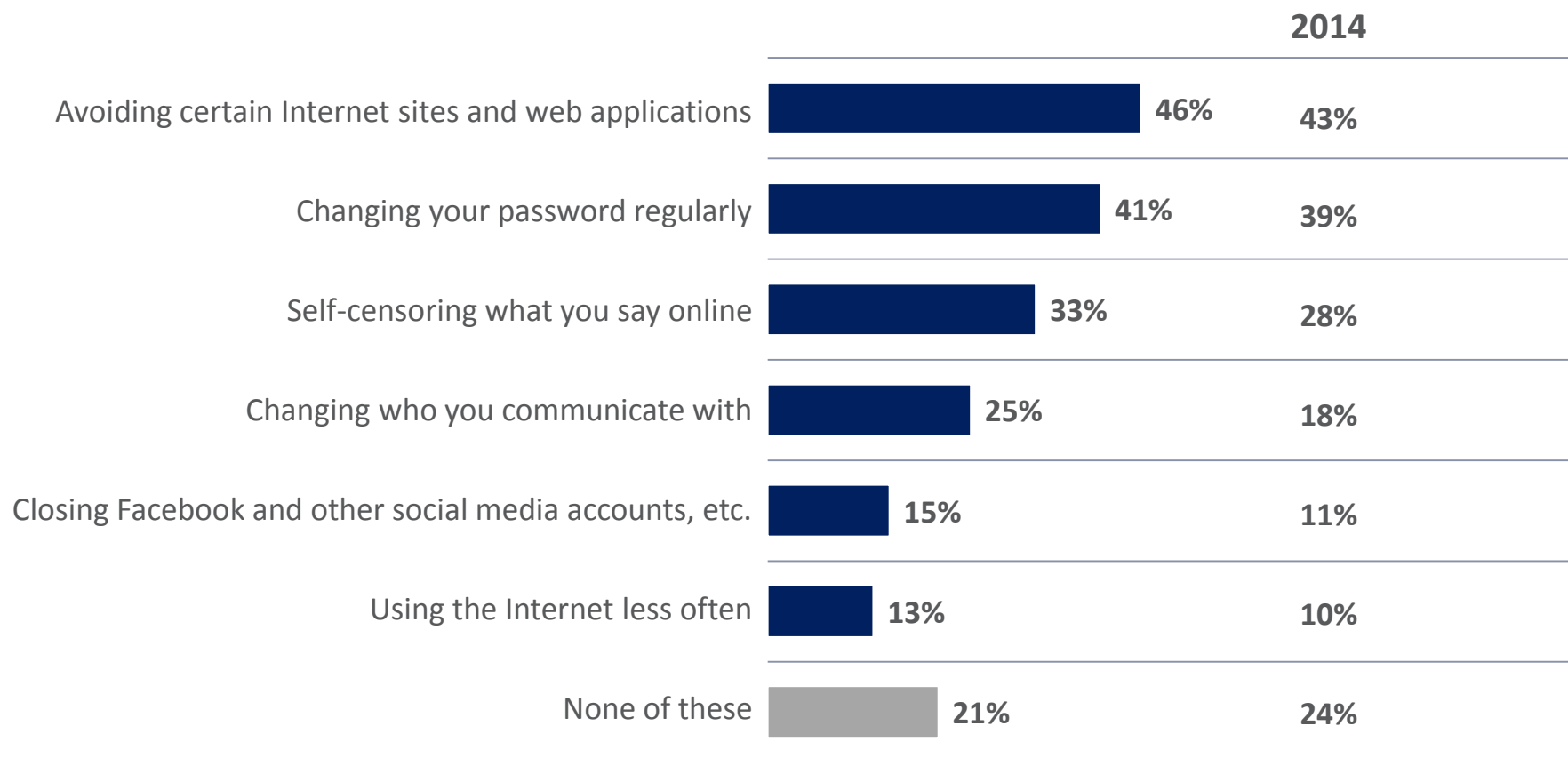
BEHAVIOUR CHANGES



Over half (55%) avoid opening emails from unknown addresses, and four in ten cut down on biographically accurate information given online and/or use commercial antivirus software (39%)



There has been a general increase in online behaviour changes compared to 2014, with avoiding certain websites and changing passwords remaining as the most mentioned changes

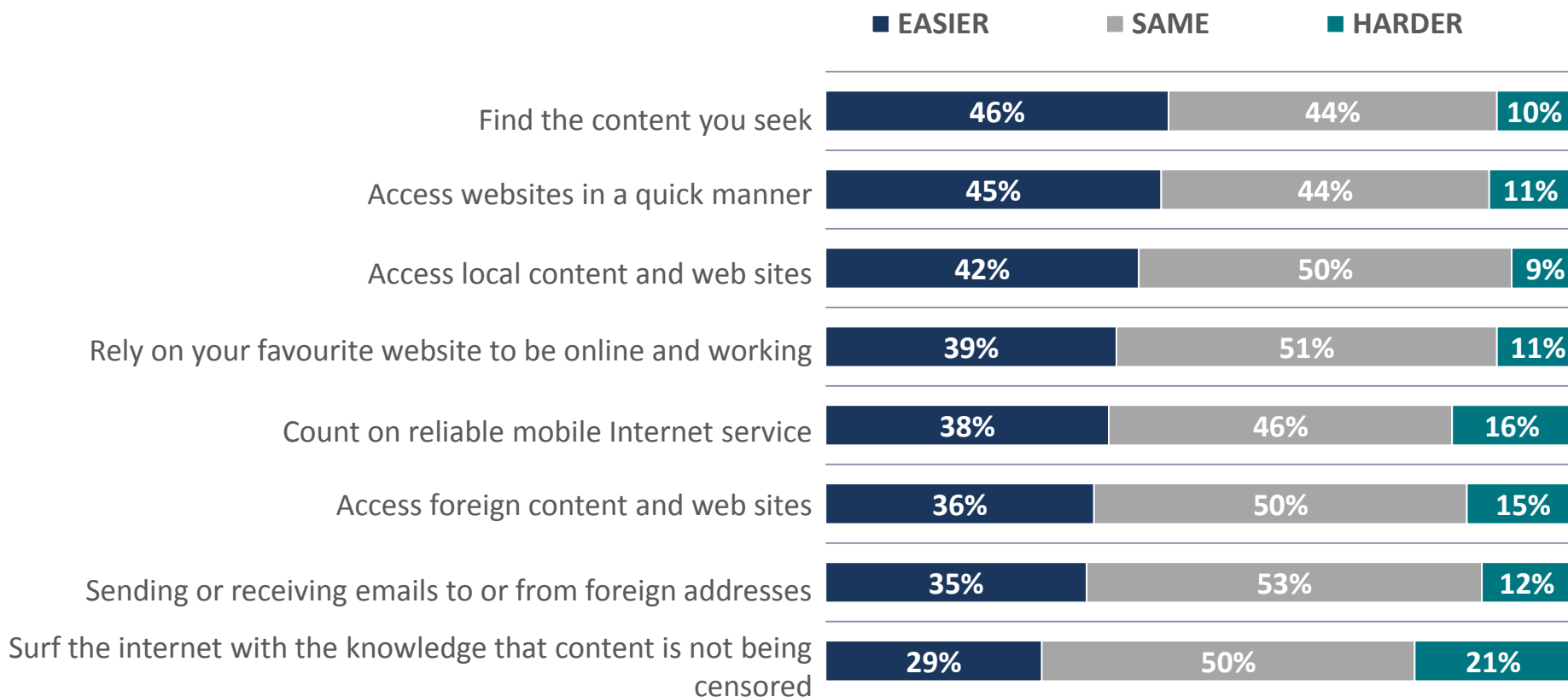




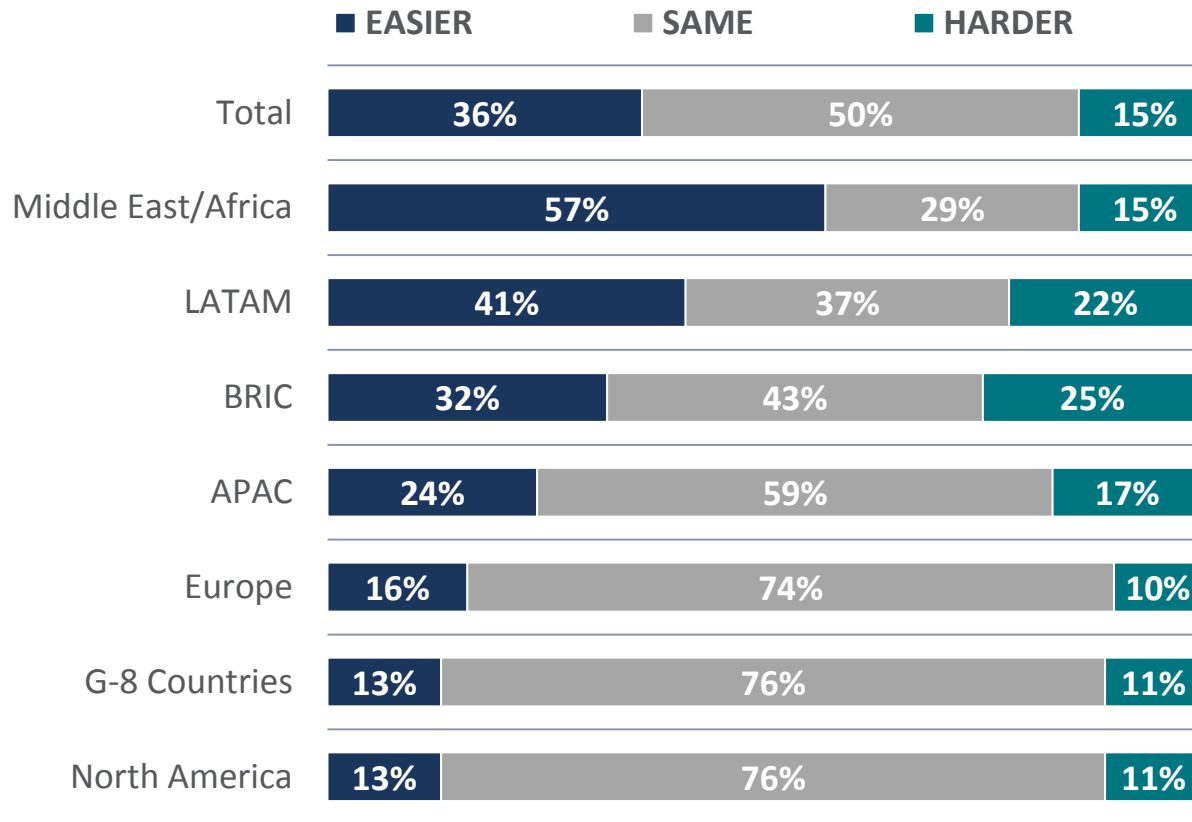
INTERNET ACCESS COMPARED TO ONE YEAR AGO

