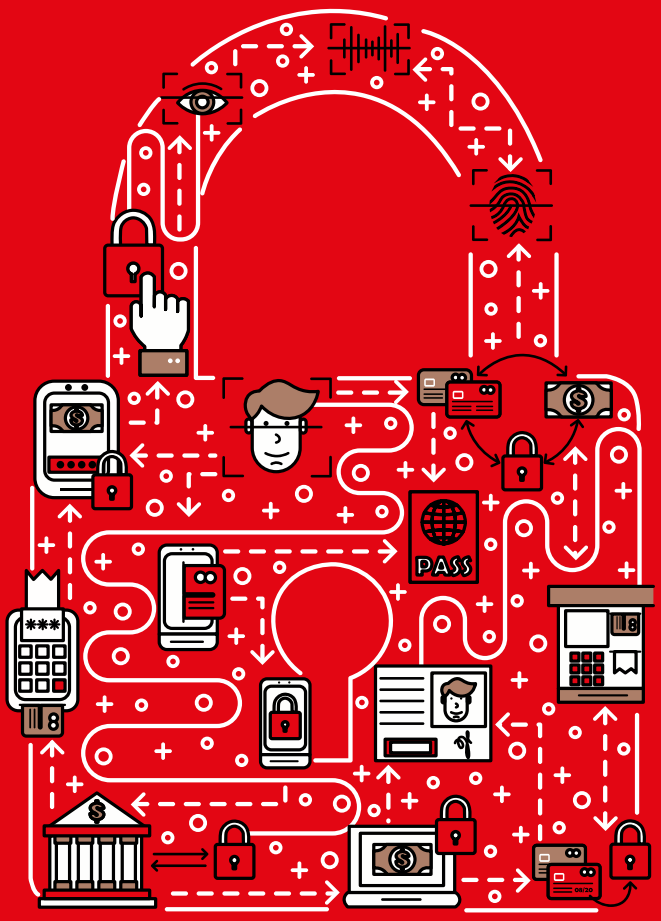
The Economist INTELLIGENCE UNIT



THE TRANSPARENT BUSINESS BAROMETER:

Preparing for the end of easy data

Sponsored by:

ANT FINANCIAL

Contents

About the research and acknowledgements

The transparent business barometer: Preparing for the end of easy data is a report from The Economist Intelligence Unit, sponsored by Ant Financial. Kim Andreasson is the author and Michael Gold the editor. Scott Aloysius assisted with data analysis. The report is largely based on a survey of 250 executives conducted in October-December 2018. All respondents represent a company that is primarily business to consumer and are very or somewhat involved with their organisation's consumer data-collection operations.

Survey takers come from China, the US, Western Europe and South-east Asia, with a minimum of 60 respondents in each country or region. Half of all respondents occupy the C-suite while the remaining half are senior executives and managers. Technology, financial services and retail are the most commonly represented industries. The main functional roles are IT and technology, general management, and marketing. Half of all executives come from companies with more than US$500m in global annual revenue while half come from companies earning below that threshold. See appendix I for a full breakdown of the survey demographics.

To better understand the opportunities and challenges of a changing data-privacy landscape, interviews were conducted with advisory board experts and supplemented with wide-ranging desk research to inform the executive survey. Our thanks are due to the following advisory board members for their time and insights:

- Daniel Castro, vice-president, Information Technology and Innovation Foundation
- Ann Cavoukian, distinguished expert-in-residence, Privacy by Design Centre of Excellence, Ryerson University
- J Trevor Hughes, president and CEO, International Association of Privacy Professionals
- Yan Luo, of counsel, Covington & Burling
- Zhou Hanhua, professor of law, Chinese Academy of Social Sciences

Additional insights were obtained from in-depth interviews conducted after the completion of the survey. Our thanks are due to the following individuals:

- Andrew Ballen, founder and CEO, AVD Digital Media
- Simon Chesterman, provost's chair and dean, National University of Singapore Faculty of Law
- Gus Hosein, executive director, Privacy International
- Mohan Veloo, technology lead, Asia-Pacific, China and Japan, F5 Networks
- Steve Wood, vice-president, Asia-Pacific, Aruba, a Hewlett Packard Enterprise company

Executive summary

The rapidly growing amount of data created in digital societies has led to an increase in personal data collection and usage for commercial purposes. Many large international companies use data to sell targeted advertising and services, while smaller organisations may also collect and sell such information to other businesses, or for other reasons. For instance, data gathering can reduce costs, help improve existing services and provide opportunities for innovation, such as geo-location information to match supply and demand in certain fields, like ride-sharing.

