NortonLifeLock™

MARCH 30, 2020

2019 CYBER SAFETY INSIGHTS REPORT GLOBAL RESULTS

PREPARED BY

The Harris Poll

Harris Insights & Analytics LLC, A Stagwell Company

Survey Method

The research was conducted online by The Harris Poll on behalf of NortonLifeLock among 10,063 adults (aged 18+) in 10 countries. The survey was conducted November 5 to December 2, 2019 in Australia (n=1,006), France (n=1,001), Germany (n=1,003), India (n=1,017), Italy (n=1,012), Japan (n=1,002), Netherlands (n=1,007), New Zealand (n=1,009), UK (n=1,005), and US (n=1,001). Data are weighted where necessary to bring them in line with their actual proportions in the population; India was weighted to the population of those who are online. Weighted variables varied by country and included one or more of the following: age, gender, race/ethnicity, region, education, employment, income, marital status, internet usage, language proficiency, household size, household income, socioeconomic status, locale, and propensity to be online. A global postweight was applied to ensure equal weight of each country in the global total. No estimates of theoretical sampling error can be calculated.

Due to changes in countries included in the 2018 versus 2019 survey, year over year trending is shown at the country level only.

Table of Contents

KEY FINDINGS

Key Findings

With over a third of consumers across 10 countries (roughly 350 million people) experiencing cyber crime in the last year alone, consumers are understandably concerned about their privacy and attempting to take action to protect it. However, despite taking precautionary steps, many feel it's too late or even impossible to protect their privacy. Two-thirds report being more alarmed than ever about their privacy (67%) and are very worried their identity will be stolen (66%), with 92% expressing at least some concern when it comes to data privacy. Two in three (66%) have at times chosen not to download a certain app or use a specific service solely based on its privacy policy, and over a third (37%) have chosen not to purchase a smart home device due to privacy or security concerns.

While the majority (84%) also report having taken at least one step to protect their online activities and personal information, most are taking basic steps (clearing cookies, limiting information shared on social media) with fewer going to greater lengths (using anonymous payment methods, deleting social media accounts, using a VPN). Despite this, over 6 in 10 feel it's impossible to protect their privacy (64%) or that it is too late to do so (60%). Importantly though, consumers largely don't feel they should own responsibility for ensuring their information is protected as half (52%) believe that individuals should be held *least* responsible (compared to companies and the government) for ensuring their own information is protected.

[1] Most common steps taken are clearing or disabling cookies (44%) or limiting information shared on social media (44%). See slide 15 for other steps taken.

Key Findings

Globally, it is governments that are expected to bear the most responsibility for protecting personal information, despite a general lack of trust and confidence in them to do so. Fewer consumers are trusting of government than most other organizations when it comes to managing and protecting their personal information[1] and less than half (44%) believe their government is doing enough when it comes to data privacy and protecting personal information. Yet, more consumers believe that government (42%) should be held *most* responsible in doing so than the companies collecting the information (34%) or the individuals supplying it (24%).

Companies faulted for not doing enough to protect personal information, making privacy policies vague and difficult to understand, and not providing choices. Much like the sentiments around government, less than half of consumers (43%) believe that companies are doing enough when it comes to data privacy and protecting personal information. And with regards to privacy policies, nearly all consumers (95%) admit they don't always read them, most of whom say its because they are too confusing (73%) or they feel they have no choice but to accept them in order to use an app or service (78%). Importantly, a majority (82%) say they would be more willing to read policies if they were given choices about how their information could be used. In fact, consumers are just about four times more likely to prefer an opt-out option (79%), preventing companies from selling their personal information in exchange for lower prices, to an opt-in option (21%).

Even among those who do read privacy policies, more than half (55%) say they usually don't understand them and 80% of all consumers go as far as saying that companies make privacy policies vague and difficult to understand on purpose.

[1] More consumers trust healthcare providers (89% a lot or a little), retailers/online shopping sites (82%), internet service providers (81%), financial institutions (79%), and smart device manufacturers (74%) than they do government (72%) when it comes to managing and protecting personal information. The only organization less trusted than government is social media providers (57%).

Key Findings

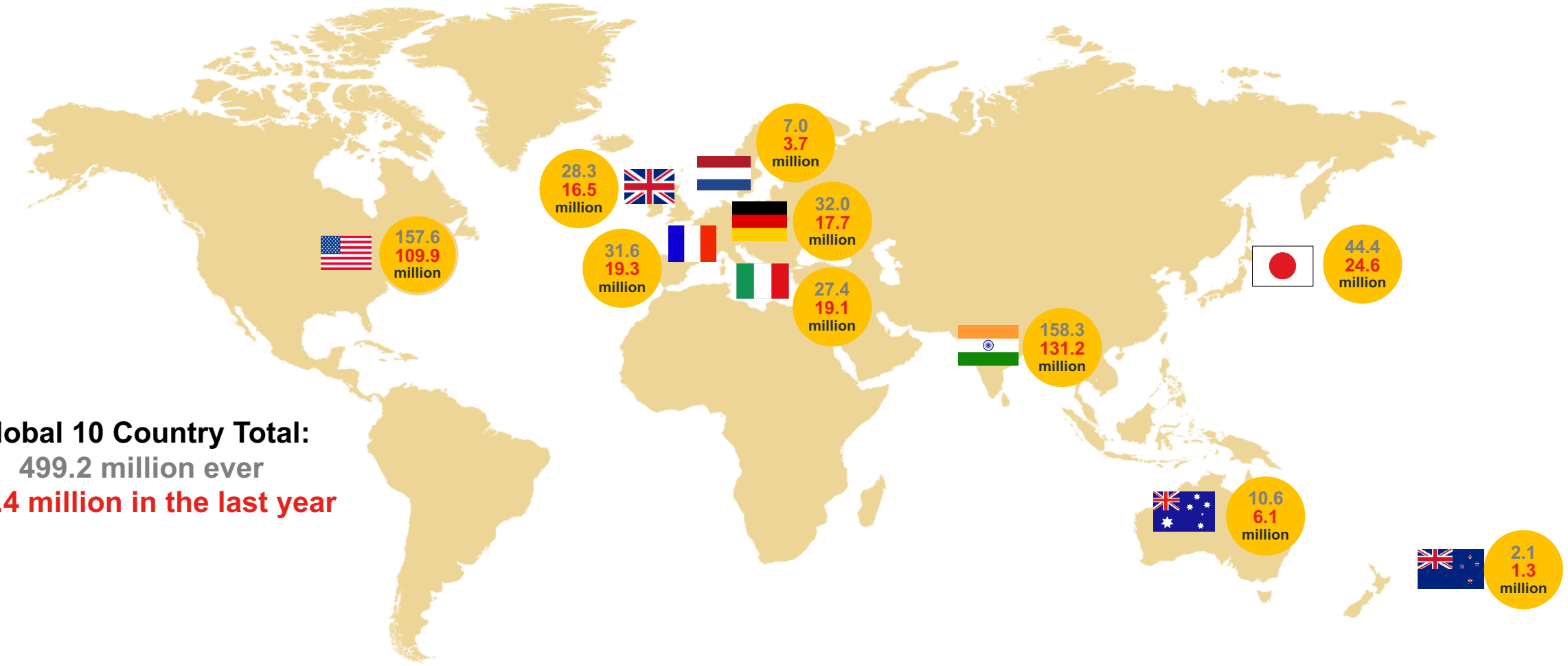
Consumers report some, though not a lot of, knowledge about facial recognition and where it's currently being used. And while concerns exist, majorities support its use among law enforcement, schools, and even retailers. Most consumers say they have only heard the name (42%) or are somewhat familiar (37%) with facial recognition. While consumers overwhelmingly think businesses (87%) and government (86%) should be required to inform/report when or where they are using facial recognition, half or fewer believe its currently being used in public spaces like airports (50%), government buildings (36%), or banks (31%). Less than 1 in 10 think its being used in stores (9%) or restaurants or bars (6%).

Cyber criminals accessing or manipulating facial recognition data to steal their identity (39%) is consumers' largest concern[1], with 62% agreeing that facial recognition will likely be abused or misused in the coming year and 45% believing it will do more harm than good. Despite these concerns, when presented with possible advantages and disadvantages of using facial recognition, most consumers would support the use among law enforcement (69%), schools (63%), and to a lesser extent retailers (54%), despite some of the risks.

[1] Respondents were asked to select up to 2 concerns

CYBER CRIME: INCIDENCE AND IMPACT

Almost 500 Million Consumers* Have Ever Been the Victim of a Cyber Crime; Nearly 350 Million in the Last Year Alone



Global 10 Country Total:

499.2 million ever

349.4 million in the last year

*The 2019 NortonLifeLock Cyber Safety Insights Report surveyed 10 countries. In 2018, 16 countries were surveyed.

More Than Half of Consumers Have Experienced a Cyber Crime, With Around 1 in 3 Falling Victim in the Past 12 Months Alone

Have Ever Experienced a Cyber Crime

56%

Experienced a Cyber Crime in the Past 12 Months

36%

% Who Have Experienced Cyber Crime by Country

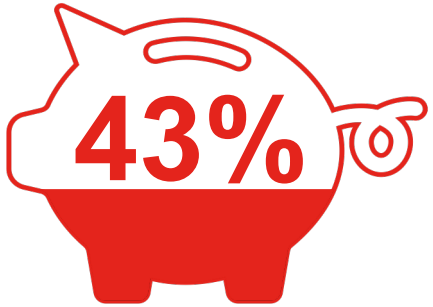
	Ever	Past 12 months	*P12M % Pt. Change vs. 2018*
Australia	57%	33%	*+3%*
France	60%	37%	*+3%*
Germany	47%	26%	*-2%*
India	80%	66%	*NA*
Italy	53%	37%	*+2%*
Japan	42%	23%	*+5%*
Netherlands	51%	27%	*+3%*
New Zealand	59%	36%	*+3%*
UK	55%	32%	*-1%*
US	61%	43%	*+2%*

In the past 12 months, India and the US saw some of the highest rates of cyber crime, while Germany, Japan and the Netherlands saw the lowest.

On Average, Past Year Cyber Crime Victims Spent Nearly 6 Hours Resolving Issues and More Than 2 in 5 Were Impacted Financially

Globally, those who experienced cyber crime in the past year…

Spent an average of 5.8* hours resolving it *for an estimated 2.1 billion hours lost globally*



Have lost money as a result of the cyber crime committed

Trended Hours Spent Resolving Cyber Crime by Country
(Average)*

	2019	*Change vs. 2018*
Australia	4.2	*-2.4*
France	7.9	*+3.7*
Germany	9.8	*+4.8*
India	7.0	*N/A*
Italy	7.2	*+0.8*
Japan	4.3	*-5.3*
Netherlands	5.2	*+0.8*
New Zealand	4.3	*-0.8*
UK	3.9	*-1.6*
US	4.8	*+1.7*

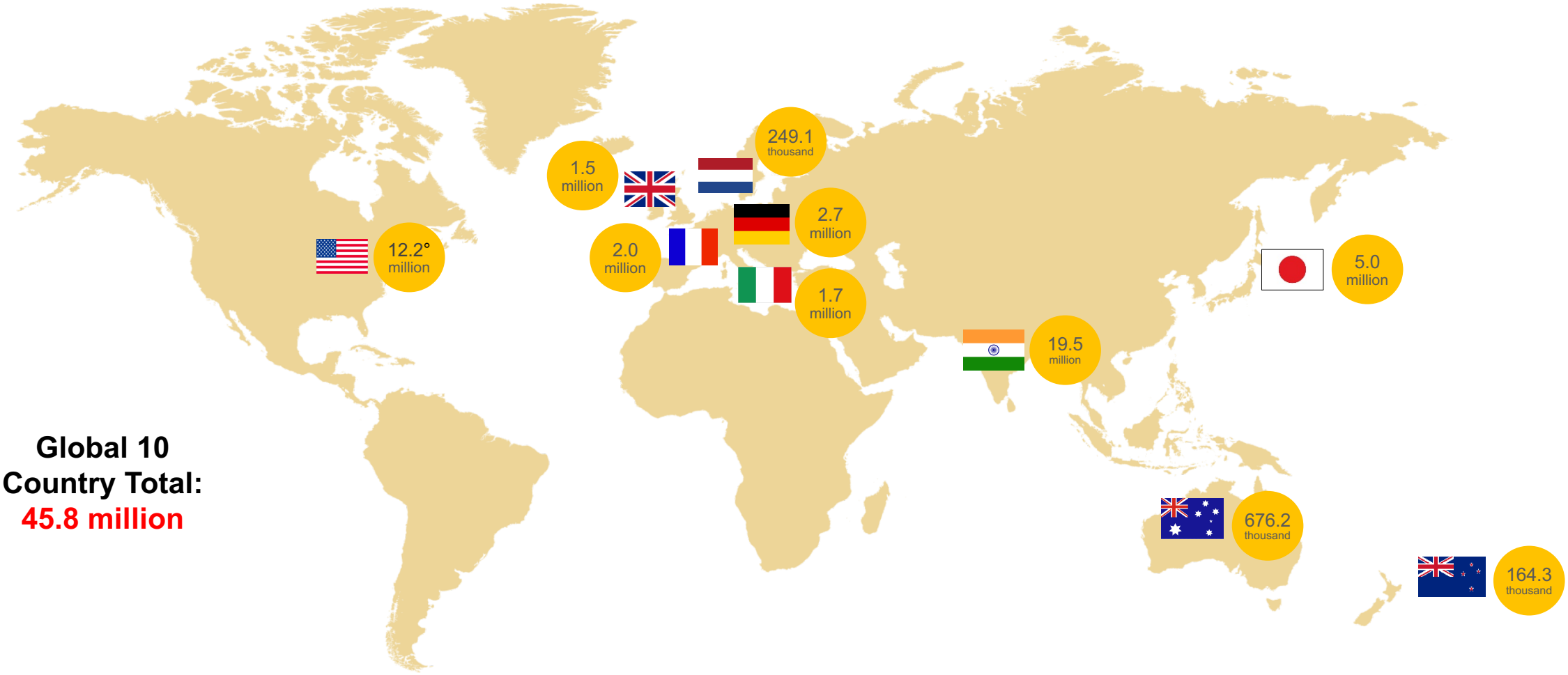
Trended % Who Lost Some Money From Cyber Crime by Country

	2019	*Change vs. 2018*
Australia	45%	*+7%*
France	39%	*+4%*
Germany	45%	*+12%*
India	63%	*N/A*
Italy	33%	*-6%*
Japan	18%	*+4%*
Netherlands	44%	*+9%*
New Zealand	30%	*-1%*
UK	41%	*-3%*
US	49%	*+9%*