GLOBAL TOTAL

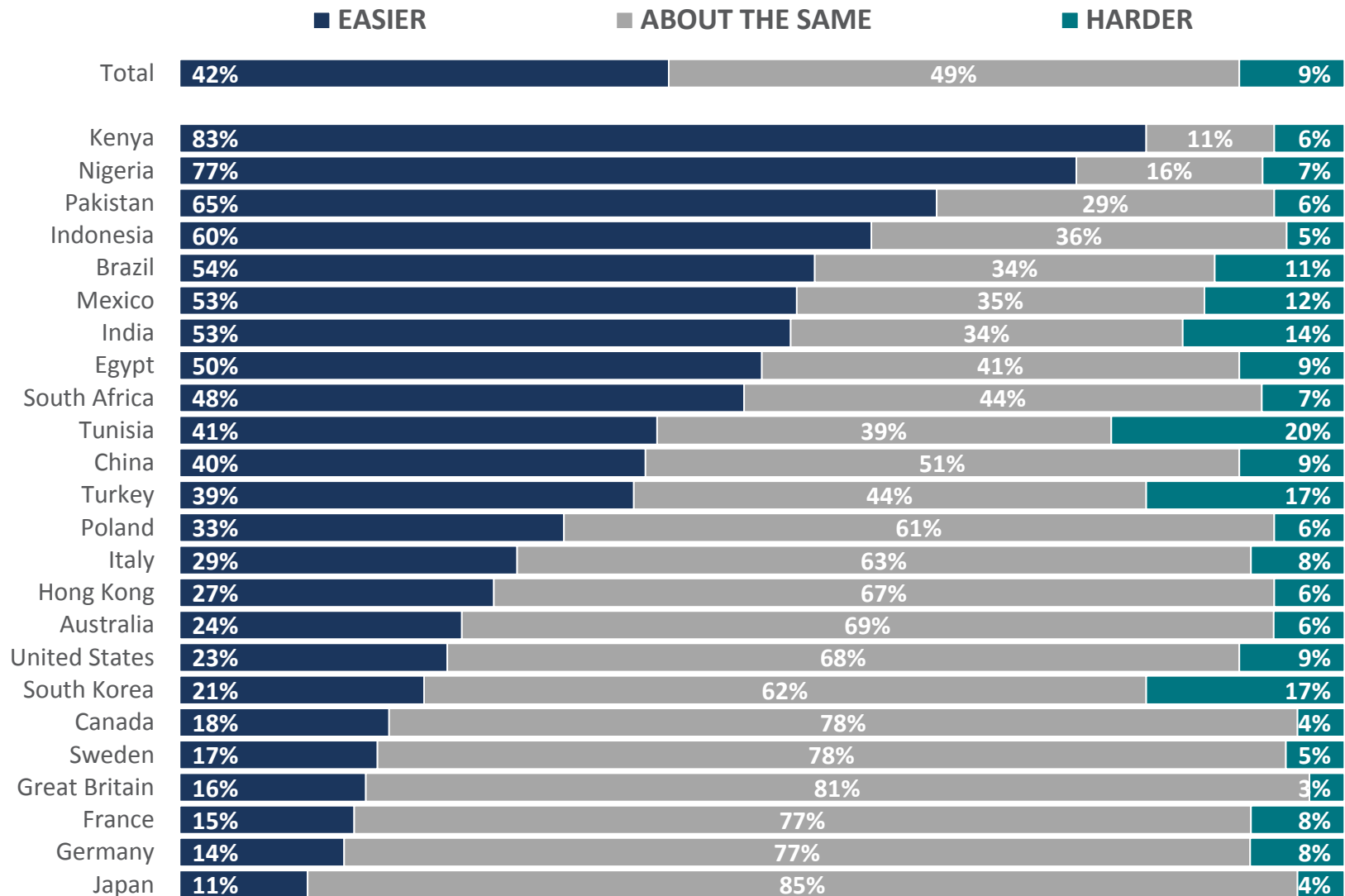
Finding and accessing websites and content are generally easier or the same compared to a year ago; none of the following activities are harder to do compared to one year ago

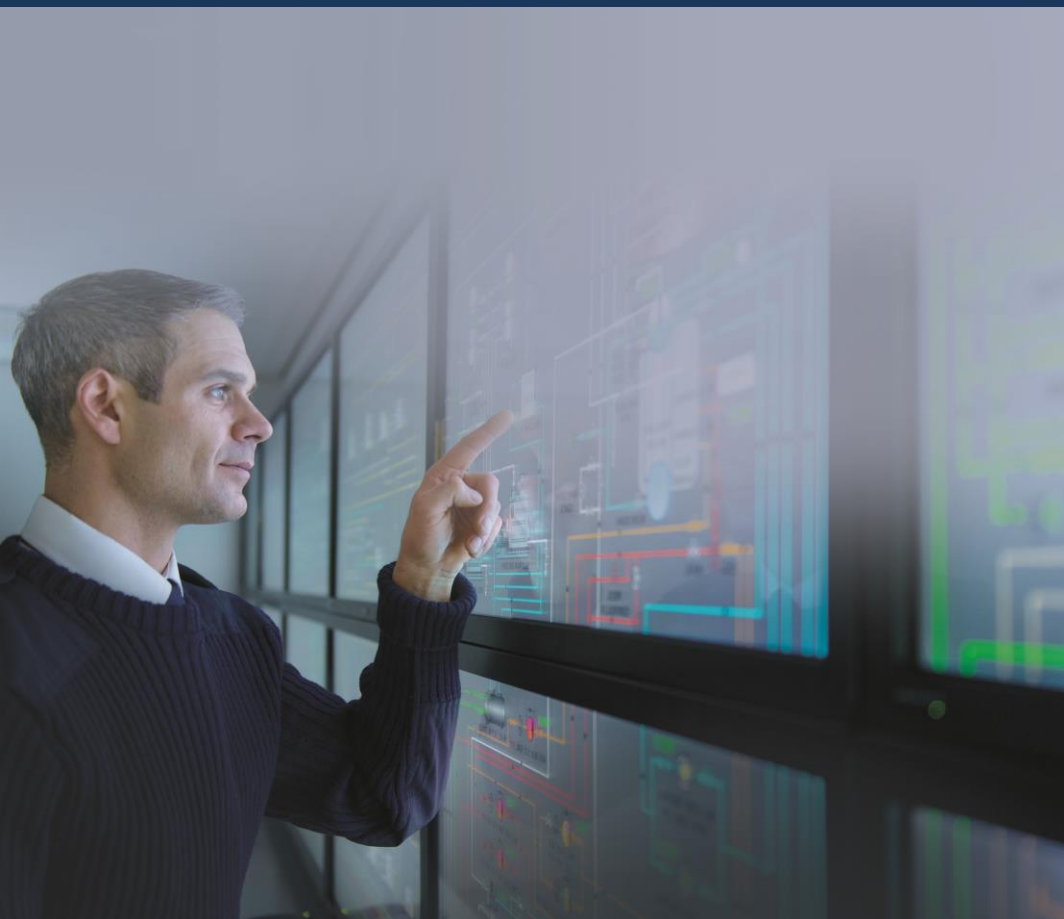


Middle East/Africa are much more likely to think it is easier to access FOREIGN CONTENT AND WEB SITES compared to a year ago



Over four in ten (42%) think it is easier to access LOCAL CONTENT AND WEB SITES compared to a year ago