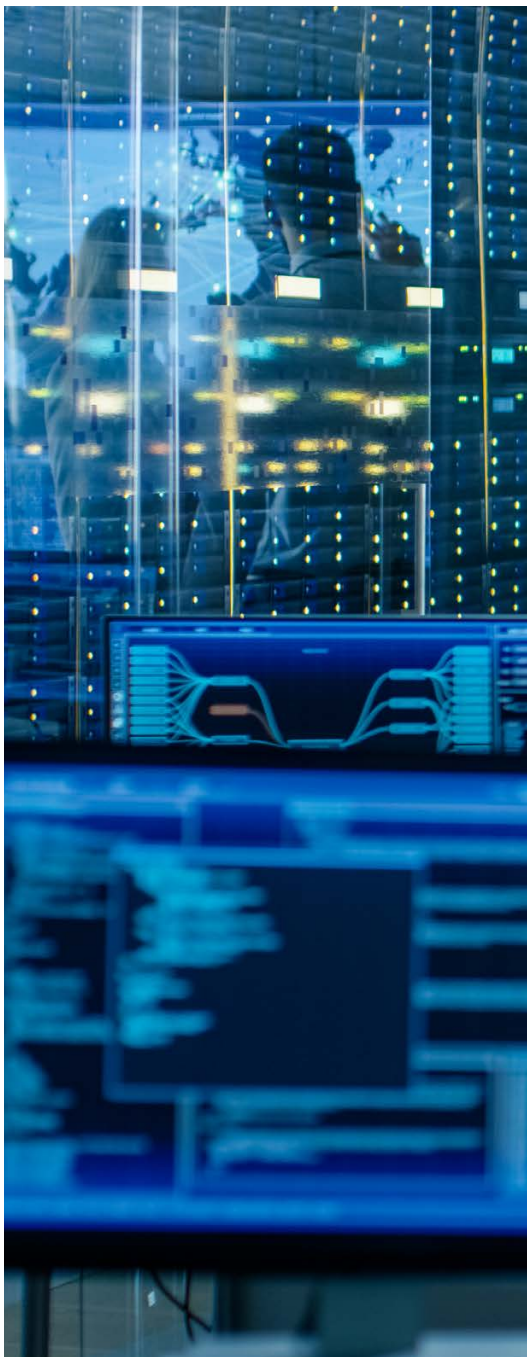
At the same time, personal data-collection efforts have increasingly been met with scepticism among regulators and the general public alike about the type and amount of data that companies can hold about individuals and how it can be used, largely due to privacy and cyber-security concerns.

This report finds that companies are aware of the importance of data privacy and are taking measures to meet the new reality of a more privacy-conscious world; however, there are differences between regions and large and small companies in both preparedness and measures taken. The key findings are:

- **Data privacy is becoming increasingly important to organisations in the face of numerous rising concerns.** In an era in which data-privacy topics make international headlines almost daily, nearly 100% of survey takers in Asia, Europe and the US agree that data privacy is important to their organisation today and 91% say it will be much more or more important in three years' time.
- **Executives in China and South-east Asia are more likely to tie data privacy practices to good corporate governance than those in the West.** Almost all executives in China (98%) agree that data privacy is an important part of good corporate governance—running counter to the commonly held view that privacy is an afterthought for Chinese firms.
- **Cyber-security concerns will be the chief driver of stronger data-protection strategies.** Illustrated by the frequency and scope of recent data breaches, the primary data-related worry among executives in our survey is the risk of data leaks from lapses in cyber-security. Boosting corporate governance and rising consumer demand take second and third place, respectively.
- **American executives believe their companies are more prepared to face regulations than those in other regions.** A barometer constructed for this study shows that companies are generally prepared and willing to take measures to meet emerging challenges, although the results vary by region, especially between Europe, which lags in readiness, and the US, which is well ahead. Regulations that create a level playing field for companies, especially those operating across borders, may be a welcome development as concerns over data privacy proliferate.
- **Executives generally believe people are willing to trade data privacy for improved services.** In our survey, three out of four American executives agreed with this sentiment, higher than the