*Average has been trimmed to remove outliers

IDENTITY THEFT: INCIDENCE AND ATTITUDES

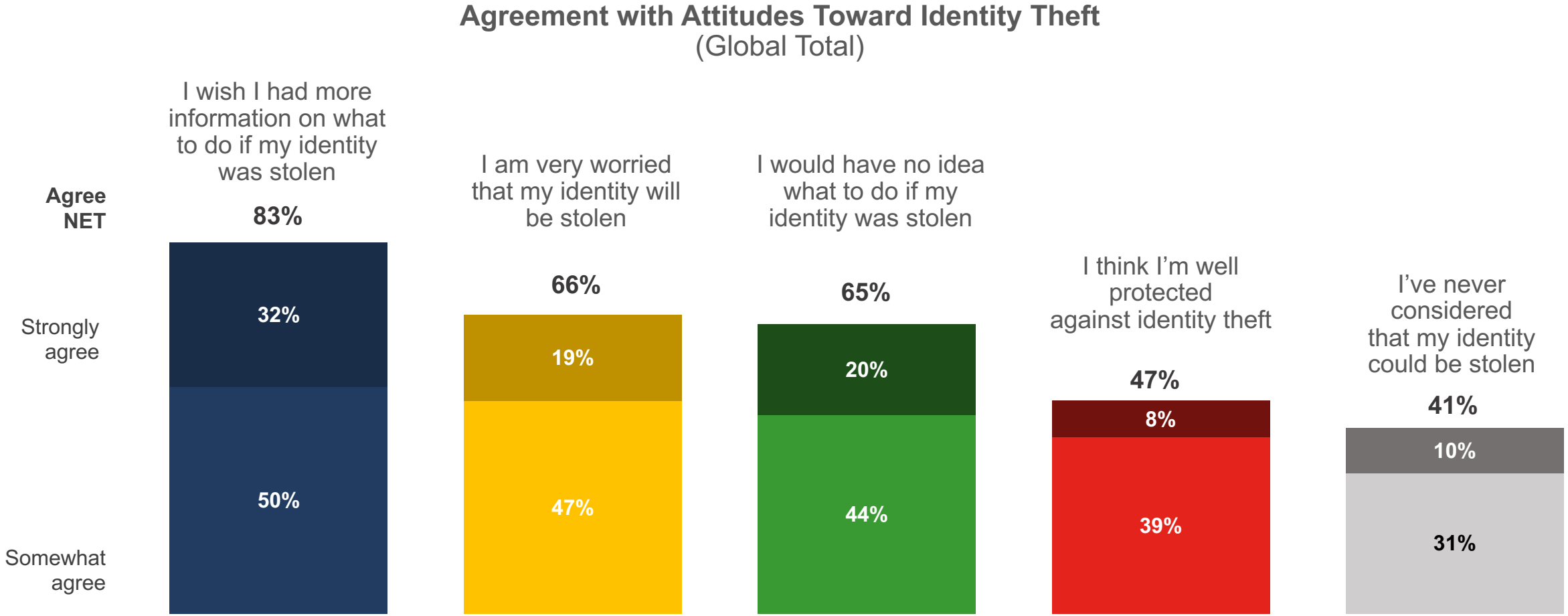
Nearly 46 Million Consumers* Were the Victim of Identity Theft Last Year



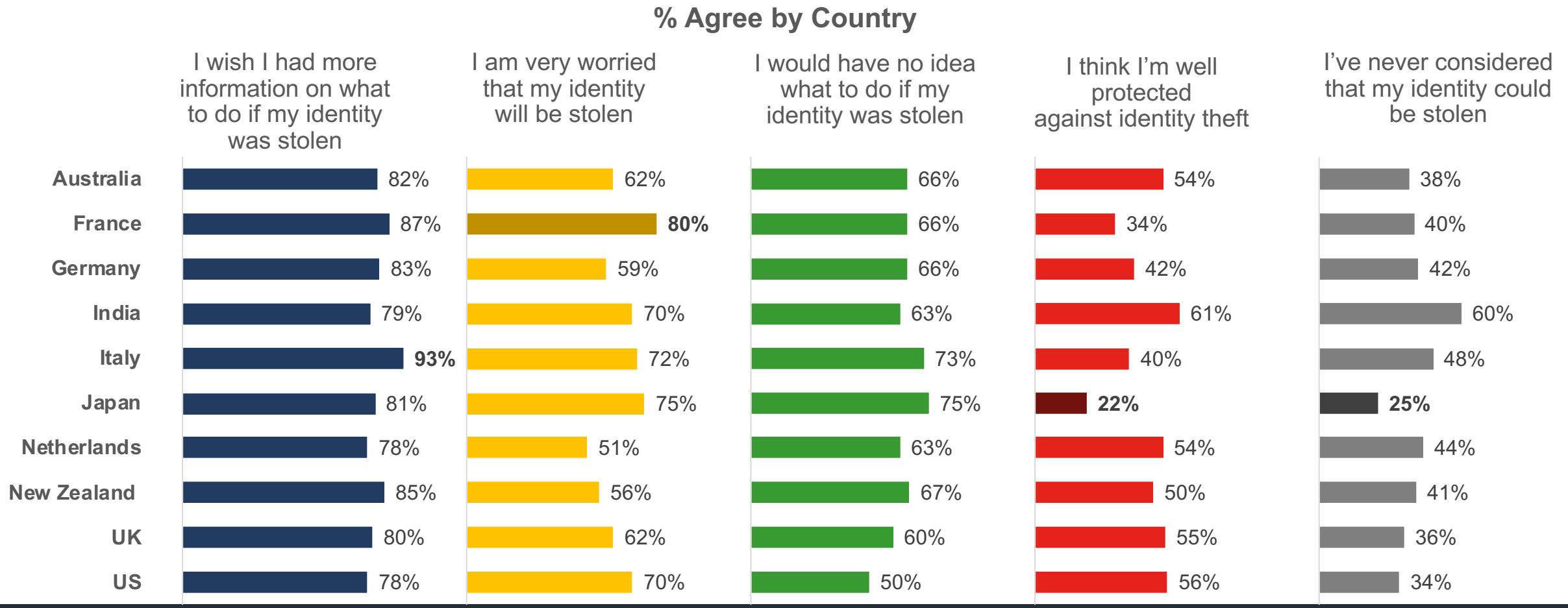
Global 10 Country Total:
45.8 million

*in 10 countries
°Source: Online survey of 5,020 US adults conducted by The Harris Poll on behalf of Norton™ LifeLock™, January 2020.

Similar Proportions Both Very Worried Their Identity Will Be Stolen and Would Have No Idea What to Do If It Were; Less Than 1 in 2 Feel Well Protected Against Identity Theft

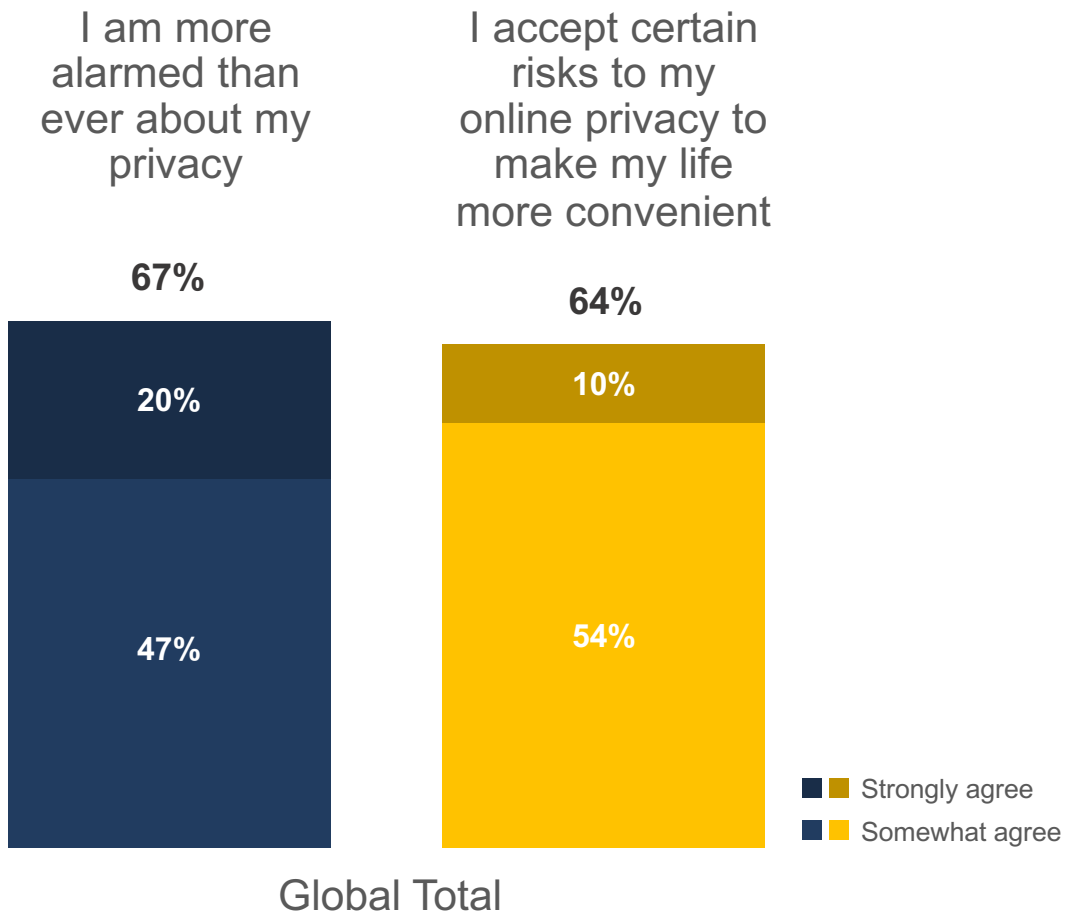


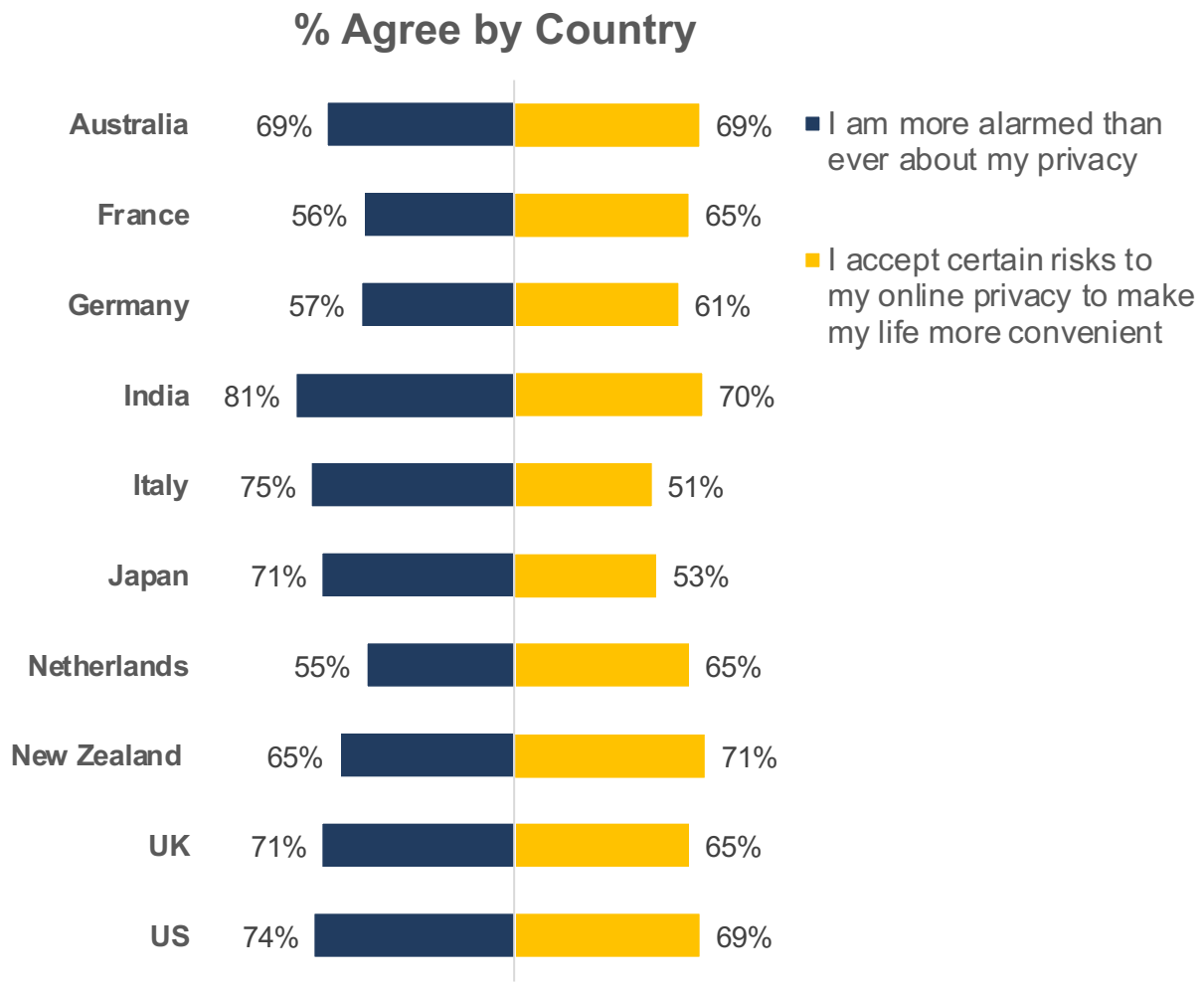
Consumers in France Most Concerned Their Identity Will Be Stolen; Those in Japan Seem to Have Considered the Threat of Identity Theft, but Also Are Least Likely to Feel Well Protected Against It



PROTECTING PERSONAL PRIVACY

Two-Thirds More Alarmed Than Ever About Their Privacy, But Willing to Accept Certain Risks to Make Life More Convenient

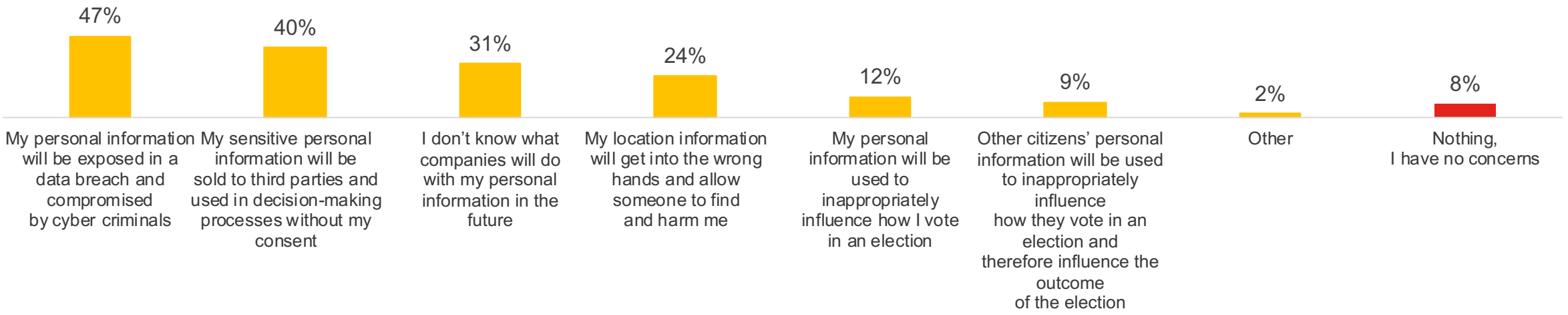




The Vast Majority Have Concerns About Data Privacy, Most Commonly That Their Personal Information Will Be Exposed In a Data Breach and Compromised by Cyber Criminals

92% have at least one concern

Biggest Concerns About Data Privacy*
(Global Total)



% Who Have At Least One Concern by Country

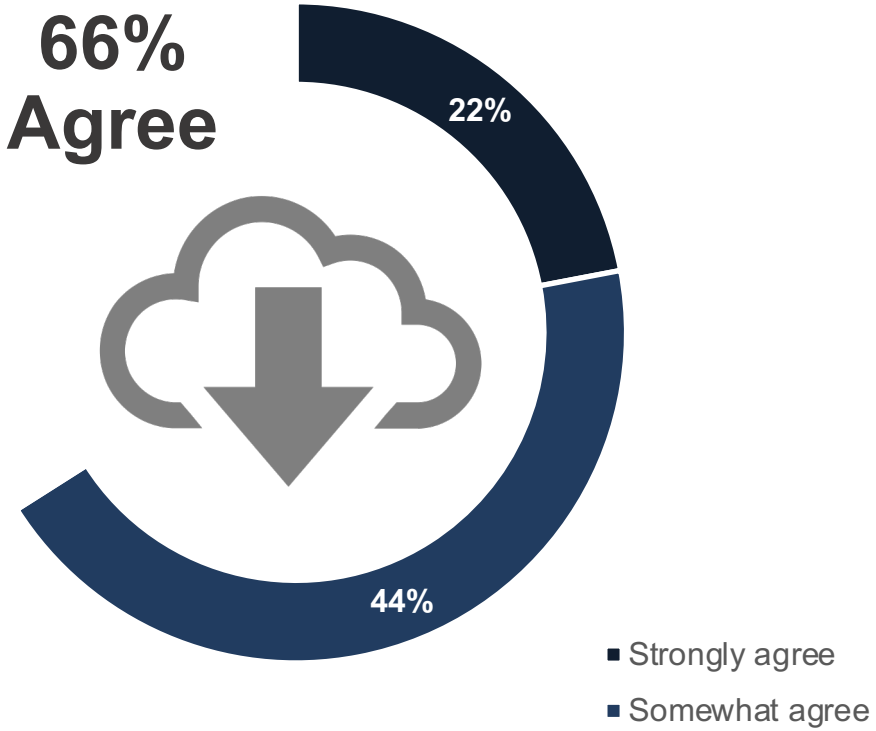
Australia	France	Germany	India	Italy	Japan	Netherlands	New Zealand	UK	US
92%	91%	91%	96%	93%	87%	88%	95%	93%	93%