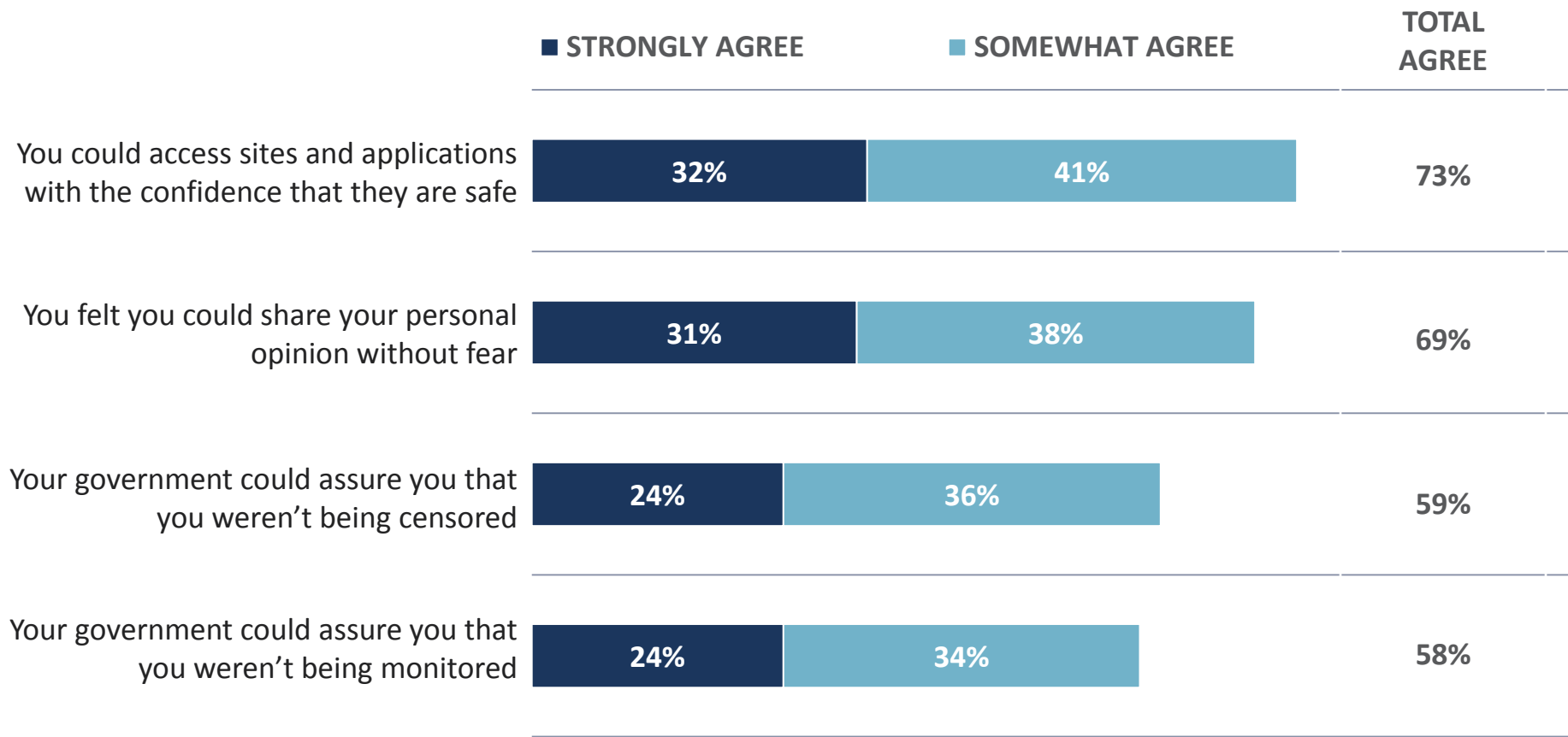




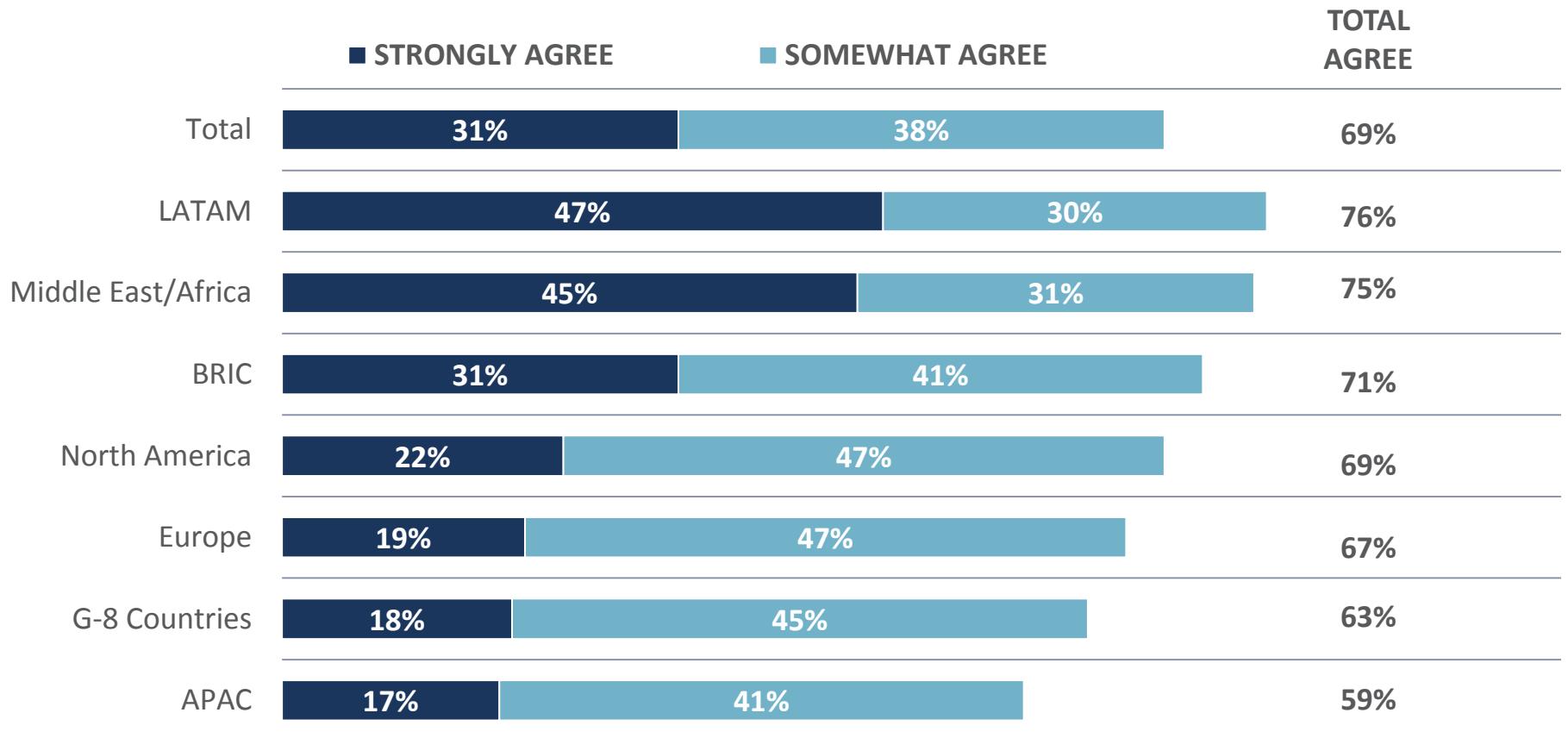
MONITORING AND CENSORING BY GOVERNMENT AND POLICE

GLOBAL TOTAL

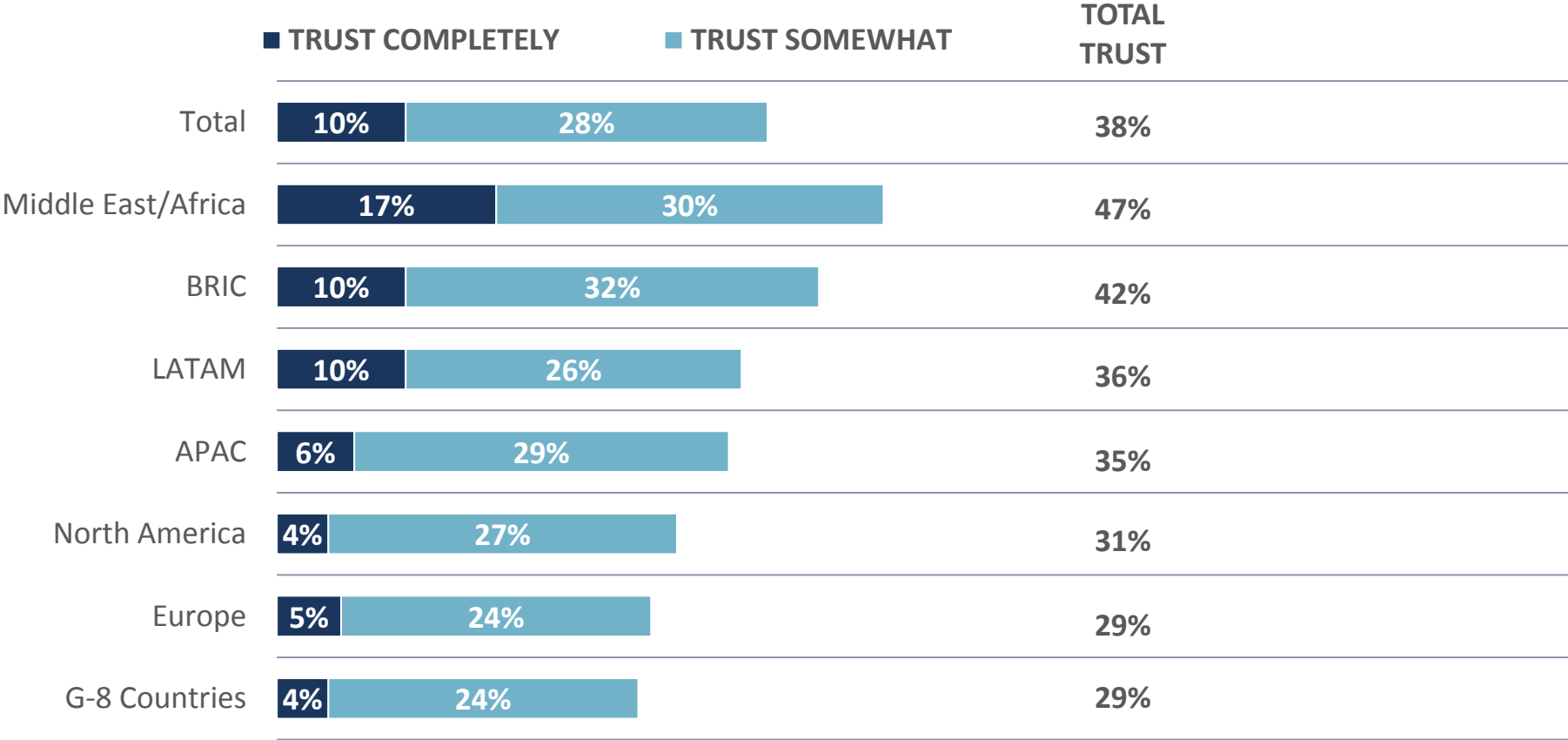
Individuals are more inclined to trust the internet if they could access sites and apps with the confidence they are safe and felt they could share personal opinion without fear