average figure of about two in three. The equivalent figure for China, meanwhile, sits at 67%, again demonstrating that regional stereotypes around privacy may warrant closer inspection.

- **Small firms lag their large counterparts in readiness to face regulations.** The argument that one-size-fits-all regulations may stifle innovation among start-ups, while large firms can use their vast resources to manage compliance, gains support among our survey panel.



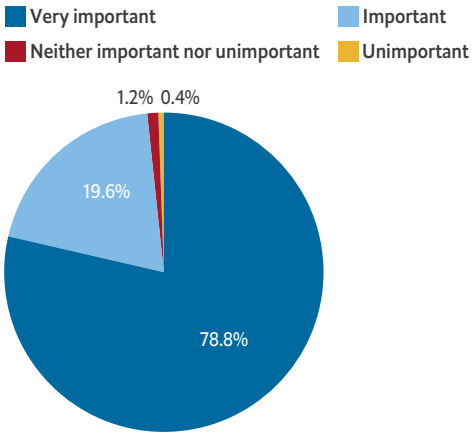
Introduction. Data in demand

By any measure, the amount of data created is increasing rapidly, with the breadth and depth of such data generating significant value for the organisations collecting them. A 2017 headline in *The Economist* exclaimed that "the world's most valuable resource is no longer oil, but data."[1] Among other actors, international platform providers such as search engines and social media companies use data, often personal, to sell targeted ads and create innovative solutions based on data analytics. A recent article in *The New York Times*, for example, illustrated that many companies use apps on increasingly ubiquitous mobile devices to gather geographical information on users, generating a location-based advertising market worth about US$21bn in 2018.[2]

Privacy proponents are objecting to such laissez-faire practices, and in response many policy-makers have established new guidelines for data collection and data privacy, such as the EU's General Data Protection Regulation (GDPR), which went into effect in May 2018 and also applies to foreign companies doing business in the region.[3] Violators of the GDPR may be fined up to €20m (US$22.8m) or 4% of annual global turnover, whichever is greater.[4] Globally, the way companies acquire and use personal data has never been under as much scrutiny as it is now, making improving data-privacy strategies a top priority for businesses. "The enormous increase in not only the scope of risk, but the complexity of risk, is the first challenge," says J Trevor Hughes of the International Association of Privacy Professionals. He notes that the pace of change, both with regard to technological innovation changing the understanding of privacy, and to the number of laws, regulations and expectations that are emerging around the world, is creating headaches for organisations.

Companies are taking notice of the changing landscape, both in terms of regulations and more broadly. In the survey conducted for this report, about four in five executives say data privacy is "very important" to their organisations today, with another one in five saying it is simply "important".

Figure I. Safeguarding the new oil
How important is data privacy to your organisation today?



Source: The Economist Intelligence Unit

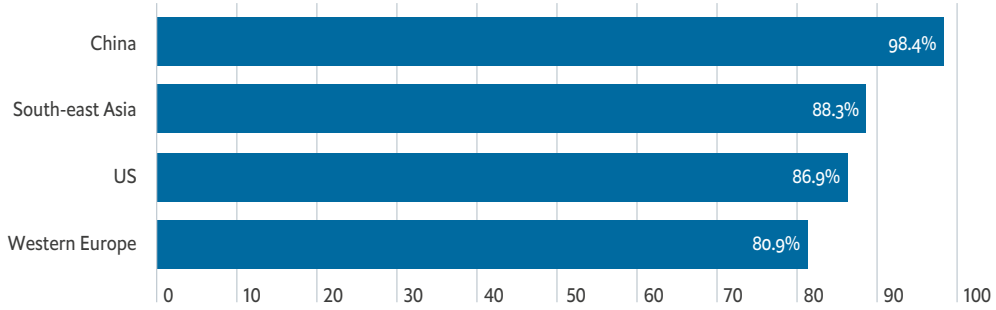
A majority (54%) of executives also say data-privacy will be much more important in three years' time.