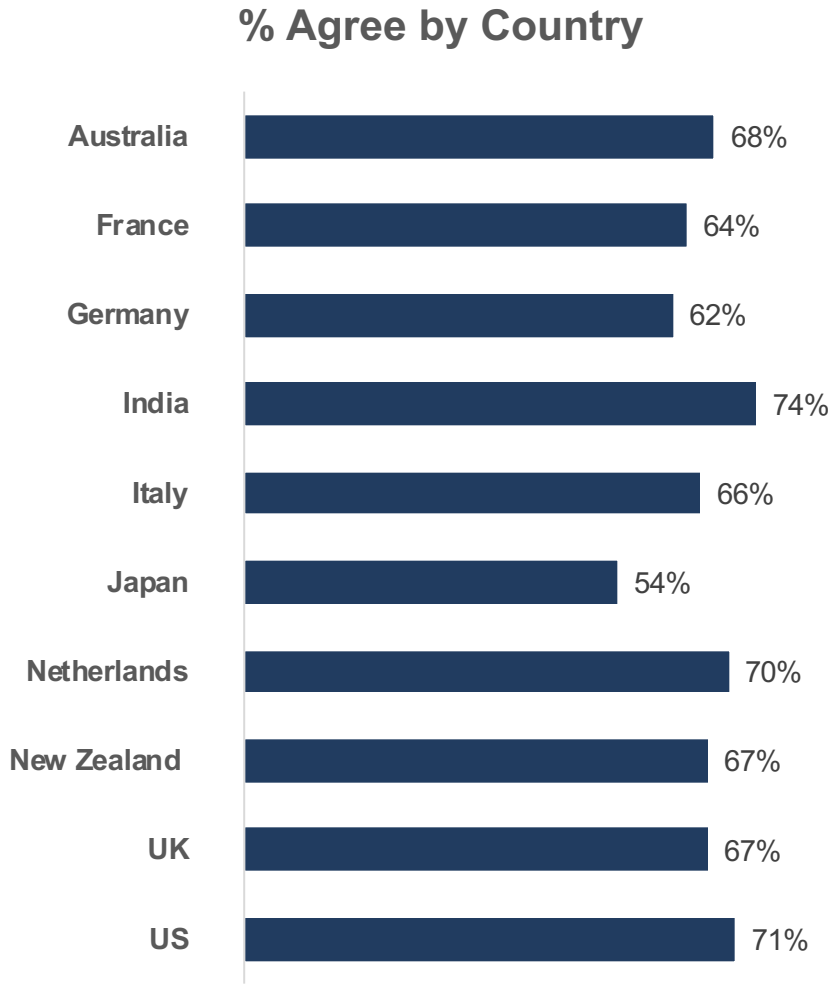
Respondents were asked to select up to 2 concerns.

Around Two-Thirds Say, At Times, They Have Chosen Not to Download Apps or Use Services Solely Based on Privacy Policies

There have been times I have chosen not to download a certain app or use a specific service solely based on the privacy policy

(Global Total)

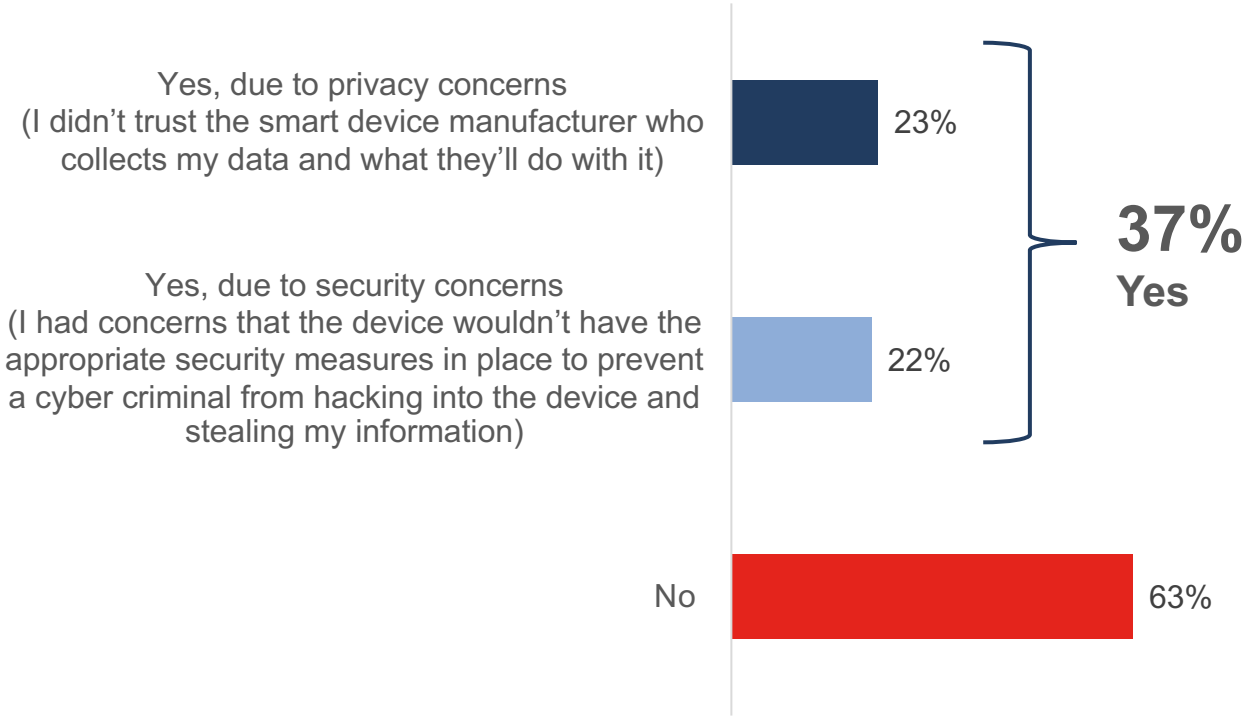




More Than 1 in 3 Consumers Have Decided Not to Purchase a Smart Home Device Because of Privacy or Security Concerns

Have you ever decided not to purchase a smart home device due to privacy or security concerns?

Global Total



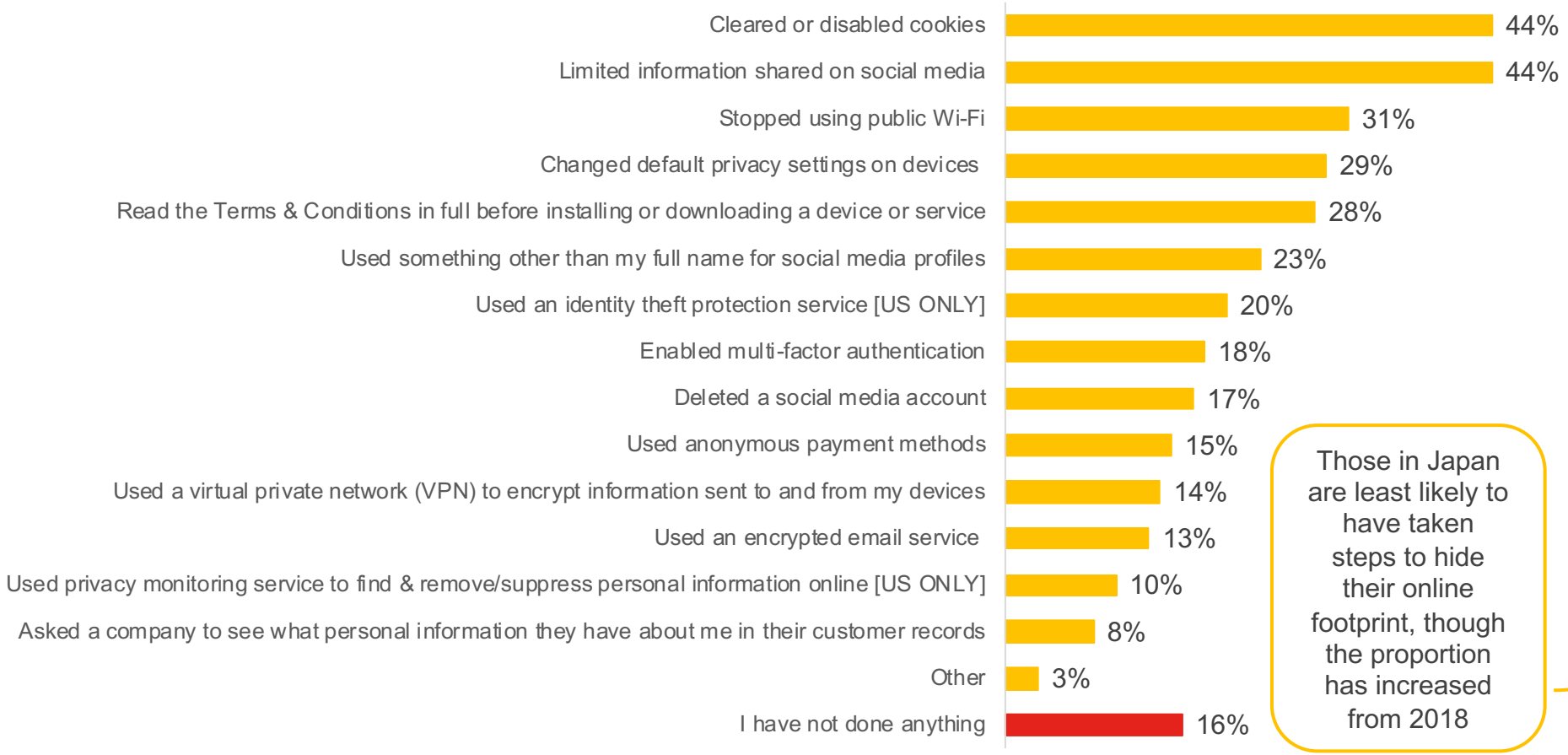
By Country

	Yes (NET)
Australia	34%
France	37%
Germany	**44%**
India	**63%**
Italy	30%
Japan	31%
Netherlands	30%
New Zealand	22%
UK	37%
US	**43%**

Those in Germany, India, and the US are more likely to say they have decided not to purchase a smart home device because of privacy or security concerns

The Majority Have Taken Some Steps to Protect Their Online Privacy, Most Commonly Clearing/Disabling Cookies or Limiting Information Shared on Social Media

Steps Taken to Protect Online Activities and Personal Information**
(Global Total)



Those in Japan are least likely to have taken steps to hide their online footprint, though the proportion has increased from 2018

84% have taken at least one step^

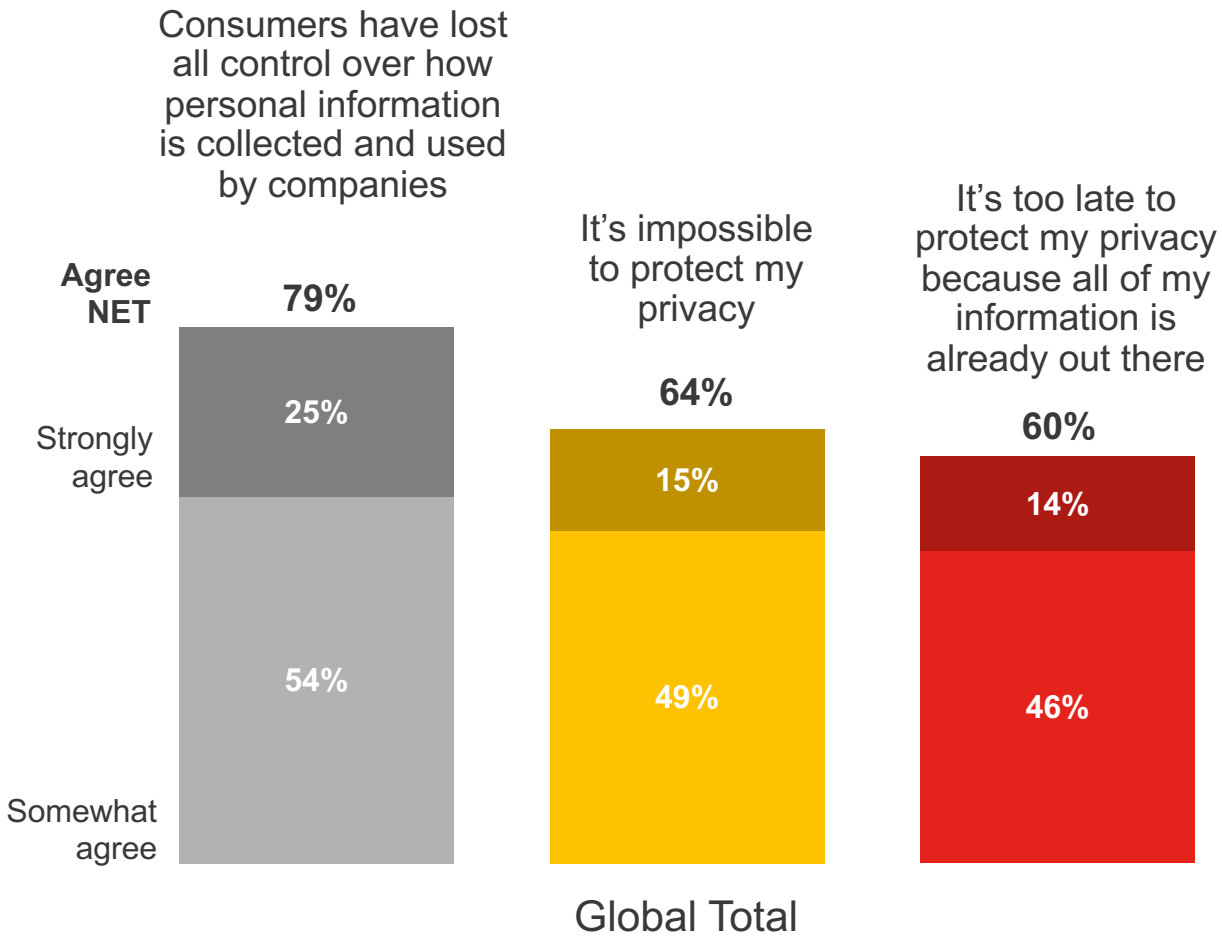
% Who Have Taken At Least One Step^ by Country

	2019	% Pt. Change vs. 2018
Australia	83%	-3%
France	85%	0%
Germany	85%	-4%
India	94%	N/A
Italy	82%	-2%
Japan	**69%**	+3%
Netherlands	81%	-2%
New Zealand	88%	-1%
UK	86%	-2%
US	87%	+1%

The proportion of consumers taking action in each country has held steady over the past year

***Expanded definition of 'personal information' to include aspects of data privacy in 2019* *^3 response options added in 2019*