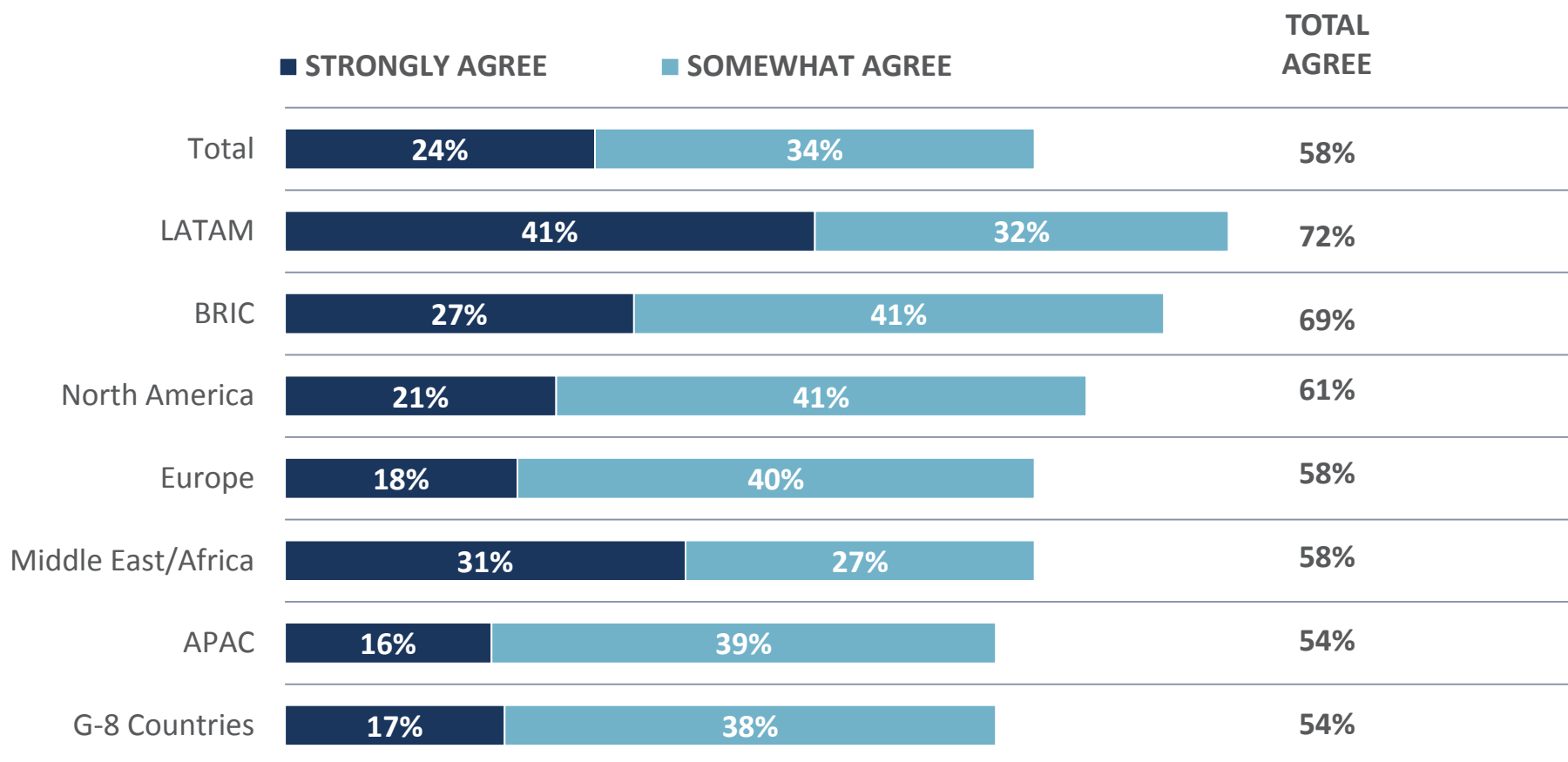
LATAM and Middle East/Africa are more likely to trust the internet more if they could SHARE THEIR PERSONAL OPINION WITHOUT FEAR



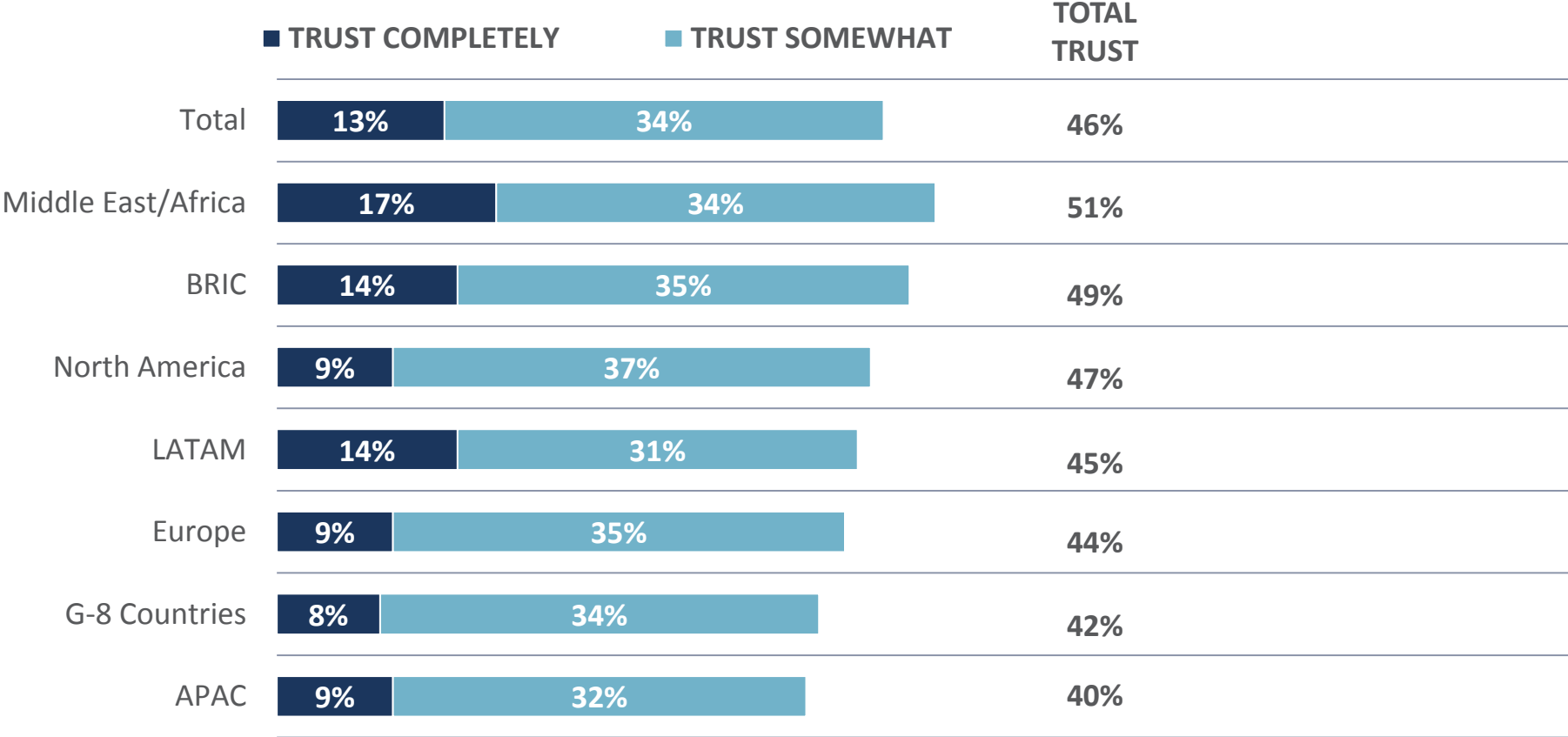
Europe and G-8 countries are most likely to be skeptical that their activities on the internet are not being MONITORED



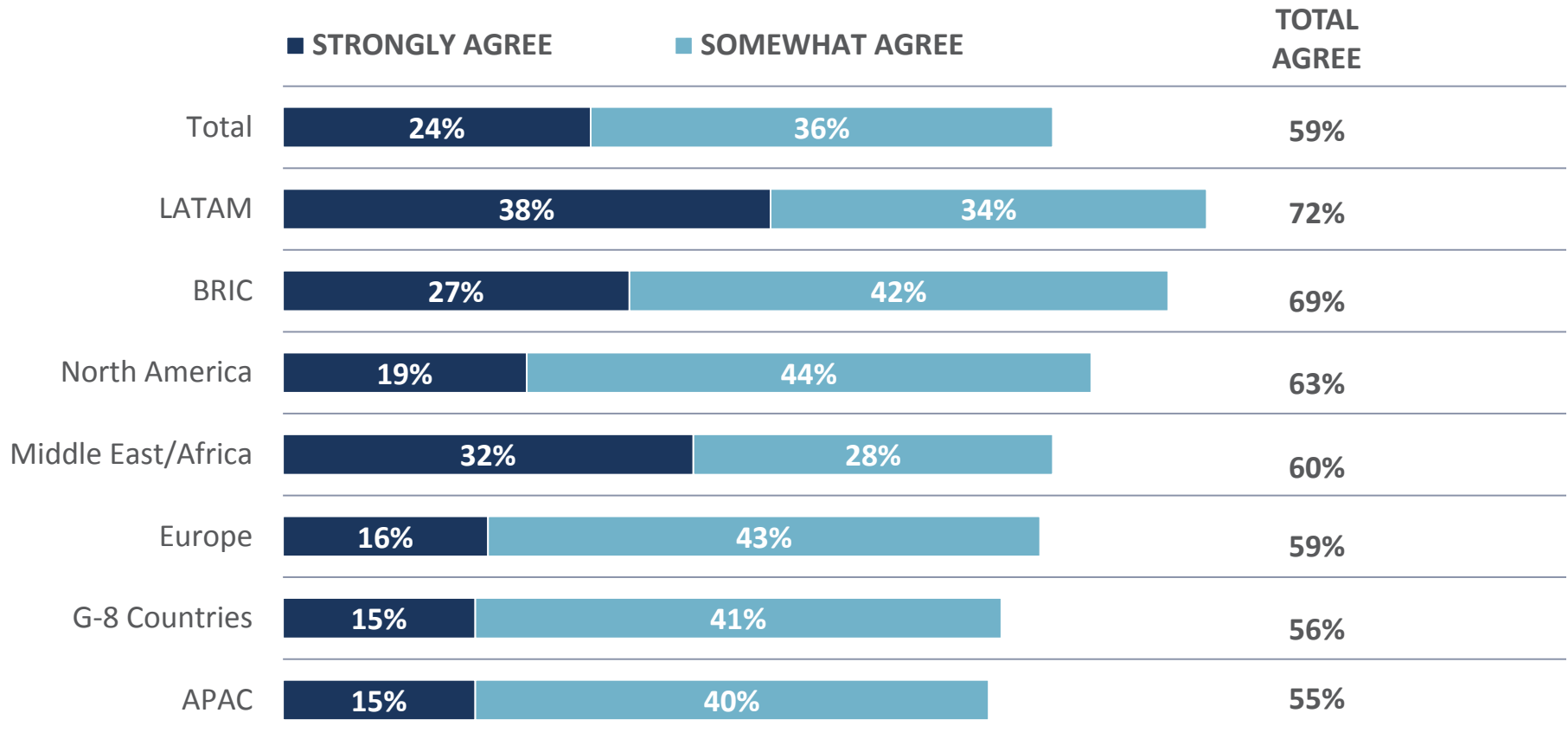
LATAM, BRIC, and North America are more likely to would trust the internet more if their government could ASSURE THEY WERE NOT BEING MONITORED