1 "The world's most valuable resource is no longer oil, but data", *The Economist*, May 6th 2017
2 Jennifer Valentino-DeVries, Natasha Singer, Michael H Keller and Aaron Krolik, "Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret", *The New York Times*, December 10th 2018
3 EU GDPR Portal
4 Ibid

One reason that executives are paying increasing attention to data privacy is its perceived importance to good corporate governance in future. Almost nine in ten (88%) executives agree with this sentiment; among Chinese executives, the figure reaches 98%. One reason for this disparity may be improved understanding of data-privacy regulations among Chinese executives. Overall, 83% of all survey takers agree that their knowledge of such laws has improved in the past three years; in China the equivalent figure is 92%. Another reason may be the importance of trust, which in China may be higher between data-gatherers (companies and/or the government) and data-providers (individuals) than in other regions.[5] "China understands how important basic online trust is in the shared economy," says Andrew Ballen of Shanghai-based AVD Digital Media.

> **"China understands how important basic online trust is in the shared economy.**
>
> *Andrew Ballen, AVD Digital Media*

Figure II. Transparent and trusted
Data privacy will be important to good corporate governance in future (% agreeing, by region)



Source: The Economist Intelligence Unit

5 David Brooks, "How China Brings Us Together", *The New York Times*, February 14th 2019

Box I. The transparent business barometer: Gauging the impact of future data-privacy regulations

In our survey, executives were asked to rate on a one-to-ten scale their readiness to face data-privacy regulations and their likelihood of taking various actions in response. Specifically, the readiness question (composed of five sub-questions) asked how prepared organisations are to deal with various aspects of regulations, including that which might restrict the ability to view, analyse, buy or sell consumer data. The likelihood question (composed of three sub-questions) asked how likely it is that organisations will take different measures moving forward, such as withdrawing operations from certain jurisdictions, in response to potentially stricter data-privacy regulations.

An answer between one and four is considered low preparedness/likelihood, a score of five to seven indicates medium preparedness/likelihood and a score of eight to ten suggests high preparedness/likelihood. Given the differences in the number of questions per category and the number of respondents per country and region, the scores were weighted in order to use numerical answers as a proxy for preparedness/likelihood across countries or regions.

Key findings

The transparent business barometer shows that survey takers are relatively well prepared to face regulations (7.36 out of ten) but relatively less likely to take different measures in response (6.47 out of ten). The average score across all geographies and categories was 7.02.

Figure III. Privacy pioneers
Transparent business barometer aggregate scores, by region

	Country or region				
	China	US	Western Europe	South-east Asia	Total
Readiness	7.35	8.04	6.69	7.42	7.36
Likelihood	6.58	7.16	5.67	6.56	6.47
Overall	7.06	7.71	6.31	7.10	7.02

Source: The Economist Intelligence Unit

There are large geographic differences. American executives are the most prepared (8.04), despite differing regulations across states and industry sectors. US executives are also the most bullish about trying different measures to meet regulations (7.16). Conversely, Europeans are the least prepared (6.69) and least willing to attempt new approaches (5.67). Scores from China and South-east Asia fall between these two outliers. See appendix II for full barometer questions and results by region.

Simon Chesterman of the Faculty of Law at the National University of Singapore explains these regional differences by noting that "Europe is driven by individual rights and America by corporate interests, while in Asia, governments have been trying to make a home for 'safe' data," which refers to a top-down approach meant to secure information on behalf of users and attract big-data companies.