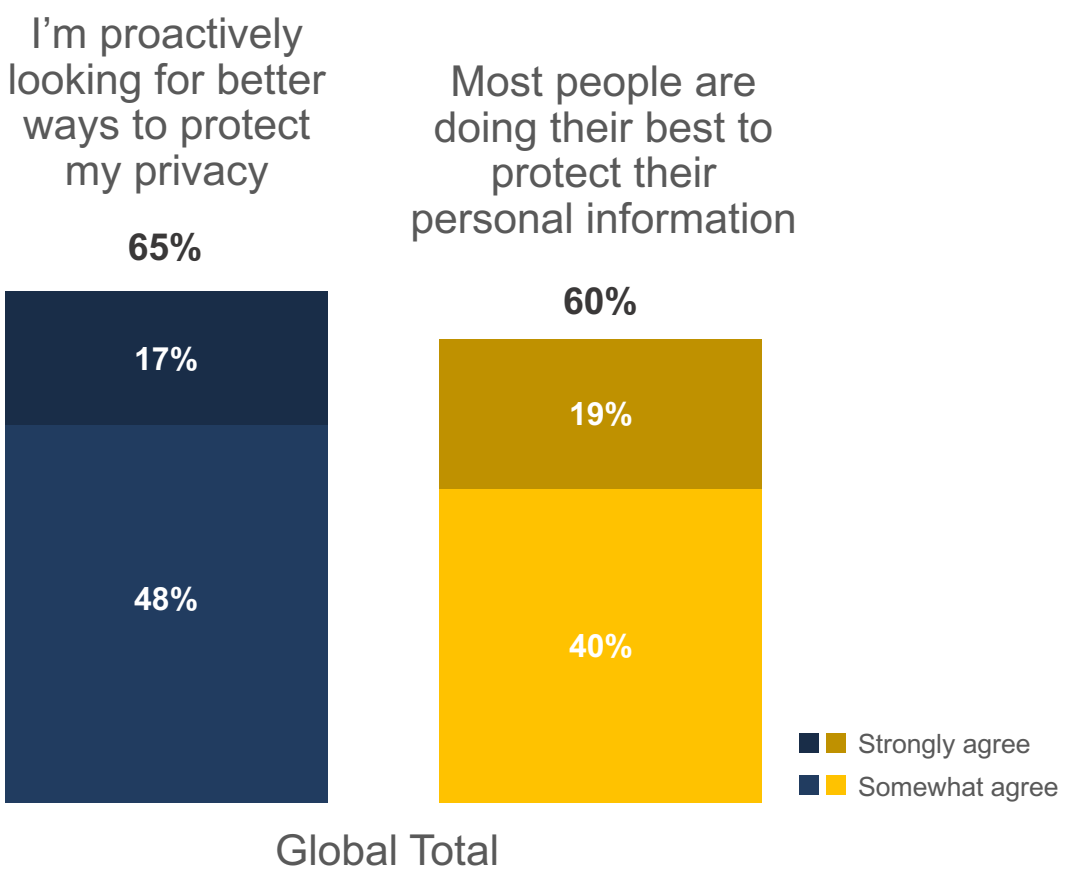
Despite Actions Taken, 4 in 5 Believe Consumers Have Lost Control on How Personal Information Is Collected/Used by Companies, and Many Think It's Impossible or Too Late to Protect Their Privacy

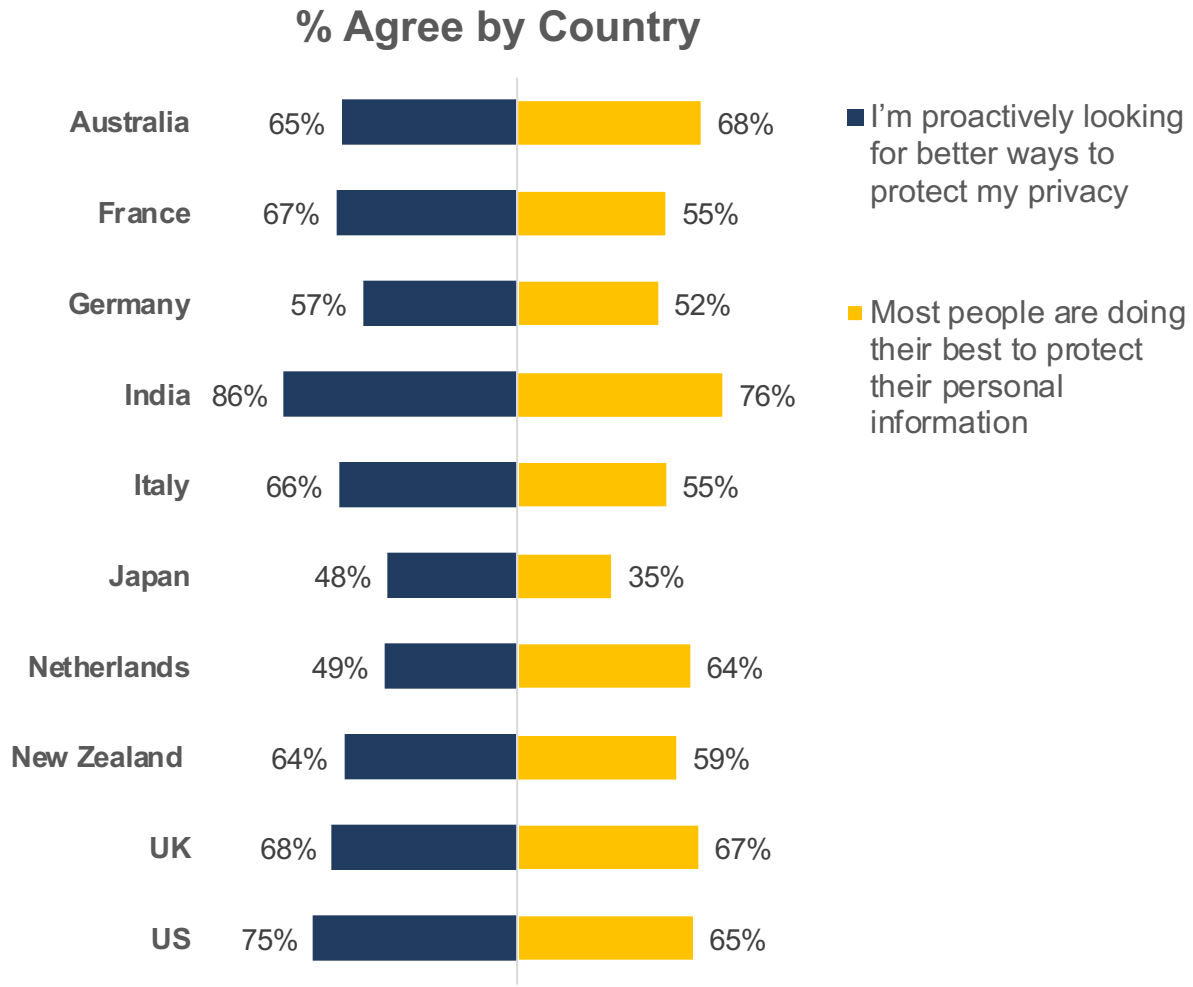


% Agree by Country

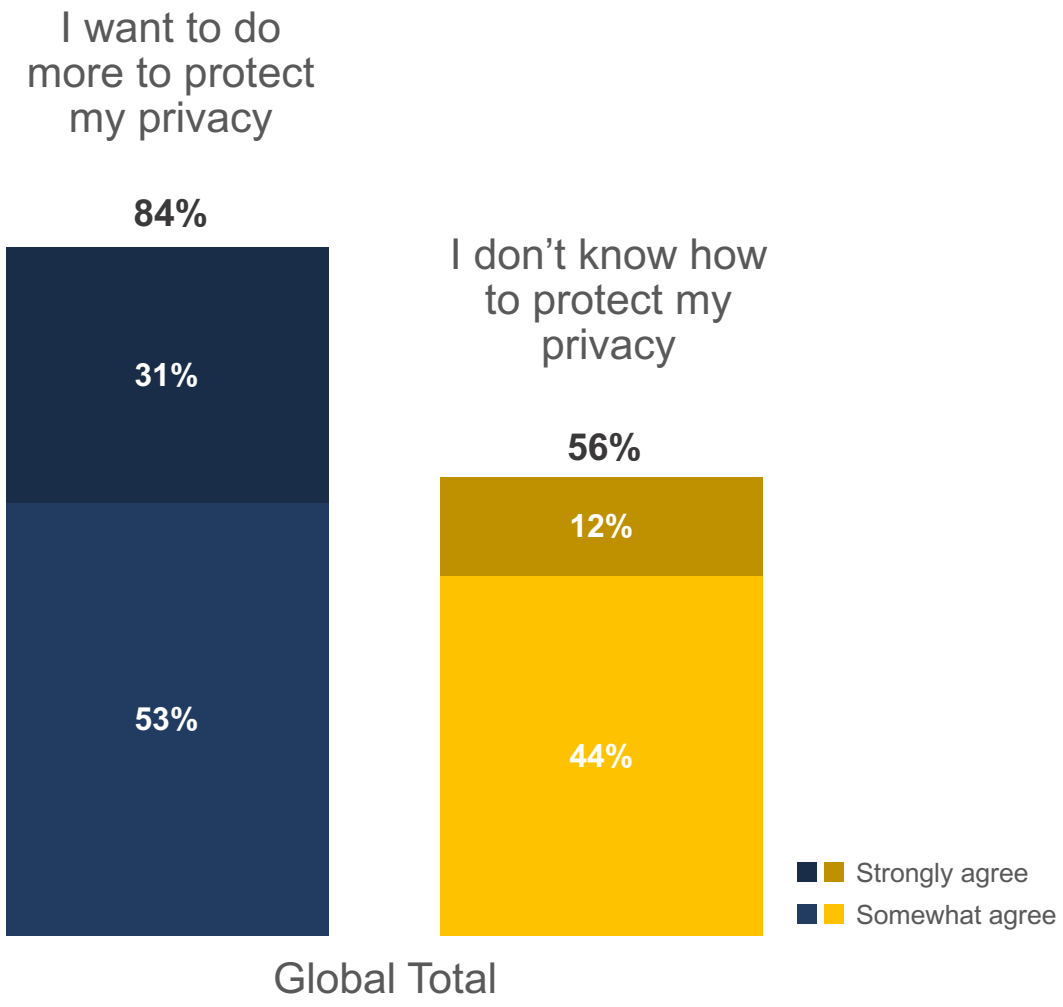
	Consumers have lost all control over how personal information is collected and used by companies	It's impossible to protect my privacy	It's too late to protect my privacy because all of my information is already out there
Australia	81%	67%	61%
France	83%	63%	60%
Germany	77%	64%	67%
India	75%	50%	56%
Italy	83%	67%	64%
Japan	73%	70%	51%
Netherlands	77%	67%	64%
New Zealand	84%	68%	59%
UK	79%	64%	61%
US	77%	58%	54%

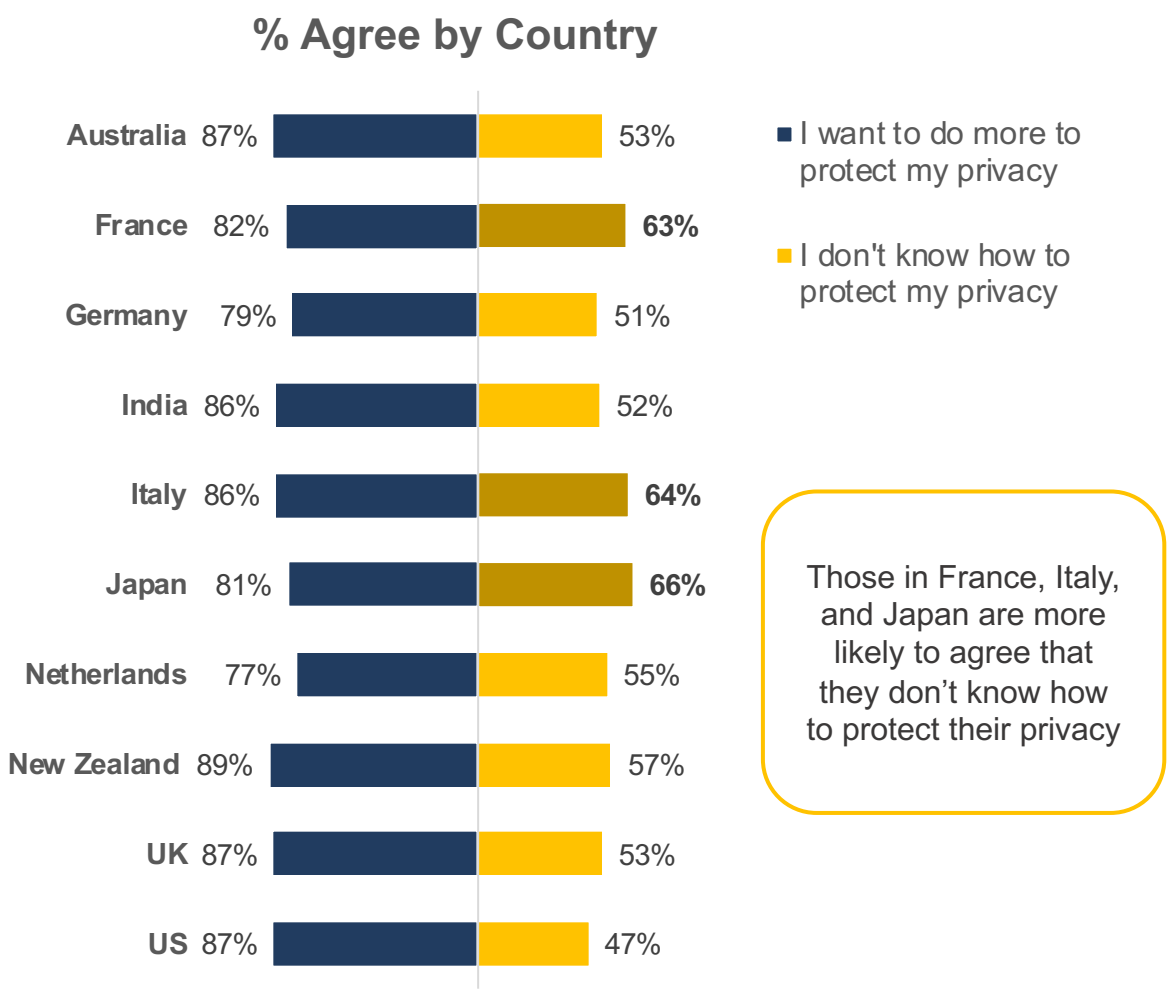
Yet Still Almost 2 in 3 Are Proactively Looking for Better Ways to Protect Their Privacy





Though Consumers Are Taking Action and Want to Do More to Protect Their Privacy, More Than Half Still Say They Don't Know How

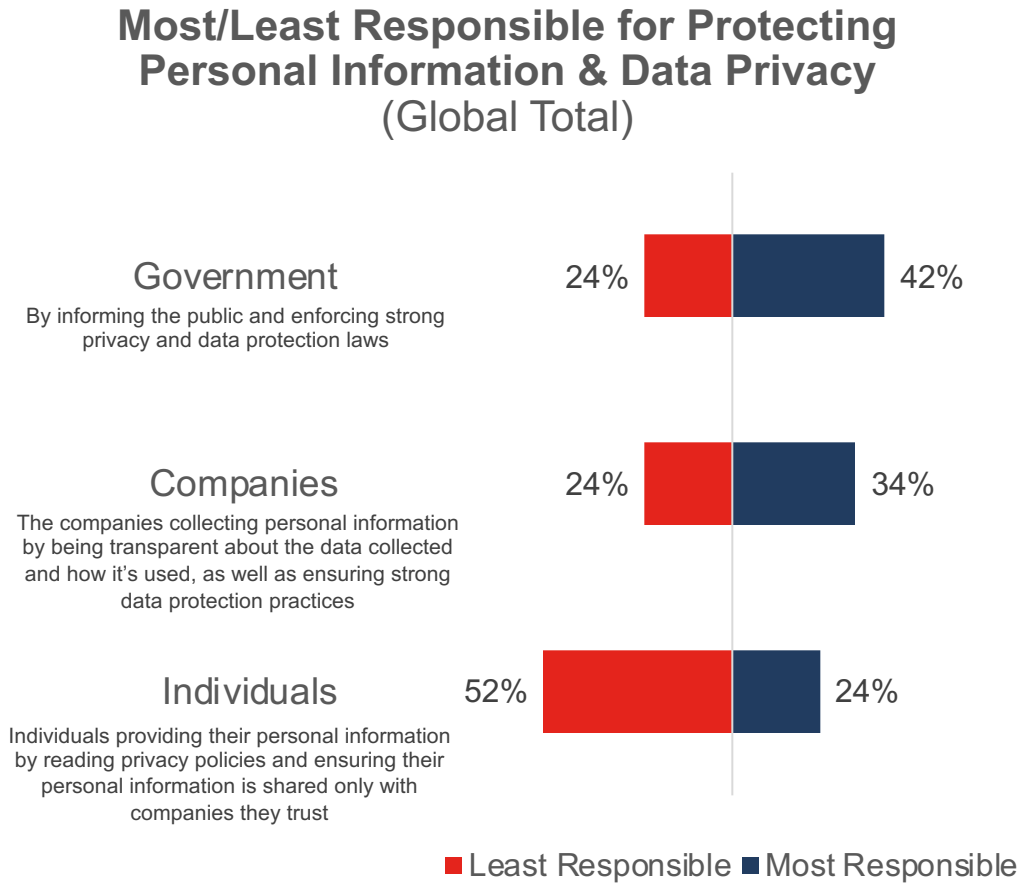




Those in France, Italy, and Japan are more likely to agree that they don't know how to protect their privacy