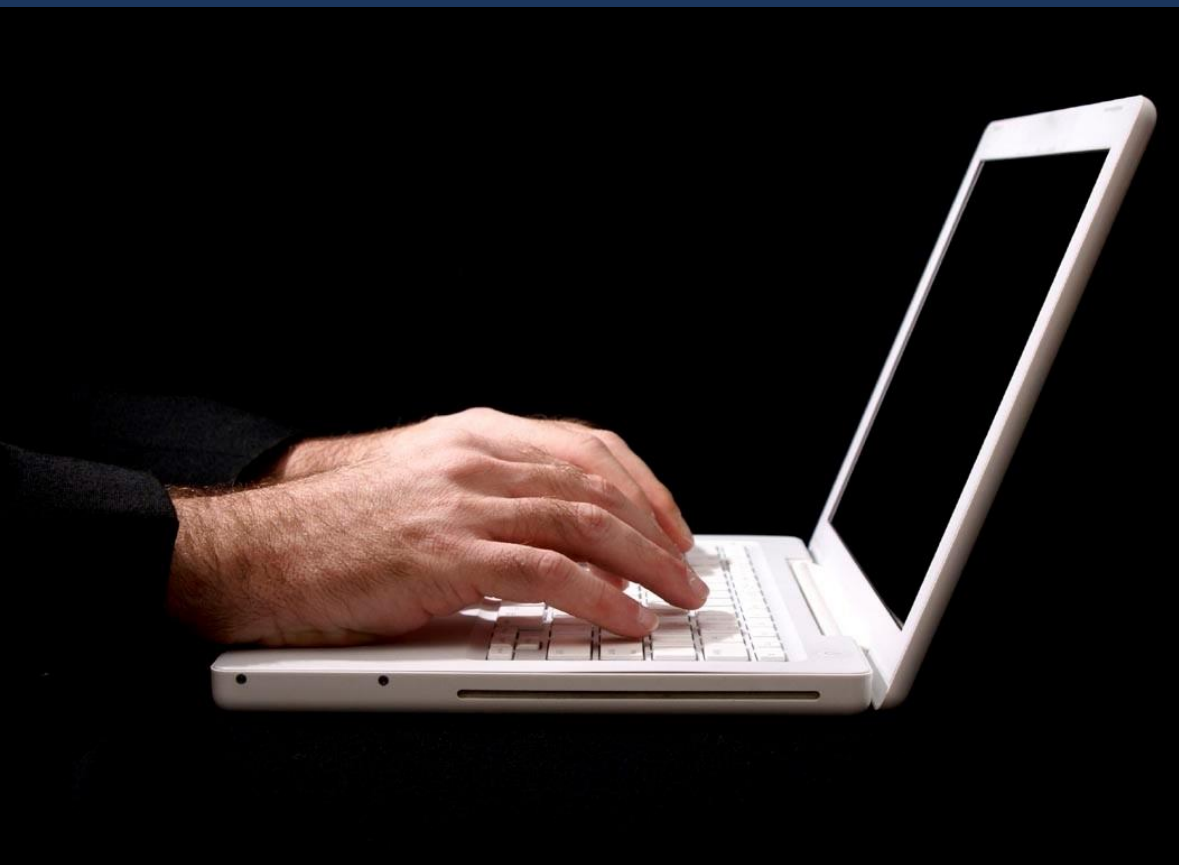


APAC and G-8 countries are most likely to be skeptical that their activities on the internet are not being CENSORED



LATAM, BRIC, and North America more likely to trust the internet more if their government could ASSURE THEY WERE NOT BEING CENSORED