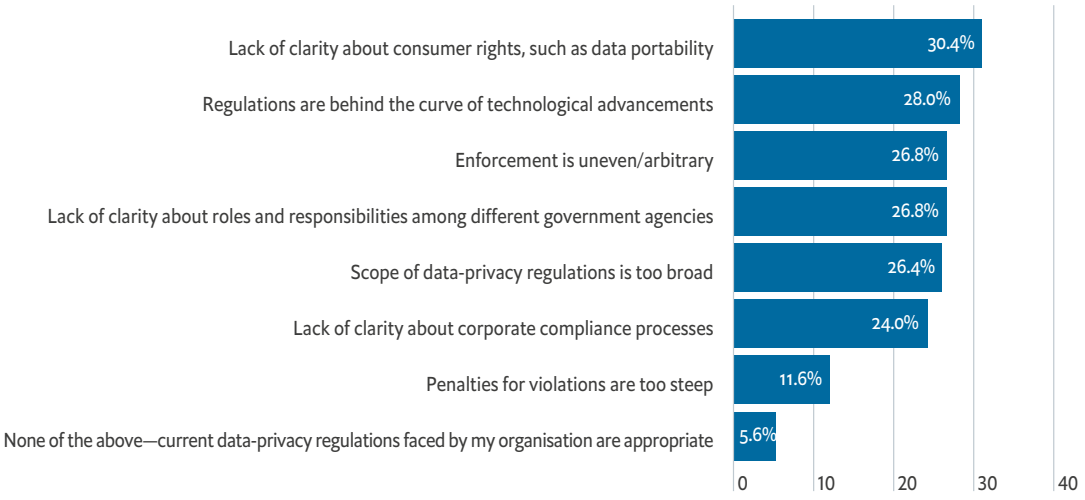
Chapter 1. Regulating their way to the top: Challenges and opportunities of data-privacy laws

The EU's GDPR has undoubtedly taken centre stage in the debate around data-privacy regulations. In January 2019 CNIL, France's data-protection regulator, slapped Google with the largest fine to date under the GDPR, to the tune of €50m (US$57m).[6]

Yet GDPR may be having less of an impact than many believe. In our survey, fewer European executives believe data privacy is very important to their organisation (71% compared with 79% of all executives) and fewer still believe it will be much more important in three years' time (38% compared with 54% across all regions). As indicated in the transparent business barometer (see box I), one reason may be that European executives are waiting to see how regulations actually play out in practice and whether hefty fines will continue to be issued. Having regulations on the books may not be effective unless they are carried out, says Gus Hosein of Privacy International, a watchdog group. "Enforcement is definitely the bigger problem."

Indeed, uneven and/or arbitrary enforcement ranks among the top regulation-related challenges, named by just over a quarter of executives. Conversely, only about one in eight cited penalties for violations as being too steep. Lack of clarity about consumer rights, such as data portability, regulations that are behind the curve of technological advancements, and lack of clarity about roles and responsibilities among different government agencies comprise the other top challenges.

Figure IV. Laying down the law
What are the biggest data-privacy barriers faced by your organisation with regard to regulations?



Source: The Economist Intelligence Unit

6 "The French fine against Google is the start of a war", *The Economist*, January 24th 2019

Following suit?

Overall, almost six in ten (59%) executives agree that data-privacy regulations in their country are stricter than those in other countries; however, executives in the US are even more likely to agree (71%)—despite the fact that regulations appear stricter in Europe, a point that may come back to enforcement.

"GDPR certainly has a capital R when it comes to regulation," says Mr Hosein. "But the US is not necessarily a Wild West when you consider how often a company gets sued." This underscores that the key difference between the two regions may be that Europeans can often turn to a regulator for redress, whereas in the US, alleged data-privacy violations frequently require a complicated legal process to settle, he says.

Rolling out the red carpet for stronger rules

Stronger regulations could be a welcome trend among companies that are worried about losing business to competitors engaging in questionable data practices, but technically following the letter of the law. "It's hard to be a good actor in this space when breaking the rules is working in places, or where there are no rules," says Mr Hosein.