ORGANIZATIONAL RESPONSIBILITY

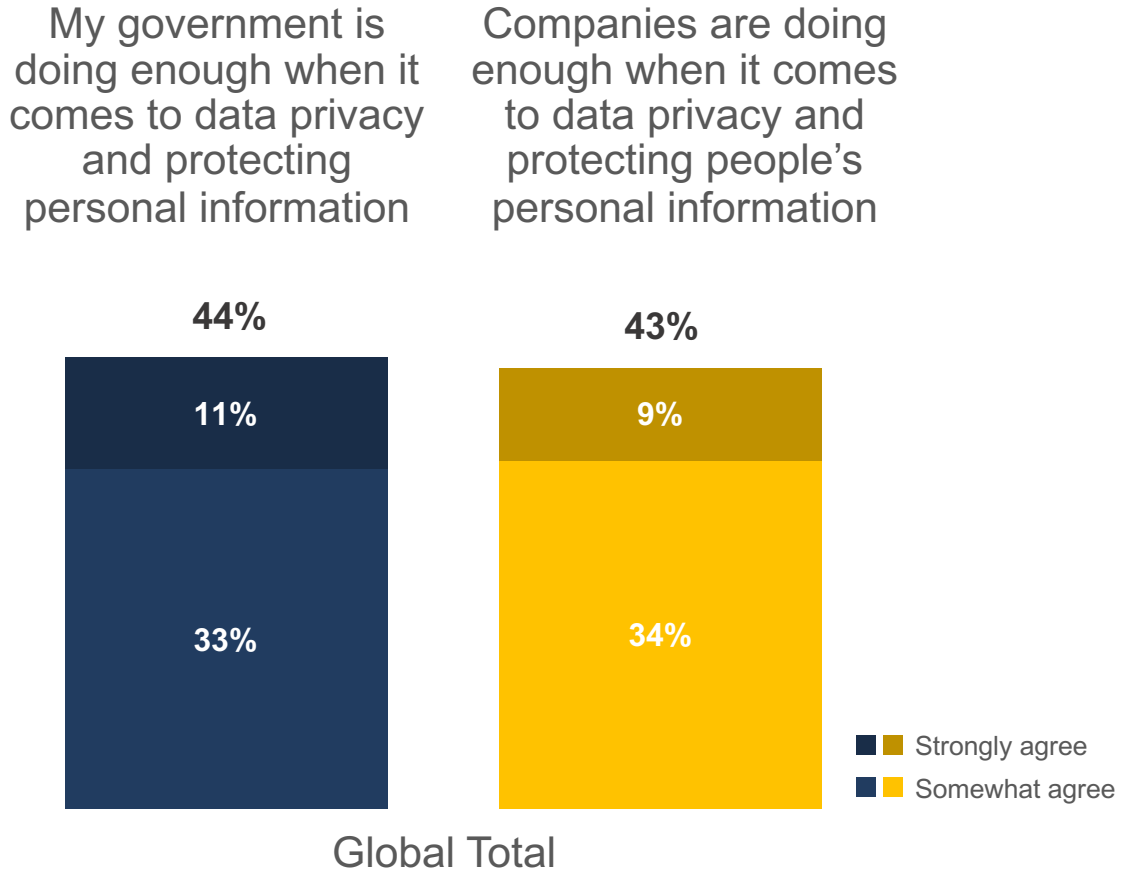
While No Clear Consensus, More Feel Government Should Be Held Responsible For Protecting Personal Information Than Companies Collecting It and The Individuals Providing It

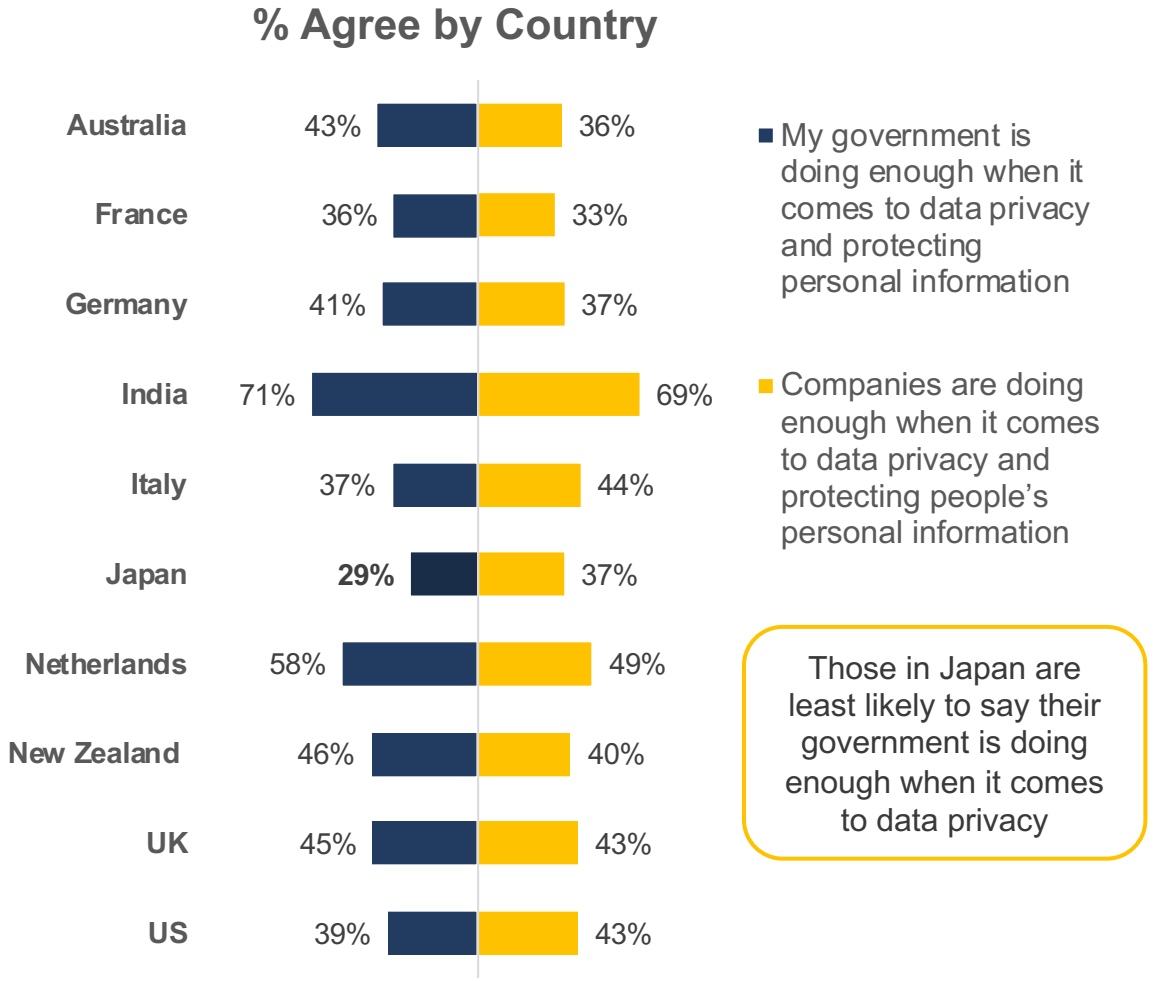


	% Most Responsible by Country		
	Government	Companies	Individuals
Australia	**42%**	33%	26%
France	**40%**	35%	25%
Germany	**42%**	36%	22%
India	**42%**	32%	25%
Italy	**41%**	39%	20%
Japan	**53%**	33%	14%
Netherlands	**53%**	28%	19%
New Zealand	**38%**	33%	29%
UK	36%	**37%**	27%
US	29%	**36%**	34%

The US is the only country where the individual consumer outranks the government as most responsible

Though They May Hold The Government Most Responsible, Less than 1 in 2 Feel Their Government Is Doing Enough For Data Privacy; The Same Sentiment is True of Companies

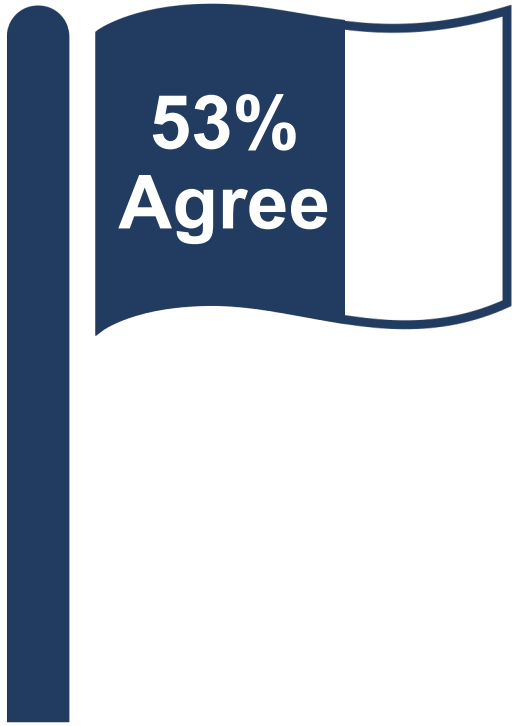


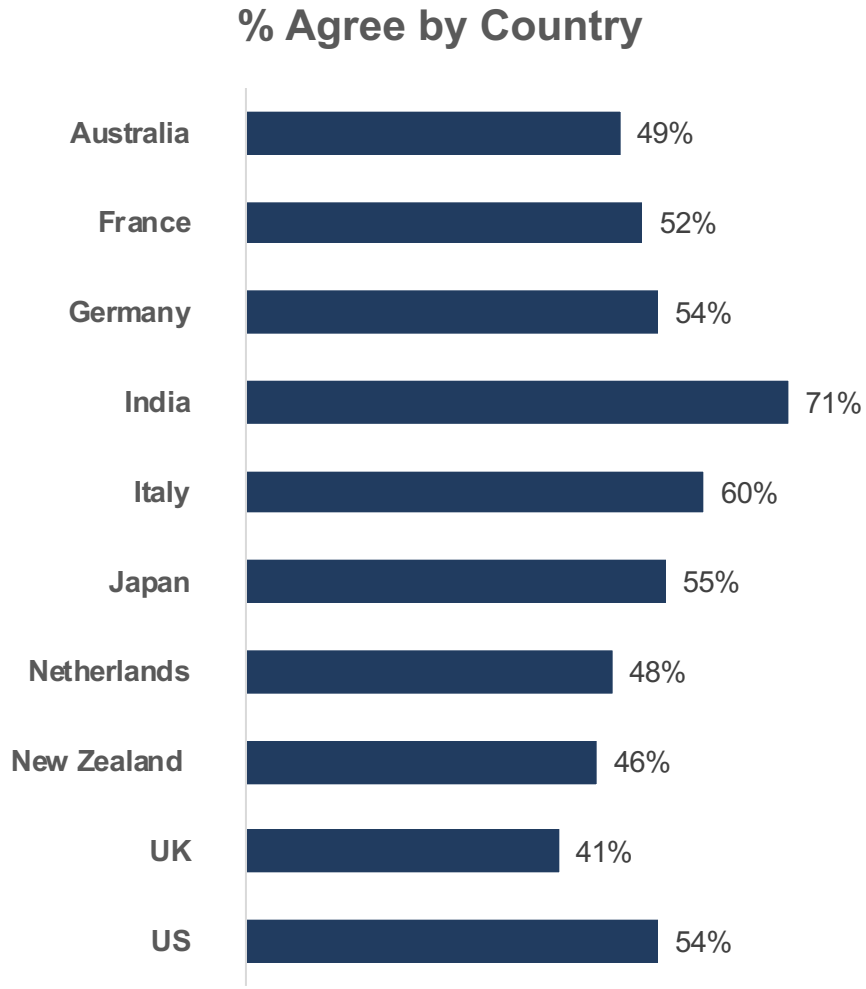


Those in Japan are least likely to say their government is doing enough when it comes to data privacy

A Slight Majority Feel Their Country is Behind Most Others When It Comes to Data Privacy Laws

My country is behind most other countries when it comes to data privacy laws (Global Total)

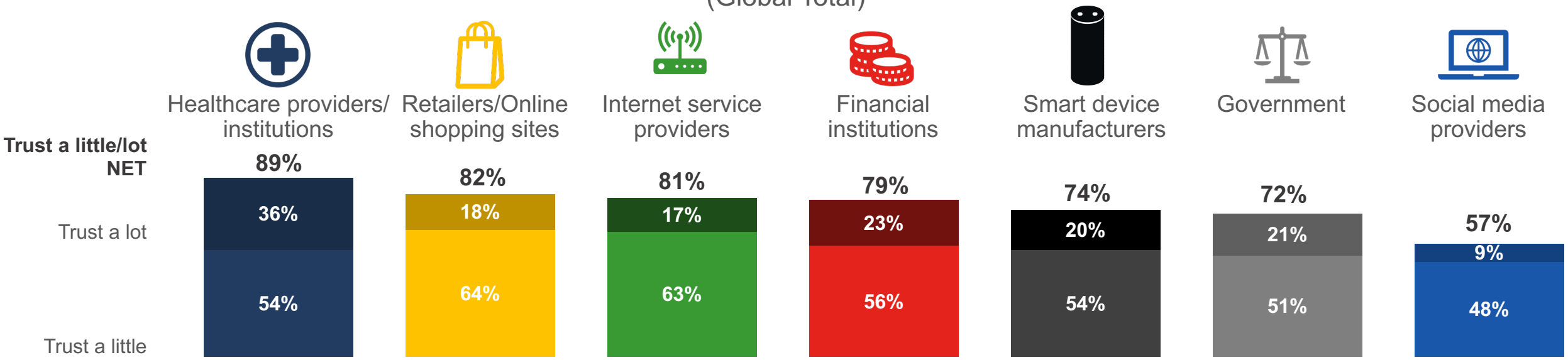




Interestingly, even with GDPR in place, Italy is still among the most likely to believe their country is behind others when it comes to data privacy laws (however, UK is among the least likely)

Trust in Social Media Providers to Protect Personal Information Notably Trails Others Holding Sensitive Information

Trust in Managing and Protecting Personal Information
(Global Total)

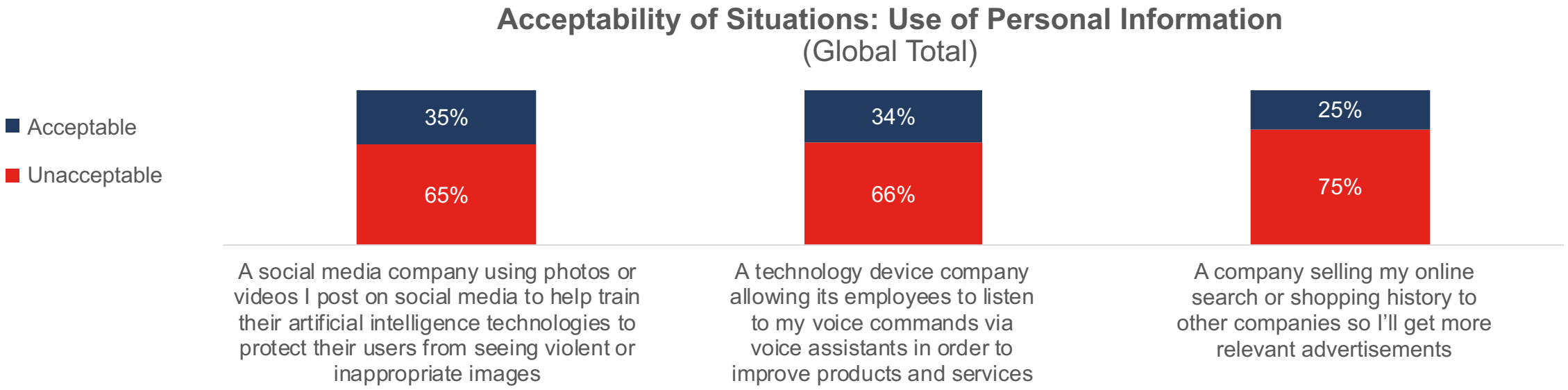


% Who Trust A Little/Lot by Country

India and Italy tend to be the most trusting markets

	Australia	France	Germany	India	Italy	Japan	Netherlands	New Zealand	UK	US
Healthcare providers	88%	86%	88%	**89%**	**92%**	88%	92%	94%	93%	84%
Retailers	79%	79%	84%	**86%**	**85%**	77%	79%	81%	85%	82%
Internet service providers	80%	81%	76%	**86%**	**85%**	77%	81%	82%	80%	77%
Financial institutions	76%	71%	75%	**85%**	**77%**	85%	81%	84%	80%	81%
Smart device manufacturers	70%	68%	62%	**90%**	**88%**	80%	68%	73%	72%	73%
Government	69%	58%	72%	**85%**	**84%**	63%	77%	84%	62%	66%
Social media providers	49%	51%	52%	**74%**	**74%**	66%	54%	46%	48%	53%