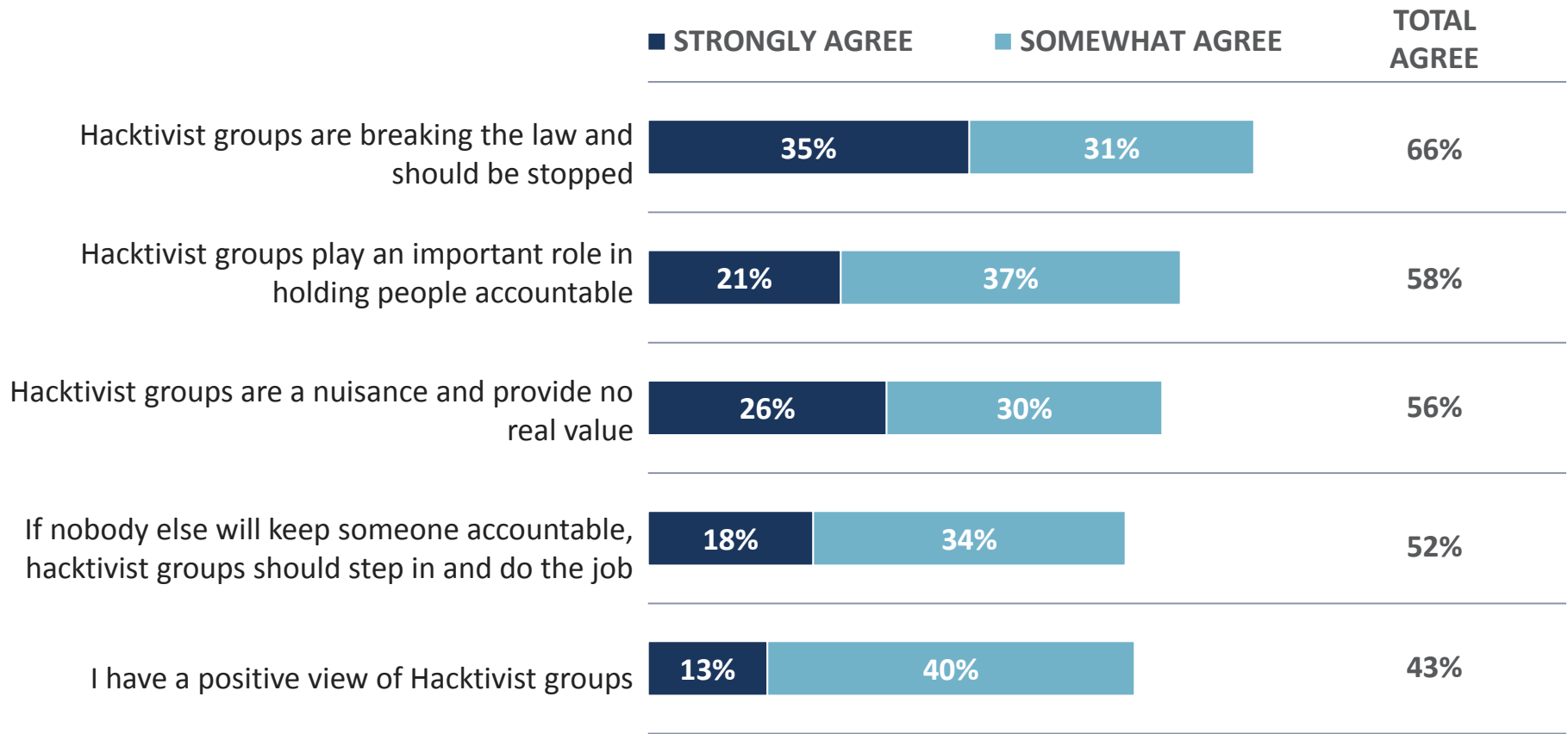


HACKTIVISTS

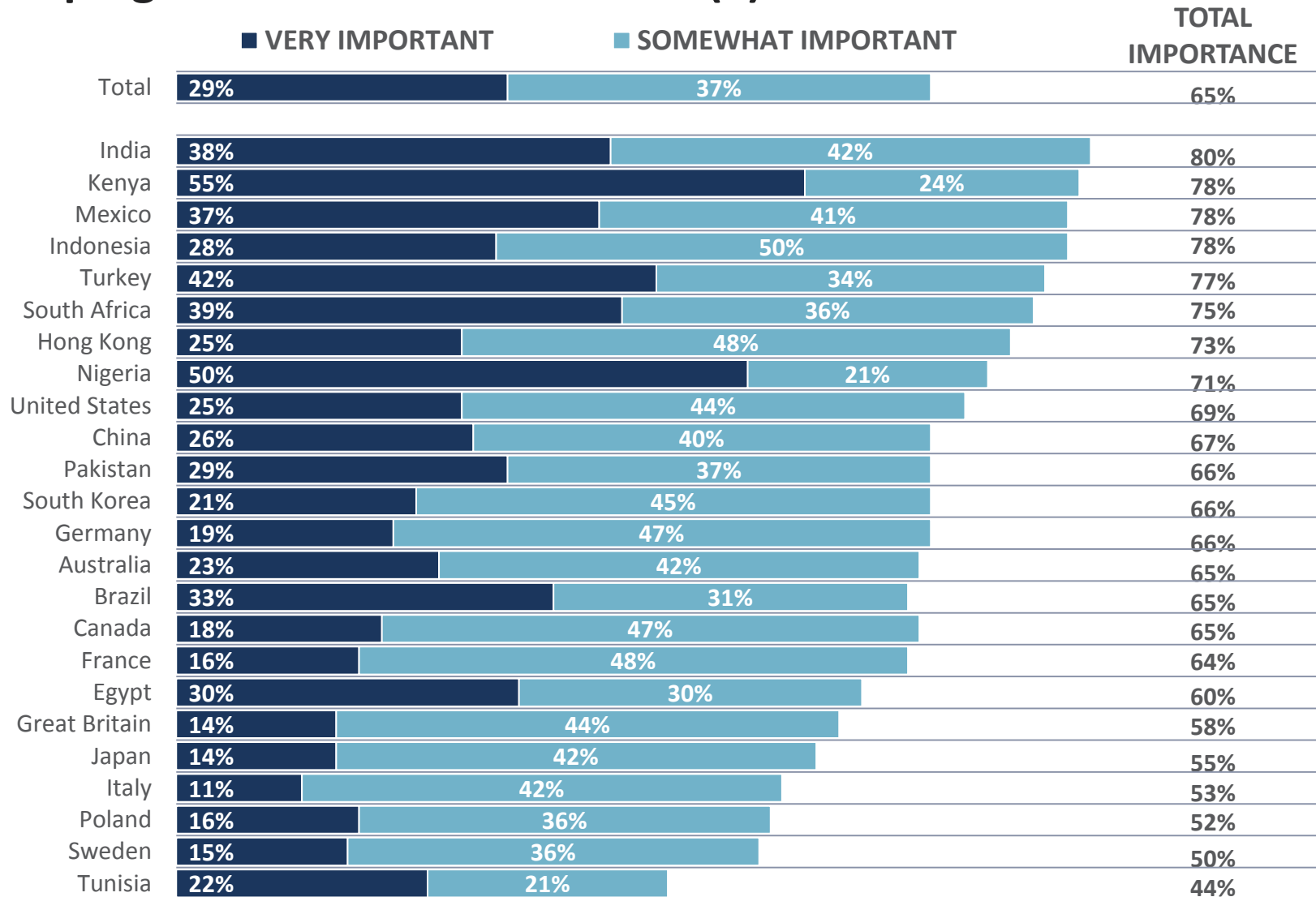
GLOBAL TOTAL



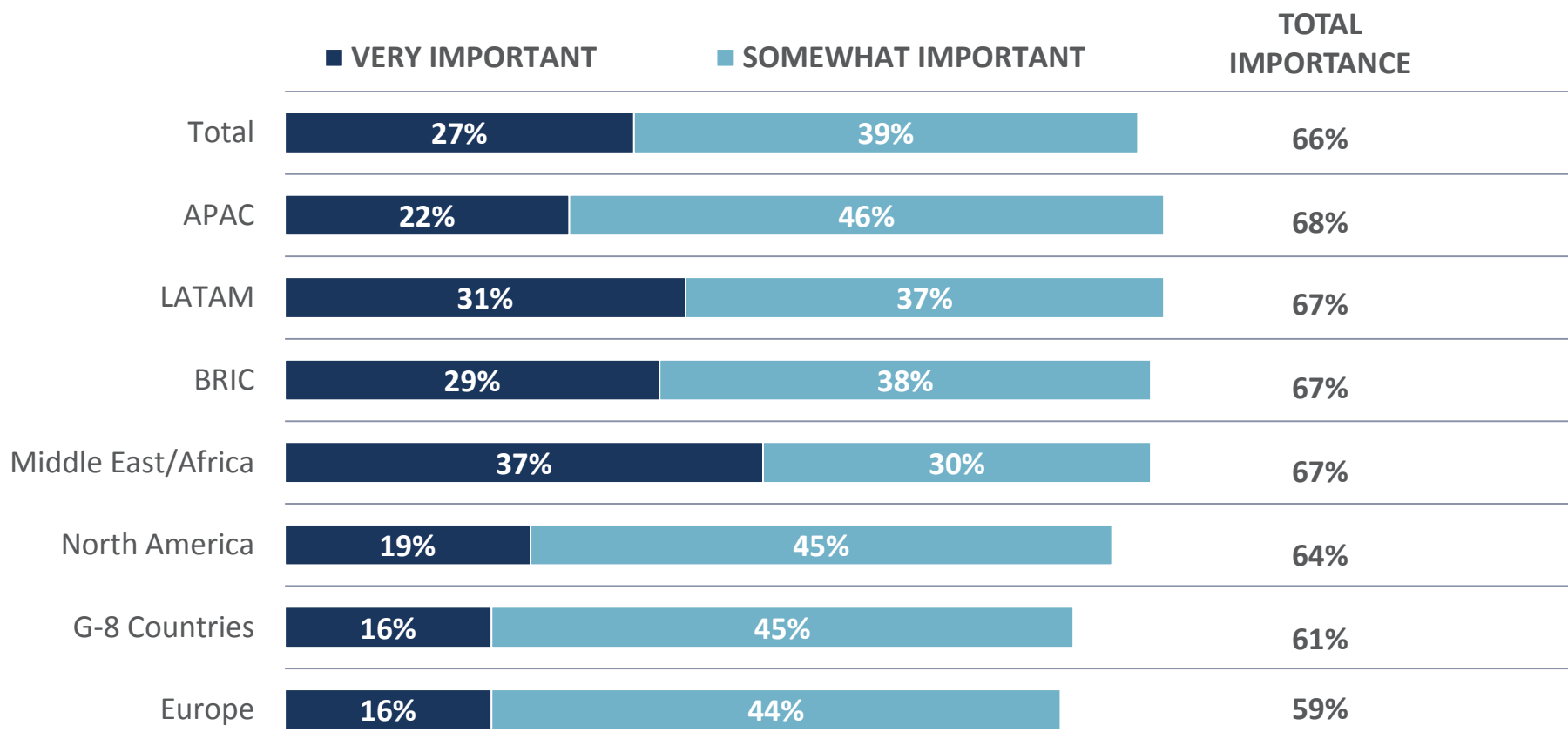
While a majority agree that hacktivist groups are breaking the law and should be stopped, only slightly fewer agree that hacktivists play an important role in holding people accountable



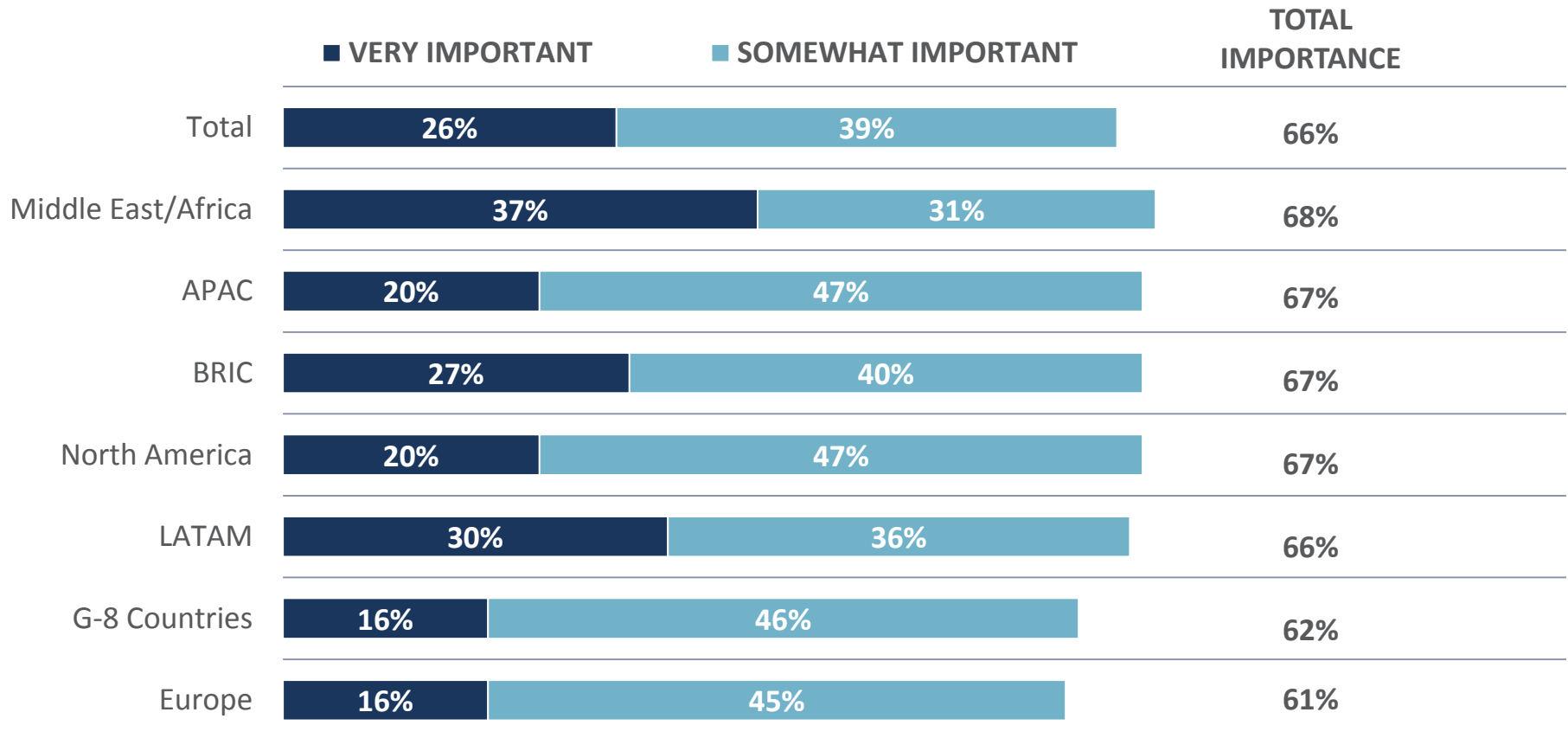
Two thirds (65%) think “hacktivists” play an important role in keeping their own GOVERNMENT(S) accountable