Contrary to the notion that any data-protection regulation creates obstacles, international companies are also increasingly lobbying for greater clarity through co-ordinated regulations that will create an equal playing field and enable data to flow across borders. "I think there is a realisation that diverse laws make it complicated to transfer data across jurisdictions," says Simon Chesterman of Singapore National University's Faculty of Law. "Many jurisdictions either have no data-protection law or have only adopted one in the last couple of years."

Indeed, some of the world's largest data-gatherers are calling for lawmakers to take action. In late 2018 Tim Cook, CEO of Apple, praised the GDPR and called on the US to establish a similar comprehensive data-privacy protection regulation to avoid poor practices and maintain trust in honest technology providers.[7] Similarly, Sundar Pichai, CEO of Google, told American legislators in late 2018 that GDPR was a "well-crafted piece of legislation" and noted the benefits of consistent regulation.[8] Many other American internet companies have lobbied for a federal privacy law to replace a hotchpotch of state privacy laws. In Asia too, there is a growing sense of the benefits of common regulations, says Mohan Veloo of F5 Networks, an IT services provider, although the region's sheer diversity and size make this more difficult to implement in practice.

> **"It's hard to be a good actor in this space when there are no rules.**
>
> *Gus Hosein, Privacy International*

7 Tony Romm, "Apple's Tim Cook blasts Silicon Valley over privacy issues", *The Washington Post*, October 24th 2018
8 Daisuke Wakabayashi and Cecilia Kang, "Google's Pichai Faces Privacy and Bias Questions in Congress", *The New York Times*, December 11th 2018

Box II. Hacking the individual: Exploring the link between data privacy and cyber-security

The primary reason executives in our survey plan to enhance their firms' data-privacy strategies is cyber-security, which is cited by 44% of respondents, significantly higher than justifications such as corporate good-governance and growing consumer demand, the second and third leading options.

This indicates a growing awareness that the collection and usage of personal data is only one part of the privacy equation: the other is keeping it secure. The increasing number and volume of data breaches, now almost daily news fodder, garner significant media attention and compel companies to pay greater attention to the issue. "It is not just the potential but inevitability of data breaches," says Simon Chesterman of the Faculty of Law at the National University of Singapore, noting the new notion in the cyber-security community that everyone will be hacked at some point.

This notion is reinforced by our survey. It is notable that the education of company management about the importance of data privacy is the most cited way that organisations plan to enhance their current data-privacy strategy (cited by 56% of respondents), indicating a current lack of awareness. The same challenge applies to cyber-security: high-level executives often recognise the importance of the topic but find it difficult to comprehend in business terms, as the lingo is often too technical and the amount of data too vast.[9] Mohan Veloo of F5 Networks, an IT services provider, notes that organisations in Asia are "just waking up to" the threat of cyber-security breaches, and that often the only time they take action is in response to an incursion.

Figure V. Cyber-spooks
What are the main reasons your organisation plans to enhance its data-privacy strategy?

Source: The Economist Intelligence Unit

9 Ramsés Gallego, "Security Think Tank: Communication is key to cyber security in digital era", Computer Weekly, December 2016

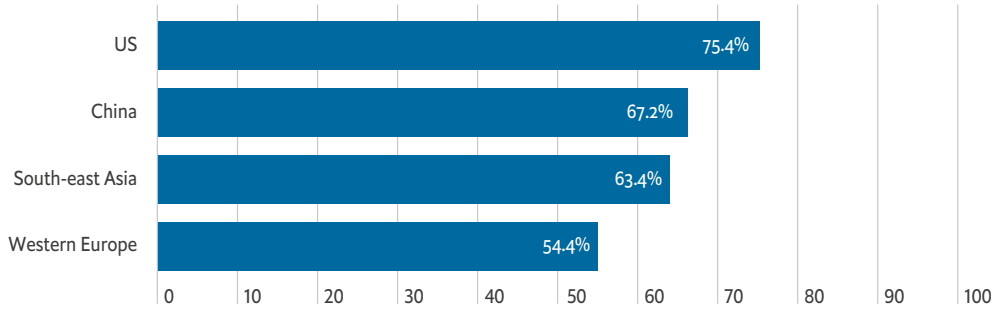
Chapter 2. Data dispersal: Who should own your personal digital information?