Most Consumers Find It Unacceptable for Companies to Use Their Personal Information, Even For Potential Benefits



% Acceptable by Country

Australia	32%	26%	21%
France	30%	36%	18%
Germany	40%	24%	19%
India	57%	66%	52%
Italy	37%	31%	29%
Japan	32%	36%	21%
Netherlands	33%	31%	23%
New Zealand	32%	30%	16%
UK	31%	29%	25%
US	30%	28%	29%

Nearly 4 in 5 Would Likely Choose to Opt-Out of Allowing Companies to Sell Their Personal Data to Third Parties, Even If It Could Mean Higher Costs or Fewer Free Products/Services

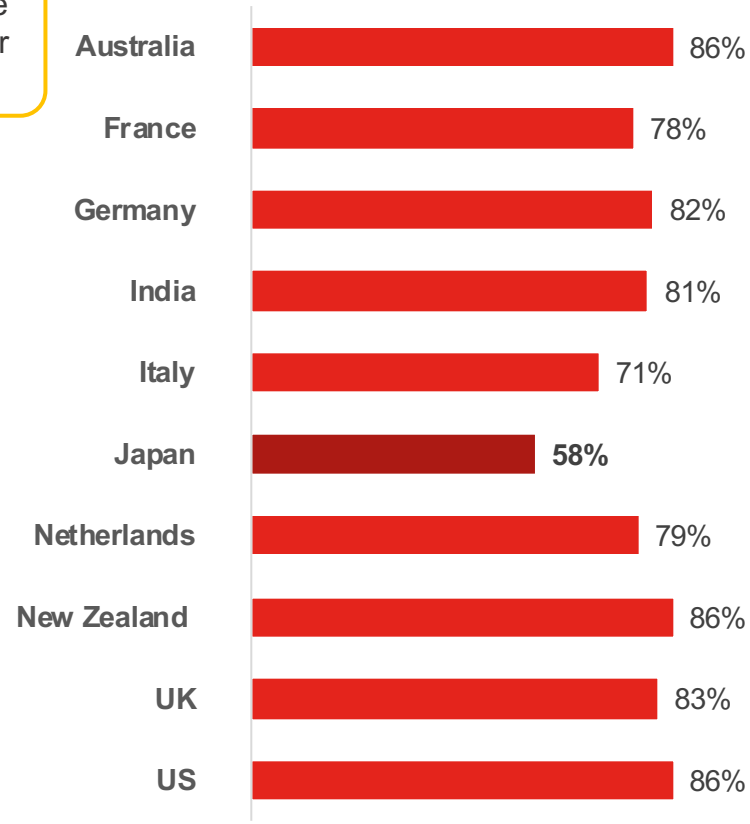
More Likely to Opt-in/Opt-Out of Companies Selling Personal Data
(Global Total)

I would opt-out, preventing companies from selling my personal information to third parties and accepting that I might see higher costs or fewer free products/service

I would opt-in, allowing companies to sell my personal information to third parties and receiving lower prices for products/services

Those in Japan are least likely to prefer an opt-out option

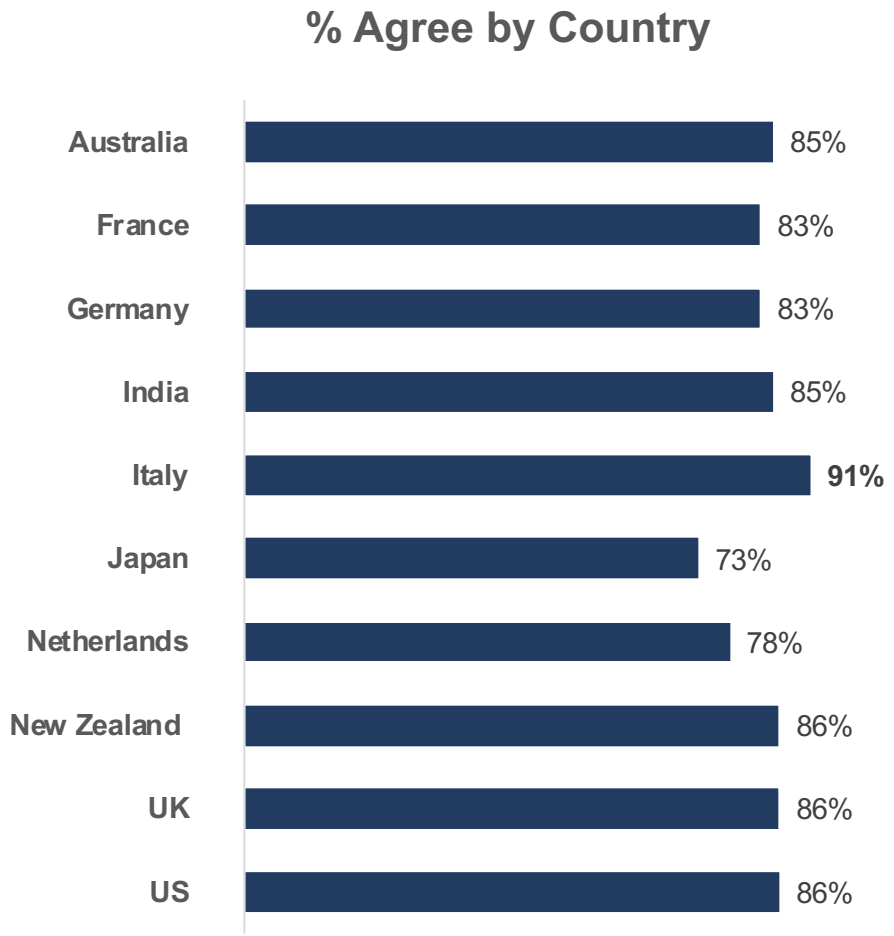
% Opt-Out by Country



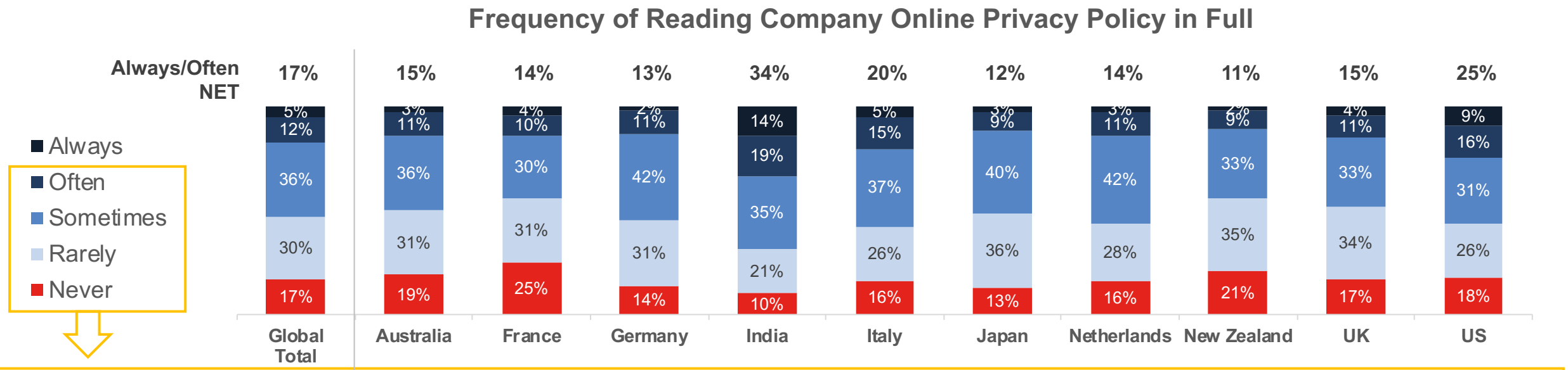
PRIVACY POLICIES

Majority Agree Consumers Should Always Read Privacy Policies in Full

Consumers should always read companies' privacy policies in full (Global Total)



Yet, Few Always or Often Read Privacy Policies in Full – Most Claim They Don't Because They Are Too Confusing or They Feel They Have to Accept Them to Use the App/Service

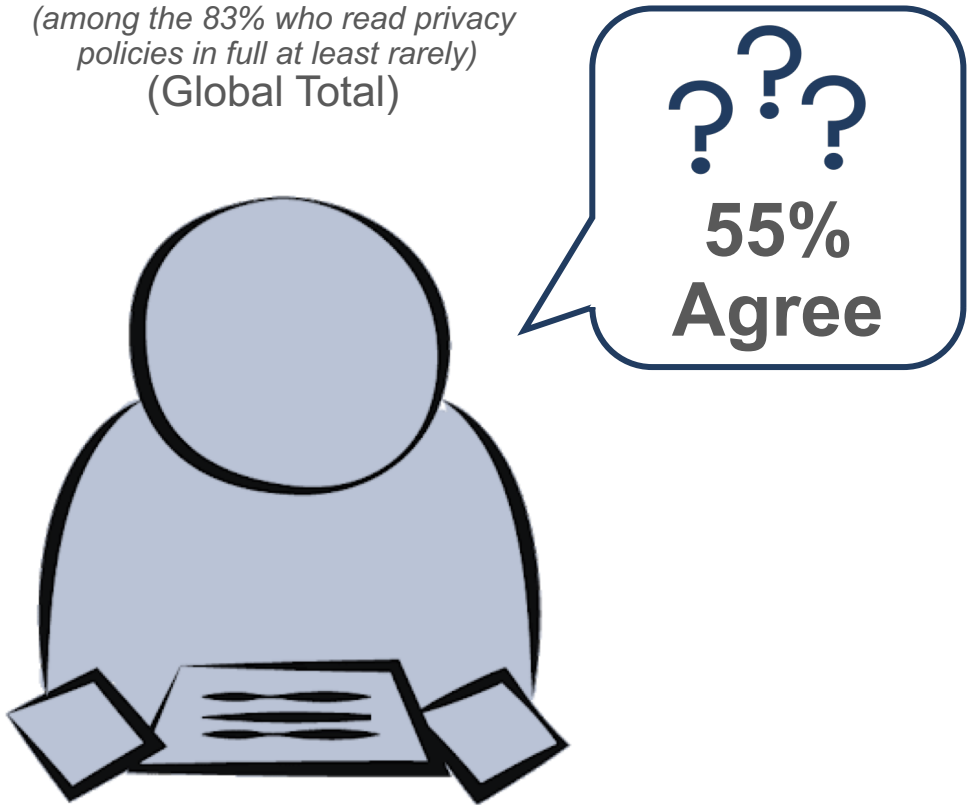


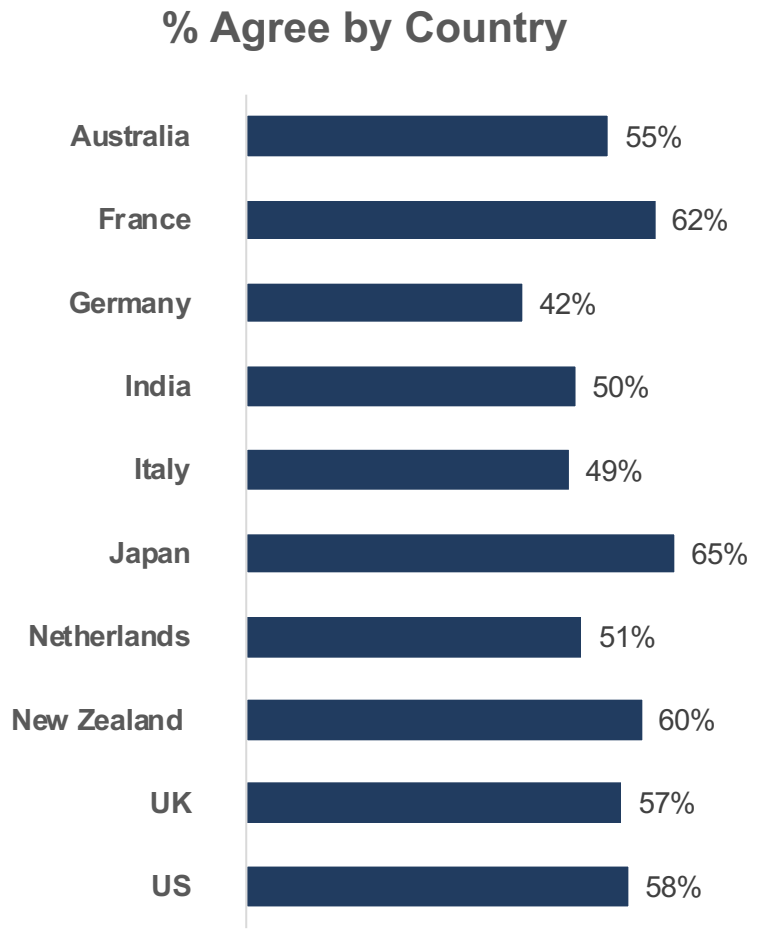
% Agree
(strongly/somewhat)

	Global Total	Australia	France	Germany	India	Italy	Japan	Netherlands	New Zealand	UK	US
I don't always read privacy policies because I feel like I have no choice but to accept them in order to use the app or service	**78%**	81%	79%	83%	72%	77%	70%	76%	**86%**	82%	78%
I don't always read privacy policies because they are too confusing	**73%**	76%	79%	72%	63%	68%	75%	68%	**80%**	76%	67%

More Than Half of Consumers Who Do Read Privacy Policies Say They Usually Don't Understand Them

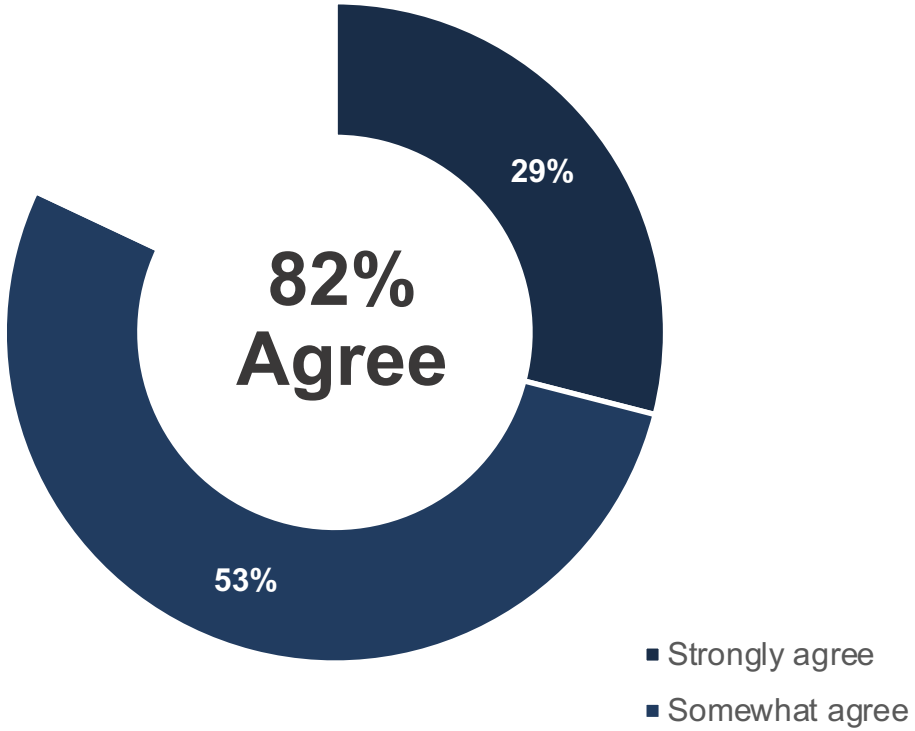
I usually don't understand privacy policies
(among the 83% who read privacy policies in full at least rarely)
(Global Total)