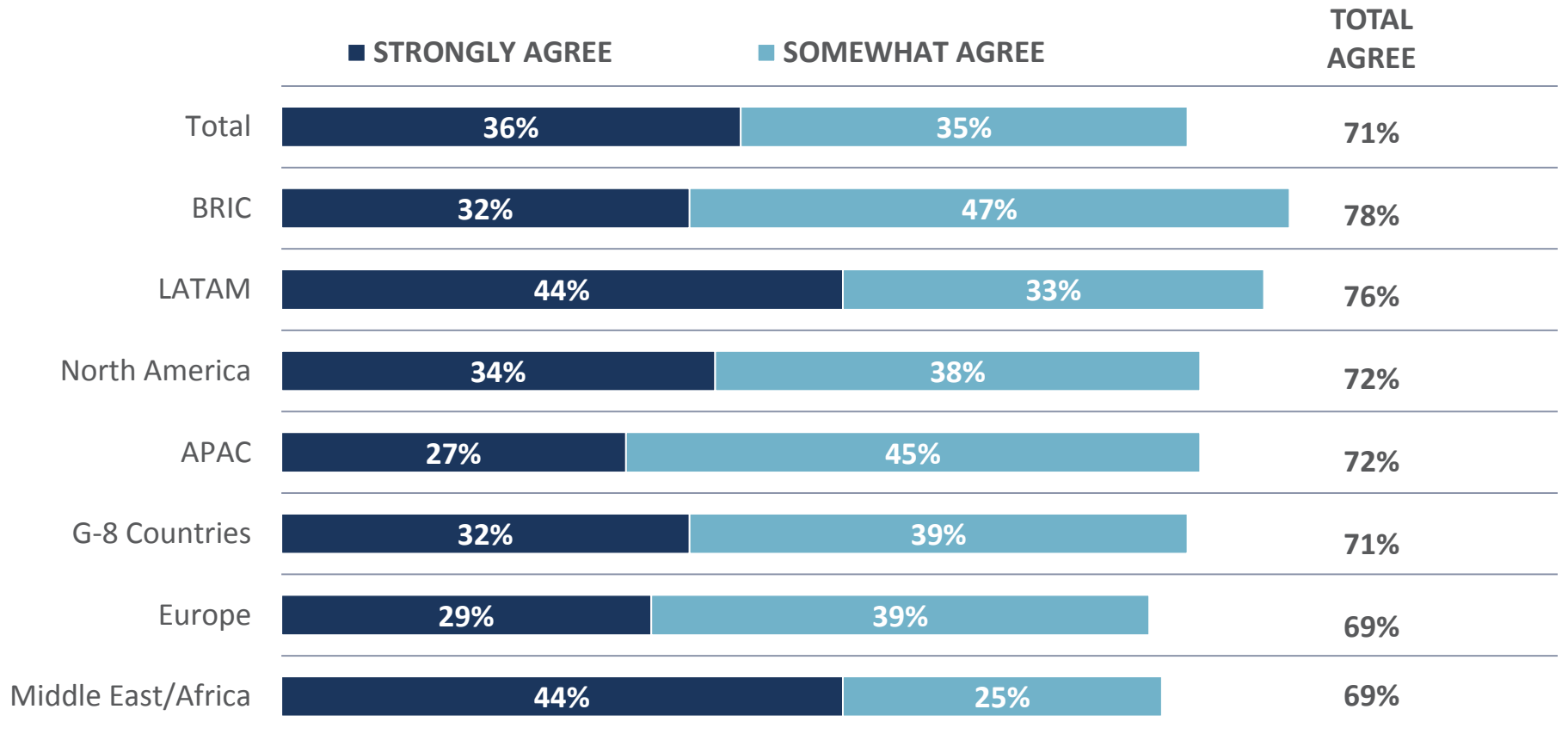
G-8 countries and Europe are also least likely to think “hacktivists” play an important role in keeping FOREIGN GOVERNMENTS accountable



G-8 and Europe are least likely to think “hacktivists” play an important role in keeping LARGE COMPANIES accountable



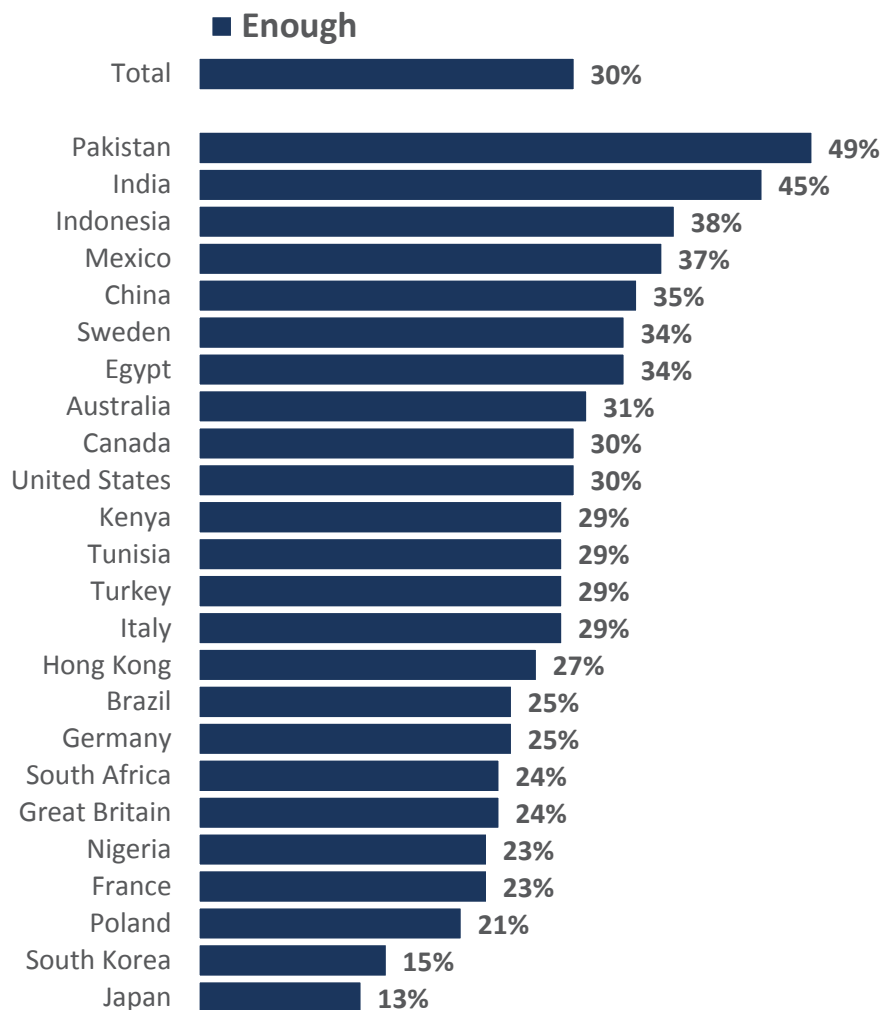
BRIC and LATAM are more likely to agree the “Darknet” should be shut down



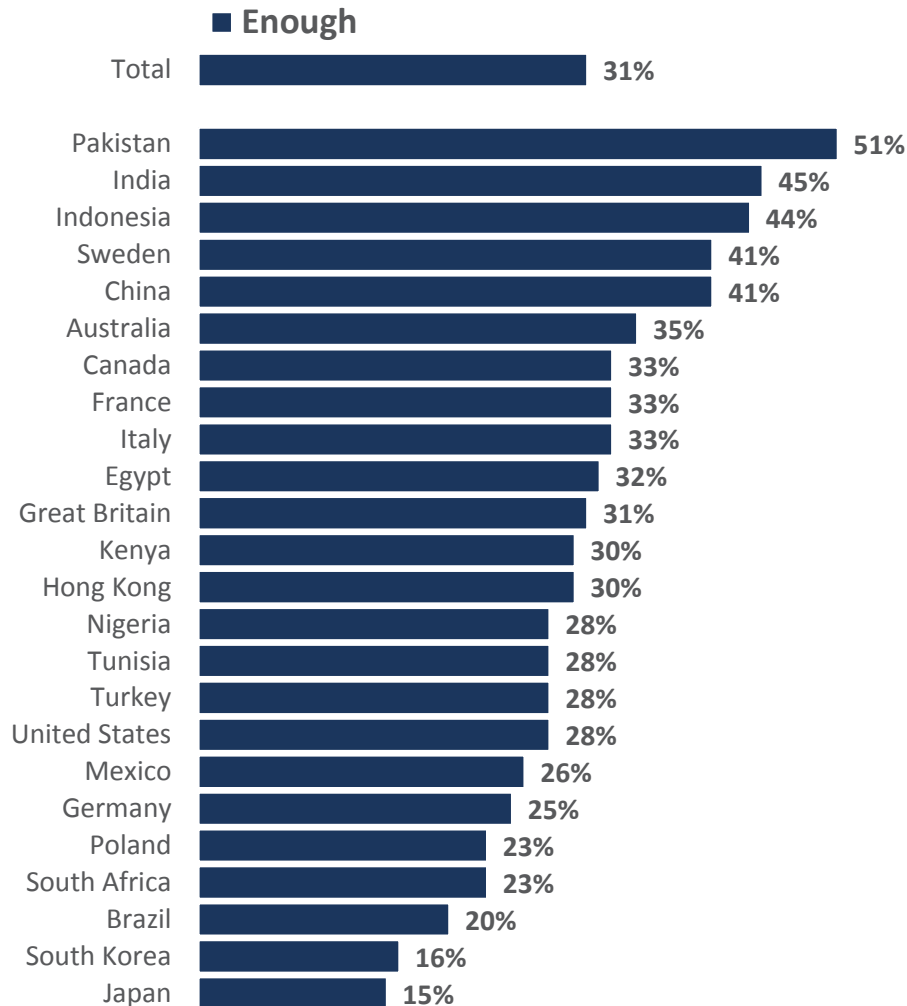


KEEPING INFORMATION SAFE & SECURE

Three in ten (30%) think the **GOVERNMENT IS DOING ENOUGH** to keep personal information secure and safe from **PRIVATE COMPANIES**