About half (51%) of survey takers strongly agree that consumers should have authority over how their data are used. However, there is a large discrepancy between regions: a majority of American (57%) and European (56%) executives strongly agree; conversely, those holding this opinion are a minority in China (38%). Although our survey captures the attitudes of executives, rather than consumers, experts acknowledge that data privacy is not always top-of-mind for individuals either. "[People] say they care about data privacy in theory, but their practices depart from that significantly," says Mr Chesterman.

This is reflected by the fact that major online platforms like Facebook remain popular despite recent lapses in data handling. Indeed, almost two-thirds (65%) of executives in our survey say consumers are willing to trade data privacy for improved services, with China just about average and far more American executives agreeing—a finding that is re-enforced by other recent research. According to a January 2019 survey from the Center for Data Innovation, a Washington DC-based think-tank, almost six in ten American respondents (58%) said they are willing to let a third party collect at least one piece of sensitive personal data, such as biometric, location or medical data, in exchange for a service or benefit. This may highlight a preference for convenience in the land of the free.[10]

> **[People] say they care about data privacy in theory, but their practices depart from that significantly.**
>
> *Simon Chesterman, Faculty of Law, National University of Singapore*

Figure VI. Service with a smile
In my country, consumers are willing to trade data privacy for improved services (% agreeing, by region)



Source: The Economist Intelligence Unit

10 Daniel Castro and Michael McLaughlin, "Survey: Majority of Americans Willing to Share Their Most Sensitive Personal Data", Center For Data Innovation, January 22nd 2019

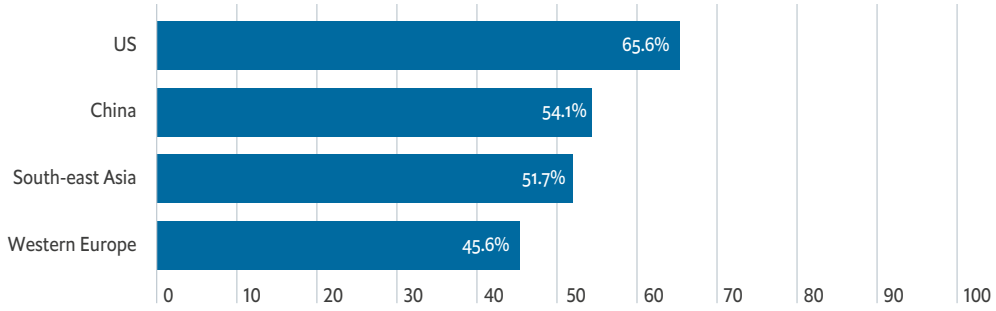
Steve Wood of Aruba, a digital infrastructure firm and subsidiary of computer giant Hewlett Packard, says the proliferation of personal data means people have come to expect companies to possess a level of insight during their interactions that they hadn't previously. "There's an expectation that you've got to know your customer" in order to provide services for them, he says.

Old-world malaise?

American companies are often considered more aggressive than those elsewhere about exploiting opportunities to seize big data to innovate and provide more targeted advertising and other services. Conversely, European firms have been accused of lagging in spearheading the types of disruptive innovation often thought to require large amounts of data; the continent largely lacks the type of nimble tech platforms currently storming the world from the likes of the US and China. This could be the reason why less than half of European survey-takers agree that the current trend in data privacy regulations threatens to stifle innovation, versus two-thirds in the US and about half in each of China and South-east Asia.