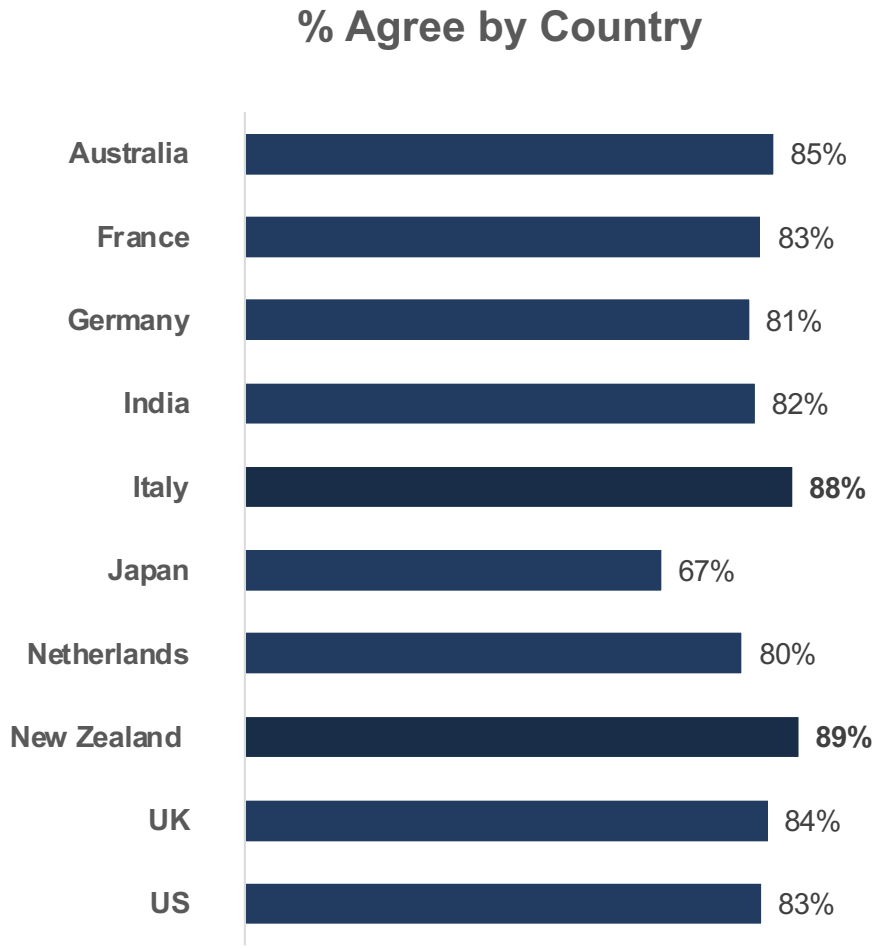




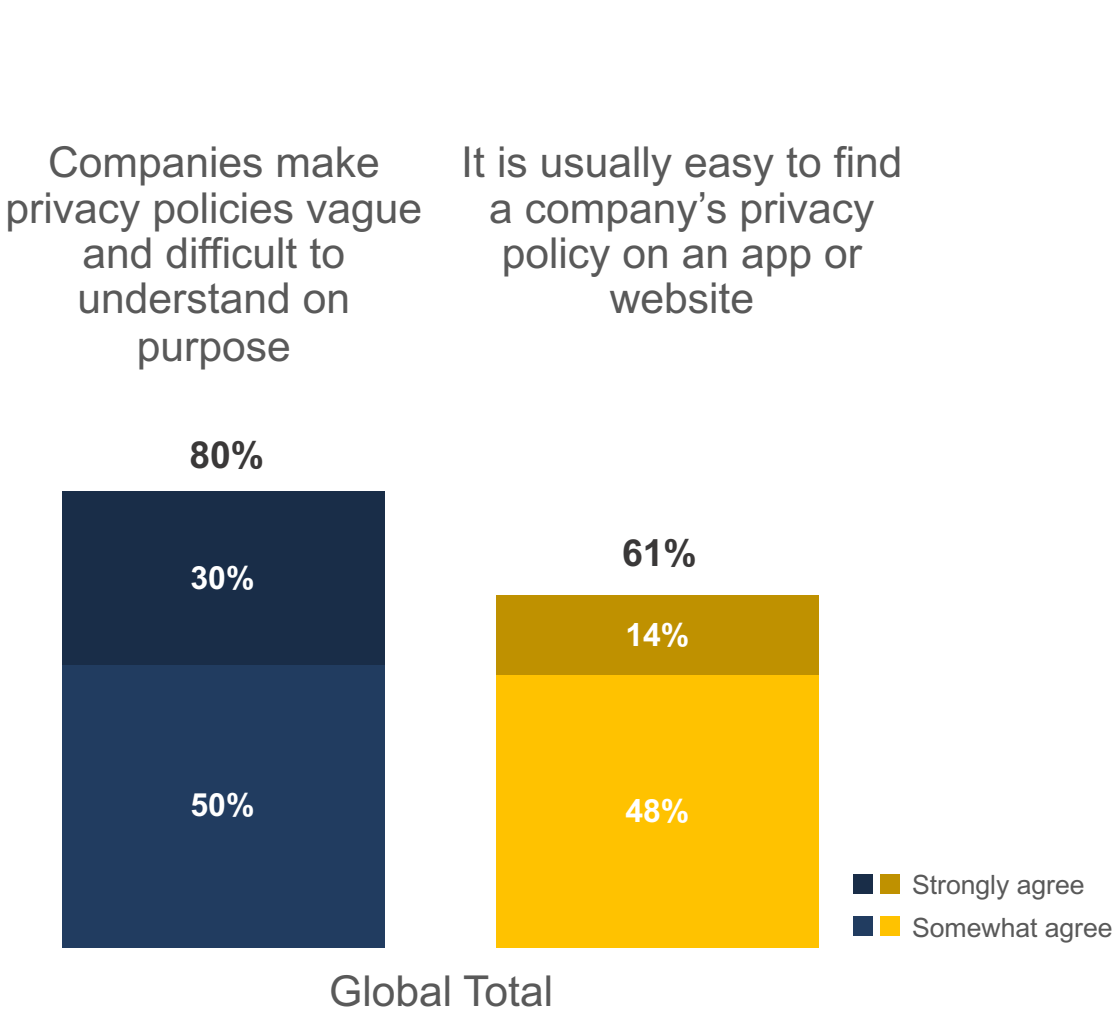
More Than 4 in 5 Would Be More Willing to Read Privacy Policies If Given Choices About How Information Could Be Used

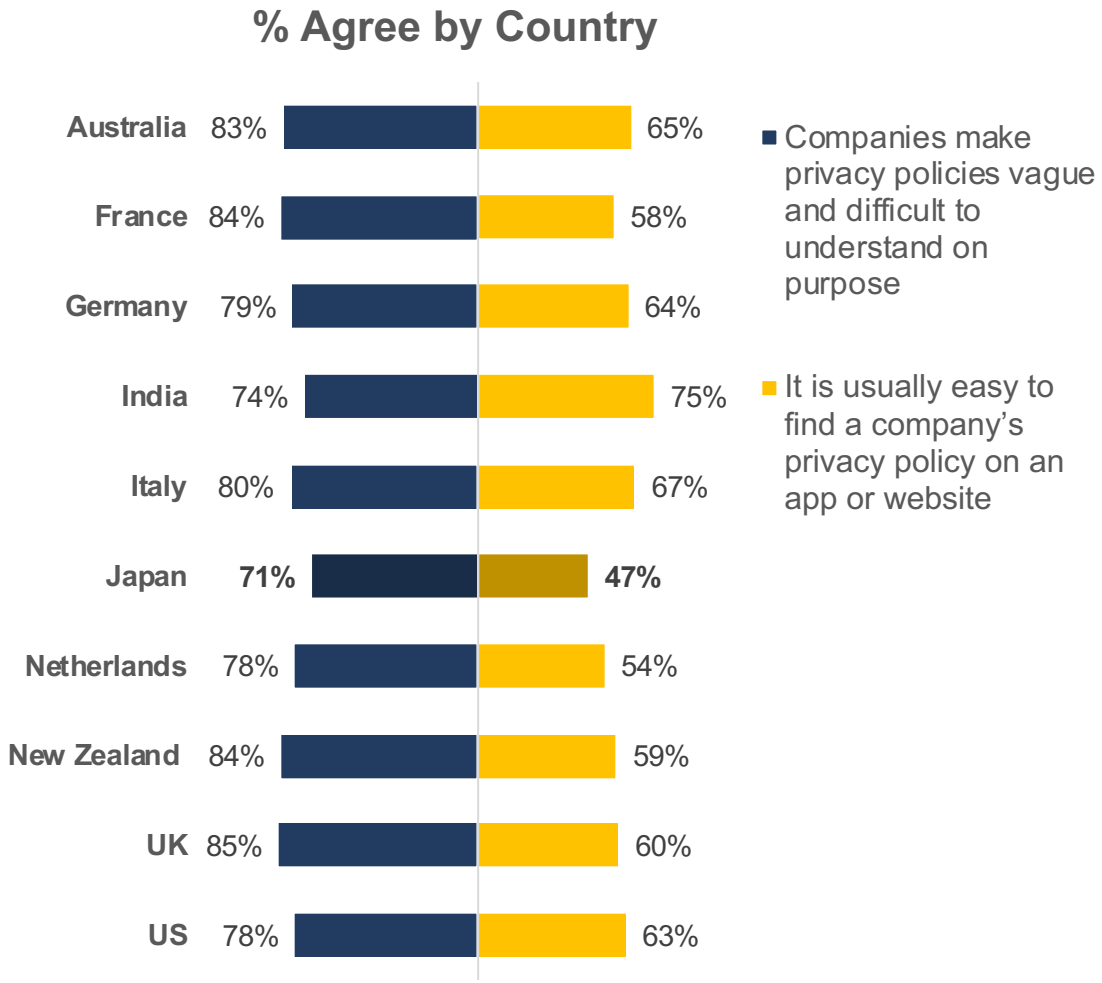
I would be more willing to read privacy policies if I were given choices about how my personal information could or couldn't be used (Global Total)





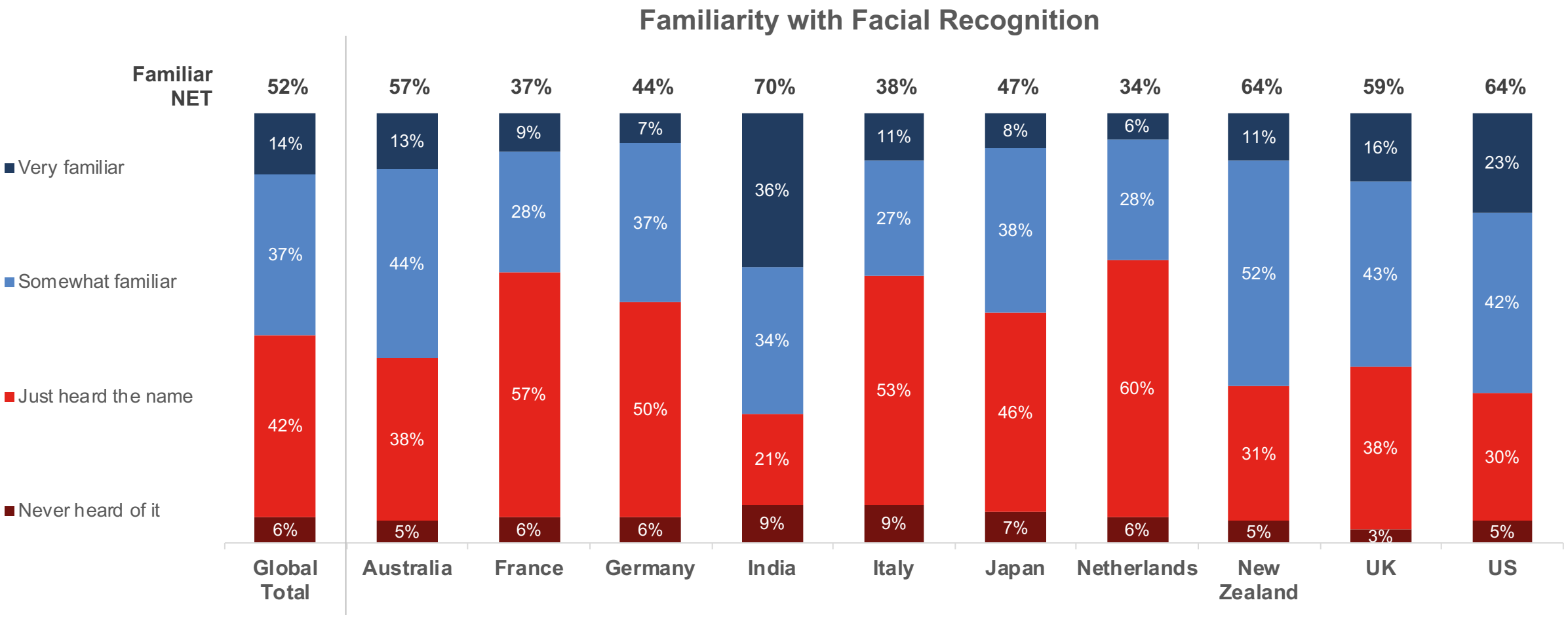
Consumers Believe Privacy Policies Are Purposefully Vague and Difficult to Understand





FACIAL RECOGNITION

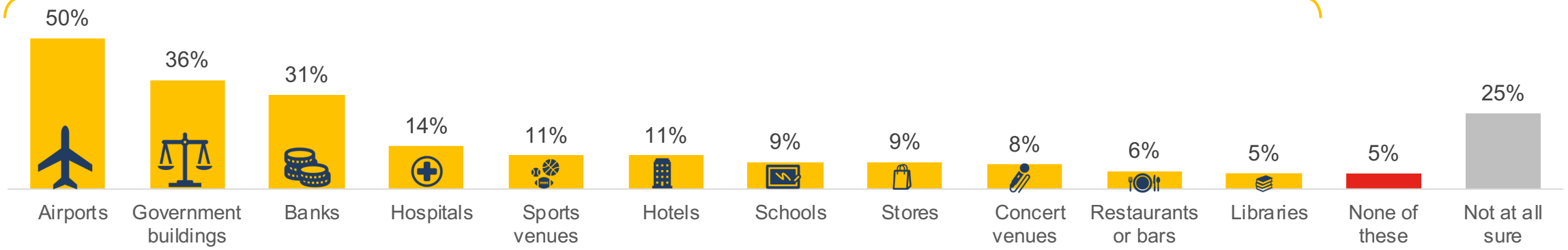
Only Half of Consumers Say They Are Familiar with Facial Recognition, With Familiarity Varying Widely by Country



While Many Believe Facial Recognition is Being Used in Some Public Spaces, Half Or Fewer Recognize Specific Locations Using The Technology, With 1 in 4 Not At All Sure

In-Person Locations Believed to Use Facial Recognition
(Global Total)

70% Believe at least one location has started to use facial recognition

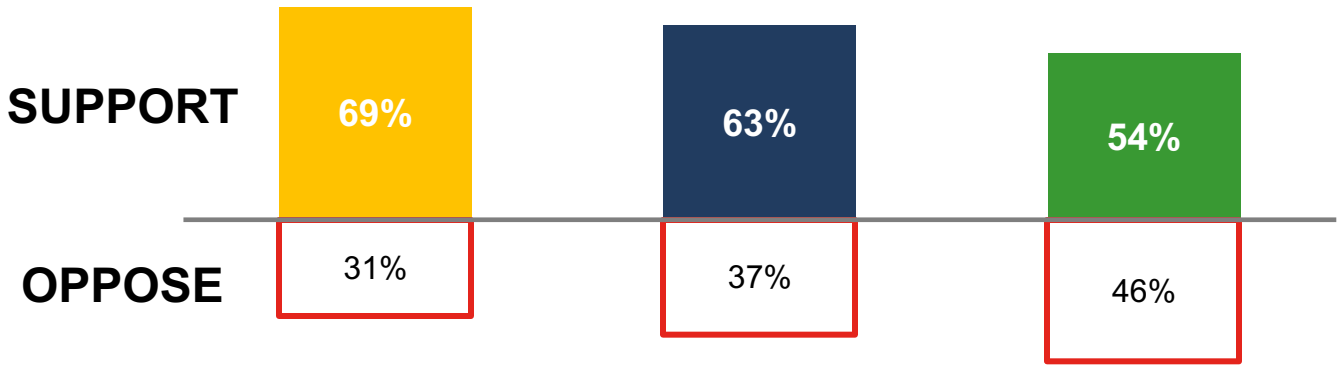


% Believe At Least One Location Has Started Using Facial Recognition by Country

Australia	France	Germany	India	Italy	Japan	Netherlands	New Zealand	UK	US
67%	73%	67%	85%	67%	65%	65%	66%	74%	67%

Despite Potential Risks, More Than 3 in 5 Consumers Support Law Enforcement and Schools Using Facial Recognition, Fewer Support Retailers Using It

Facial Recognition Scenario Support/Opposition
(Global Total)



Law enforcement
can use facial recognition cameras to scan crowds of people on the street and in public spaces, searching for known criminal suspects to better protect citizens. At the same time, law enforcement's use of facial recognition could lead to mass surveillance or mistaken identifications, leading them to blame people for a crime they didn't commit.