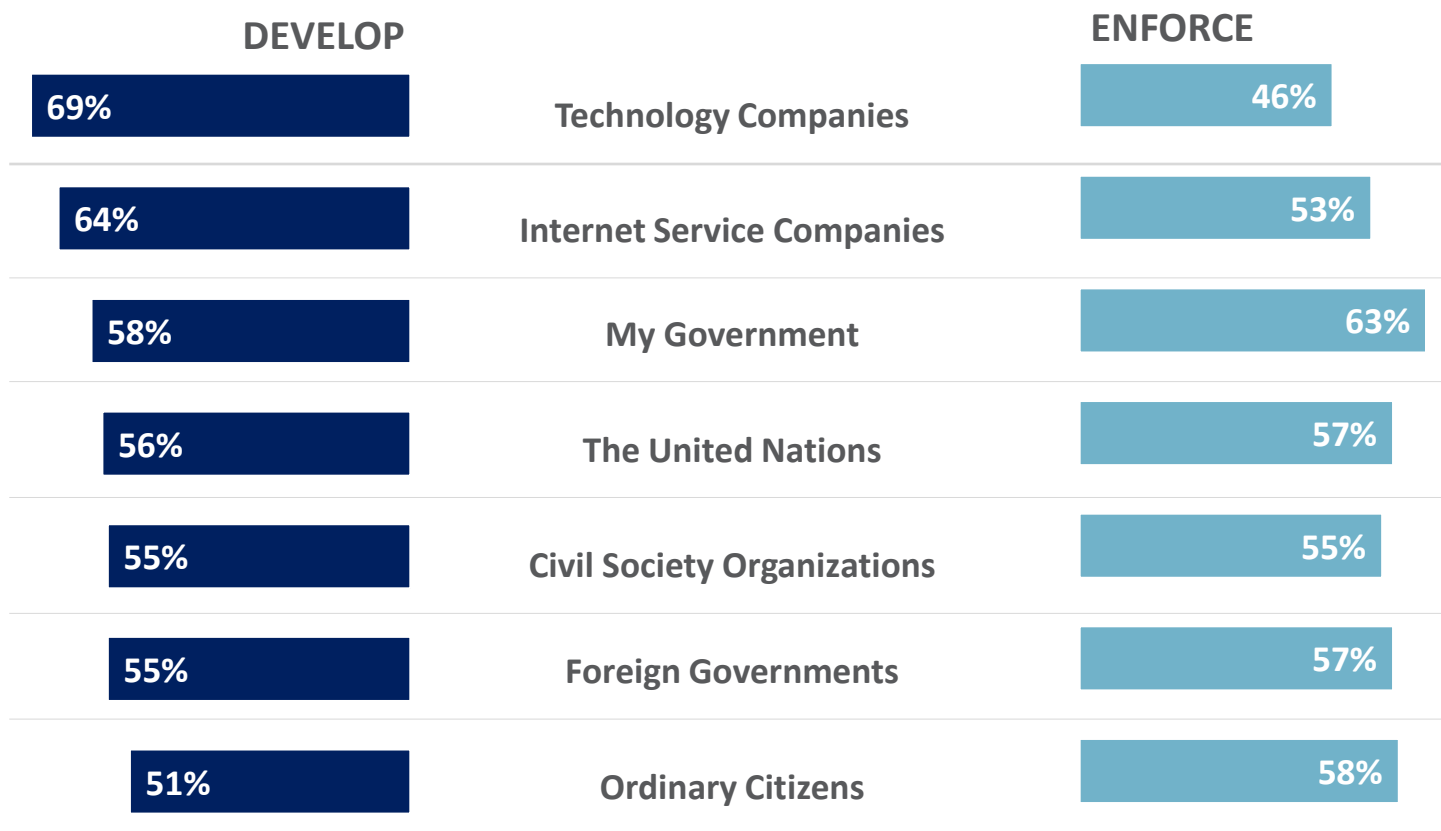


Three in ten (31%) think COMPANIES DO ENOUGH to keep personal information secure and safe from the GOVERNMENT



GLOBAL TOTAL

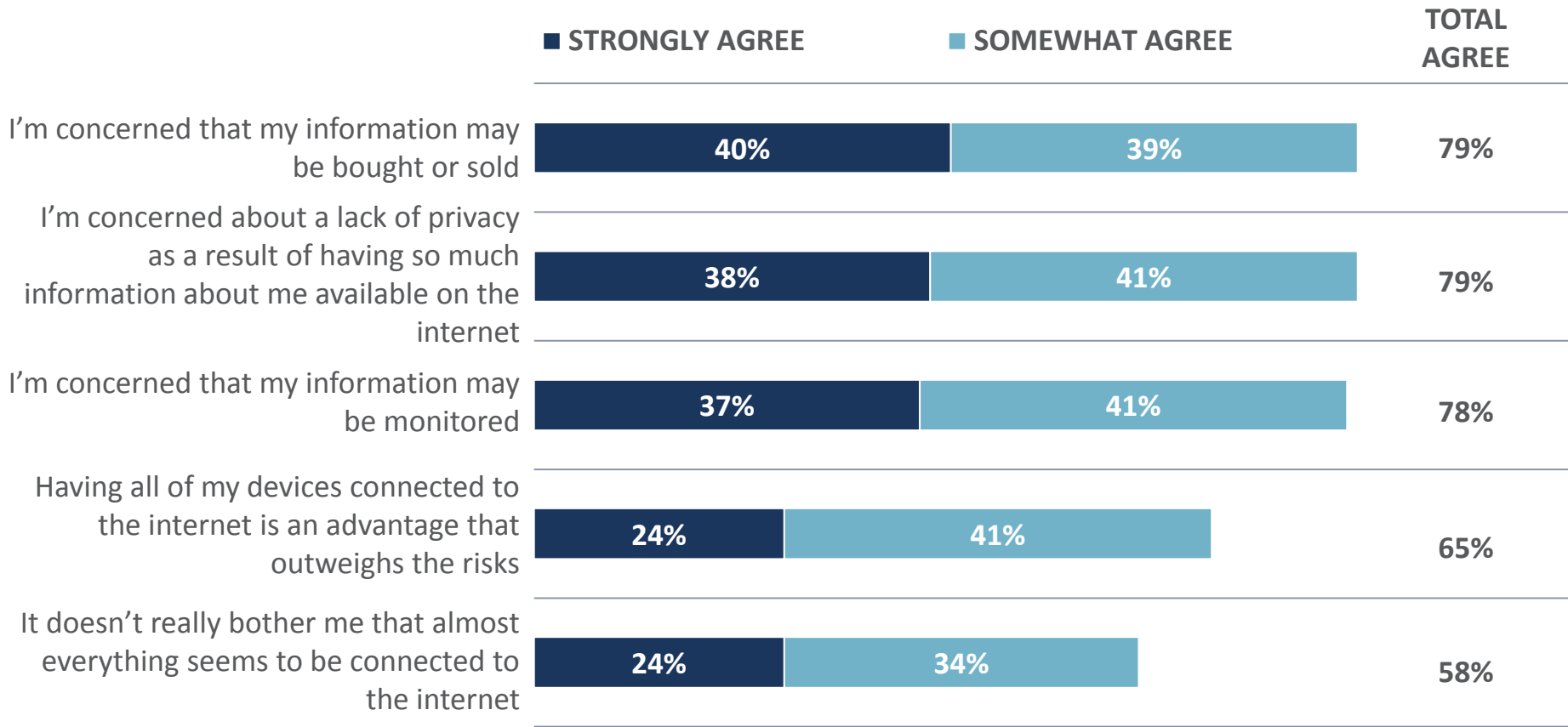
Technology companies are most likely to be seen as responsible for developing rules about how online data is used, however, the government is most likely to be seen as the enforcers of the rules



GLOBAL TOTAL



Individuals are relatively less likely to agree that having all devices connected to the internet is advantageous and that it doesn't matter that everything seems to be connected to the internet



CONCLUSIONS

-
- Worried about online privacy and security - *changes to behavior, expectations reflect this*
 - Growth of e-commerce contingent on growth of trust
 - Internet is not the “wild west” (*hacktivists, Darknet*)
 - Will concern grow with growth of technology?
 - No monopoly on trust, no immunity from responsibility
 - “Quis custodiet Ipsos custodes?”
 - Desire to see all stakeholders involved in creating and enforcing solutions
-



Fen Hampson

CIGI Distinguished Fellow
Director of the Global Security &
Politics Program
Centre for International
Governance Innovation


 fhampson@cigionline.org

 +1.519.885.2444 ext. 7201

Darrell Bricker

Chief Executive Officer,
Ipsos Global Public Affairs

 darrell.bricker@ipsos.com

 +1.416.324.2001

ABOUT IPSOS

Ipsos ranks third in the global research industry. With a strong presence in 87 countries, Ipsos employs more than 16,000 people and has the ability to conduct research programs in more than 100 countries. Founded in France in 1975, Ipsos is controlled and managed by research professionals. They have built a solid Group around a multi-specialist positioning – Media and advertising research; Marketing research; Client and employee relationship management; Opinion & social research; Mobile, Online, Offline data collection and delivery.

Ipsos is listed on Eurolist – NYSE – Euronext. The company is part of the SBF 120 and the Mid-60 index and is eligible for the Deferred Settlement Service (SRD).

ISIN code FR0000073298, Reuters ISOS.PA,
Bloomberg IPS:FP

www.ipsos.com

GAME CHANGERS

At Ipsos we are passionately curious about people, markets, brands and society. We deliver information and analysis that makes our complex world easier and faster to navigate and inspires our clients to make smarter decisions.

We believe that our work is important. Security, simplicity, speed and substance applies to everything we do.

Through specialisation, we offer our clients a unique depth of knowledge and expertise. Learning from different experiences gives us perspective and inspires us to boldly call things into question, to be creative.

By nurturing a culture of collaboration and curiosity, we attract the highest calibre of people who have the ability and desire to influence and shape the future.

“GAME CHANGERS” – our tagline – summarises our ambition.