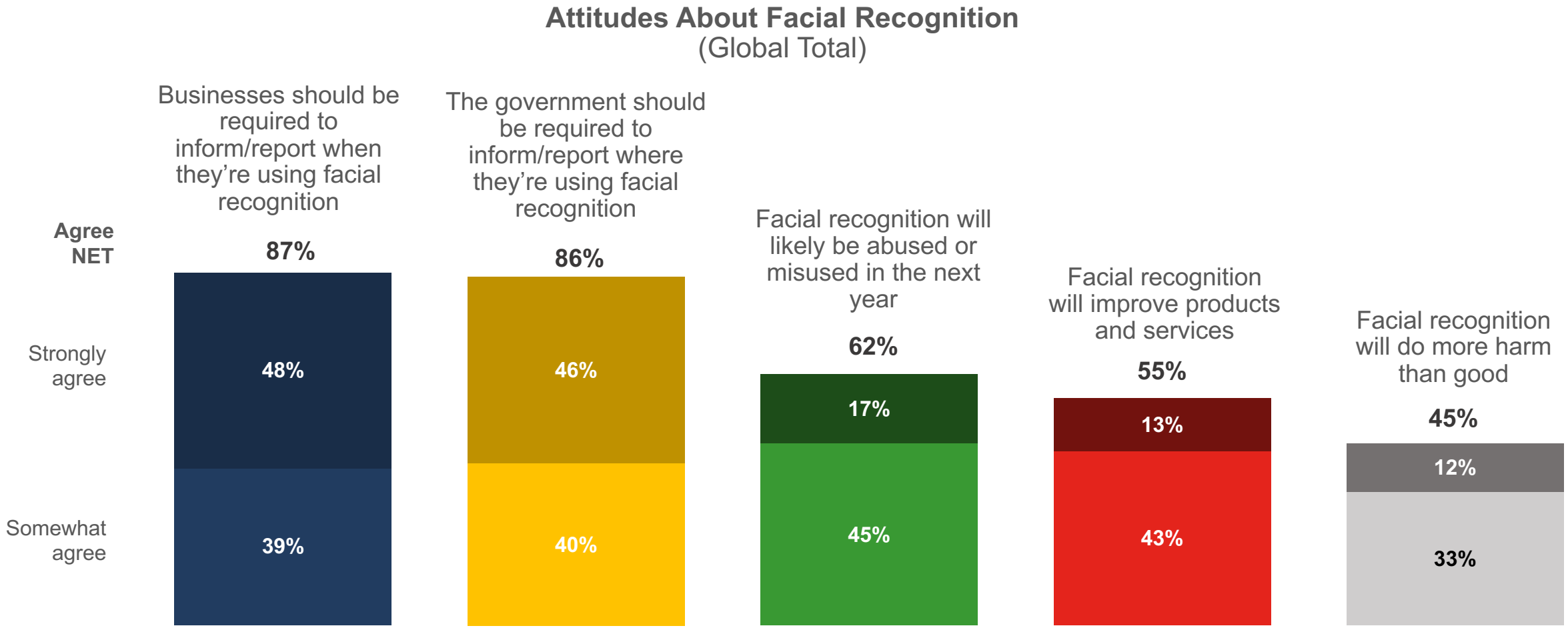
Schools
can use facial recognition cameras to better protect children's safety, scanning for suspended students, staff who were terminated, and others who are believed to pose a threat. It can also be used to identify students suspected of fighting or skipping class. The risk of using facial recognition in schools is that it can misidentify students, teachers or parents and discourage children from their freedom of expression if they feel they're being watched.

Retailers
can use facial recognition cameras to help prevent fraud and theft, comparing images of shoppers' faces against a database of known shoplifters. It can also be used to improve customer service, recognizing shoppers, so sales associates can better support customers in-store. However, if retailers use facial recognition, it's unclear where these images are saved, who has access to them and whether shoppers have the right to opt-out.

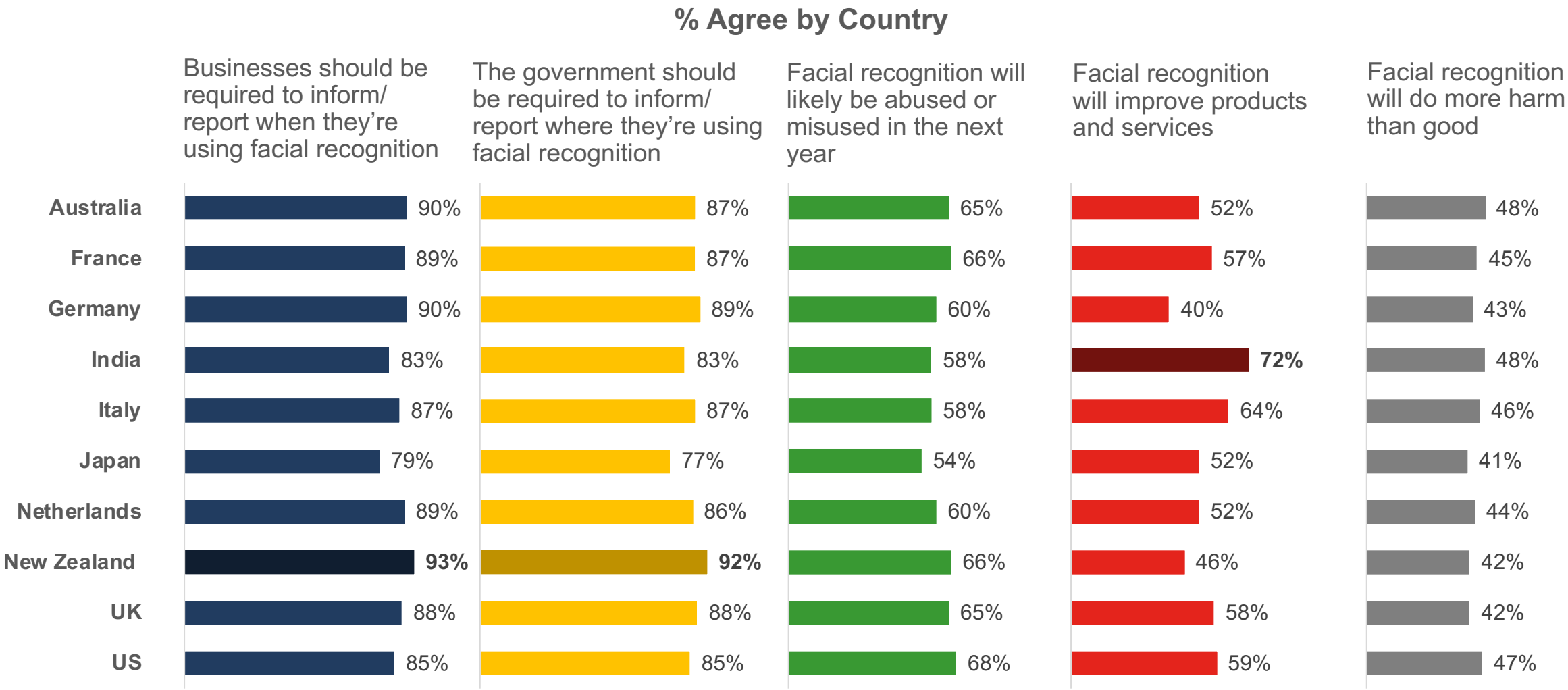
% Support Facial Recognition by Country

	Law Enforcement	Schools	Retailers
Australia	67%	59%	46%
France	66%	65%	55%
Germany	68%	53%	37%
India	76%	74%	69%
Italy	81%	74%	62%
Japan	60%	63%	59%
Netherlands	66%	57%	46%
New Zealand	67%	54%	51%
UK	72%	66%	58%
US	67%	65%	54%

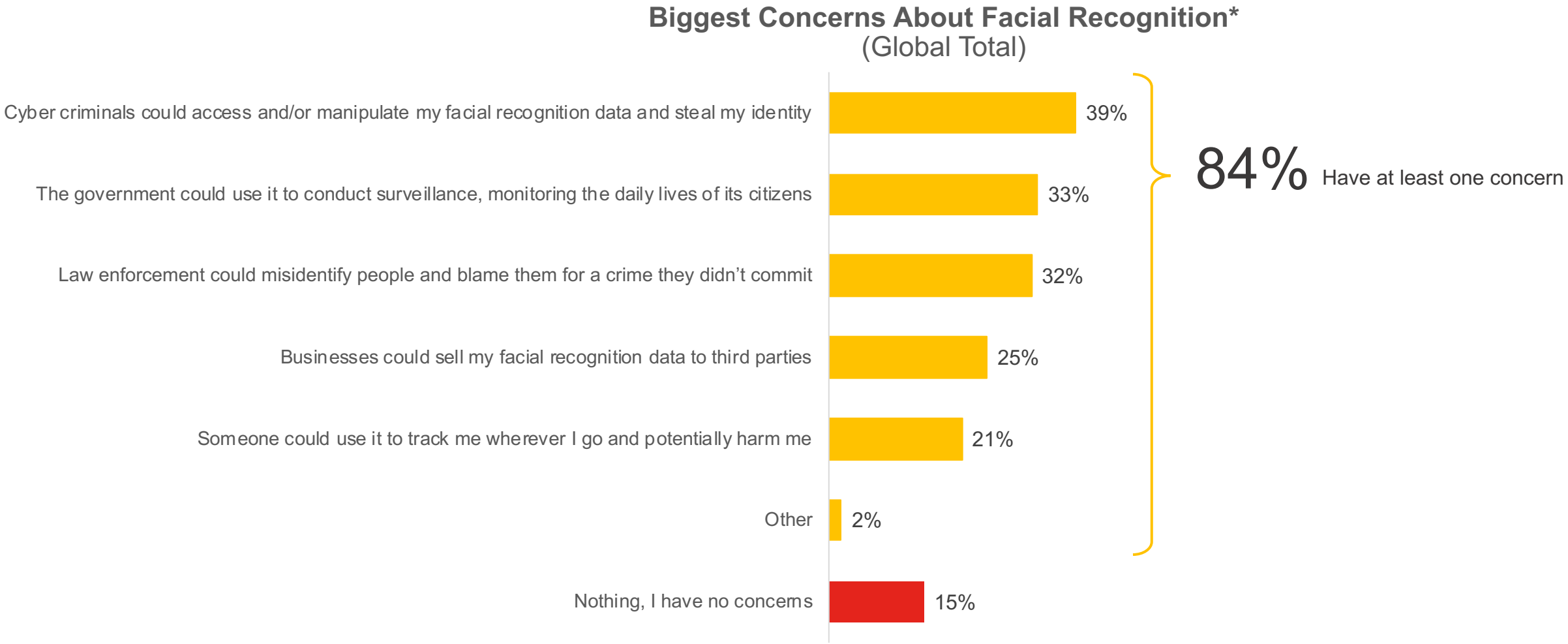
Majority Believe Businesses and Government Should Be Required to Report Facial Recognition Use; Despite Low Familiarity, Many Believe Facial Recognition Will Be Abused In The Coming Year



Majority of Consumers Think Businesses and Government Should Report/Inform Use of Facial Recognition



Majority Have Concerns About Facial Recognition, Most Commonly Cyber Criminals Accessing Data to Steal An Identity



*Respondents were asked to select up to 2 concerns.

Cyber Criminals Accessing Facial Recognition Data to Steal an Identity is One of Top 2 Concerns Across All 10 Countries

Top 2 Concerns* About Facial Recognition by Country

Australia

1. Government using it to conduct surveillance, monitoring daily lives of its citizens: 37%
2. Cyber criminals accessing/manipulating the data to steal an identity: 37%

France

1. Cyber criminals accessing/manipulating the data to an steal identity: 43%
2. Government using it to conduct surveillance, monitoring daily lives of its citizens: 38%

Germany

1. Cyber criminals accessing/manipulating the data to steal an identity: 36%
2. Law enforcement misidentifying people and blaming them for a crime they didn't commit: 34%

India

1. Cyber criminals accessing/manipulating the data to steal an identity: 46%
2. Government using it to conduct surveillance, monitoring daily lives of its citizens: 34%

Italy

1. Cyber criminals accessing/manipulating the data to steal an identity: 42%
2. Government using it to conduct surveillance, monitoring daily lives of its citizens: 29%

Japan

1. Government using it to conduct surveillance, monitoring daily lives of its citizens: 35%
2. Cyber criminals accessing/manipulating the data to steal an identity: 33%

Netherlands

1. Cyber criminals accessing/manipulating the data to steal an identity: 38%
2. Law enforcement misidentifying people and blaming them for a crime they didn't commit: 30%

New Zealand

1. Cyber criminals accessing/manipulating the data to steal an identity: 41%
2. Government using it to conduct surveillance, monitoring daily lives of its citizens: 37%

UK

1. Law enforcement misidentifying people and blaming them for a crime they didn't commit: 38%
2. Cyber criminals accessing/manipulating the data to steal an identity: 37%

US

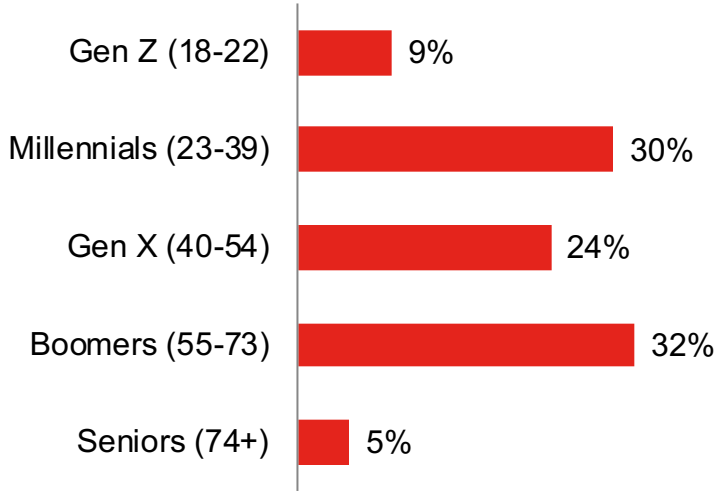
1. Cyber criminals accessing/manipulating the data to steal an identity: 39%
2. Law enforcement misidentifying people and blaming them for a crime they didn't commit: 35%

**Respondents were asked to select up to 2 concerns.*

DEMOGRAPHICS

2019 Global Demographics

Age



Gender

49% male

51% female

Current account types

86% Email account(s)

68% Social media account(s)

66% Online banking account(s)

33% Movie/media streaming account(s)

5% None of these