Some believe this will mean that Europe may lose out in the long run: organisations such as the Information Technology and Innovation Foundation, an American think-tank, have argued that current data regulations threaten Europe's potential leadership in artificial intelligence, the development of which is dependent on huge reams of data.[11]

Figure VII. Innovation nations
The current trend in data-privacy regulations threatens to stifle innovation (% agreeing, by region)



Source: The Economist Intelligence Unit

11 Nick Wallace, "Europe is About to Lose the Global AI Race – Thanks to GDPR", EURACTIV, May 25th 2018

Box III. Working with giants: Data-privacy management in large versus small firms

According to the transparent business barometer, smaller companies (those with revenue below US$500m) show less readiness to face data-privacy regulations than their larger counterparts. For example, when asked how prepared they are to face regulation that might restrict their organisation's ability to gather data directly from consumers, 48% of small-company executives say they are highly prepared (indicated by a score between eight and ten on the ten-point barometer), compared with 62% of large-company executives. Similarly, only 50% of small-company executives are highly prepared to deal with regulation that might restrict their organisation's ability to buy or sell consumer data with other companies, compared with 64% of their large-company counterparts.

Figure VIII. Data gluttons
Transparent business barometer aggregate scores, by company size

	Annual revenue		
	Less than US$500m	US$500m or more	Total
Readiness	7.09	7.63	7.36
Likelihood	5.88	7.06	6.47
Overall	6.63	7.41	7.02

Source: The Economist Intelligence Unit

Smaller companies are also less likely to say they would change their business model to reduce reliance on consumer data (38% compared with 63% among larger companies) or lobby government at a national or international level to change data-privacy regulations (32% v 48%). See appendix II for full barometer results by company size.

Only 50% of small-company executives are highly prepared to deal with regulation that might restrict their organisation's ability to buy or sell consumer data with other companies, compared with 64% of their large-company counterparts.

Ann Cavoukian of the Privacy by Design Centre of Excellence at Ryerson University, and a three-term privacy commissioner for Ontario, Canada, believes small and medium-sized enterprises are struggling most likely because they have limited finances and limited ability to address data-privacy issues. "Large companies have privacy professionals, legal staff and IT people [to help them face these challenges]," she says, noting that the best way to protect data privacy for the consumers that use the services of these large firms is to work with them proactively, rather than taking a punitive approach.

Conclusion. Privacy and propriety: Managing uncertainty in a data-driven world

It has become clear that data privacy is not a concern only of large platform companies like Facebook and Google, but rather has risen to the top of corporate agendas across the board due to new and emerging regulations and increasingly common and vast cyber-security breaches. Companies are taking notice of these and are generally well prepared and willing to make changes to business-as-usual, even though attitudes differ by region and company size.

There is, however, a great deal of uncertainty about the path forward. "The reality of the [GDPR] is that it is too soon to know if it even works," says Mr Hosein, expressing a sentiment reflected in the barometer readings. "Merely passing a law is meaningless compared with seeing how the regulator responds." At the same time, many international consumer-facing data and platform providers are calling for regulations to create greater clarity in this fast-moving space, especially for those doing business across borders. These may signify an end to the availability of "easy data", but it will hopefully make the business world more transparent and trustworthy going forward.

Trust is the corporate carrot

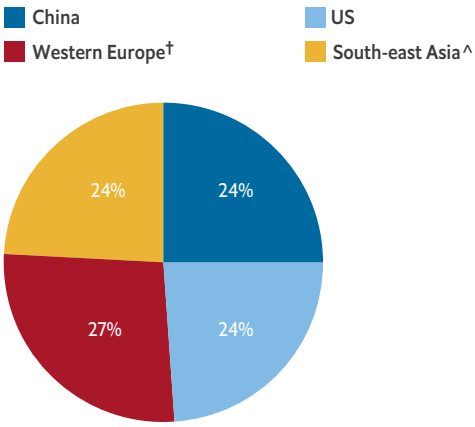
Although the tension between data privacy and improved services will not ease anytime soon, Ann Cavoukian of the Privacy by Design Centre for Excellence at Ryerson University, and a three-term privacy commissioner for Ontario, Canada, says one easy fix companies can take is to allow consumers to "opt-in" to data gathering and manipulation, rather than forcing them to opt-out. "Building trust is huge," says Ms Cavoukian. "If you have privacy by design, you have a trusted relationship."

This trust will inevitably feed into a company's corporate reputation, a factor that will probably surface as a key competitive differentiator in a future data-driven world. Ms Cavoukian sums up the sentiment: "We need to position privacy and business interests as a win-win in all areas."

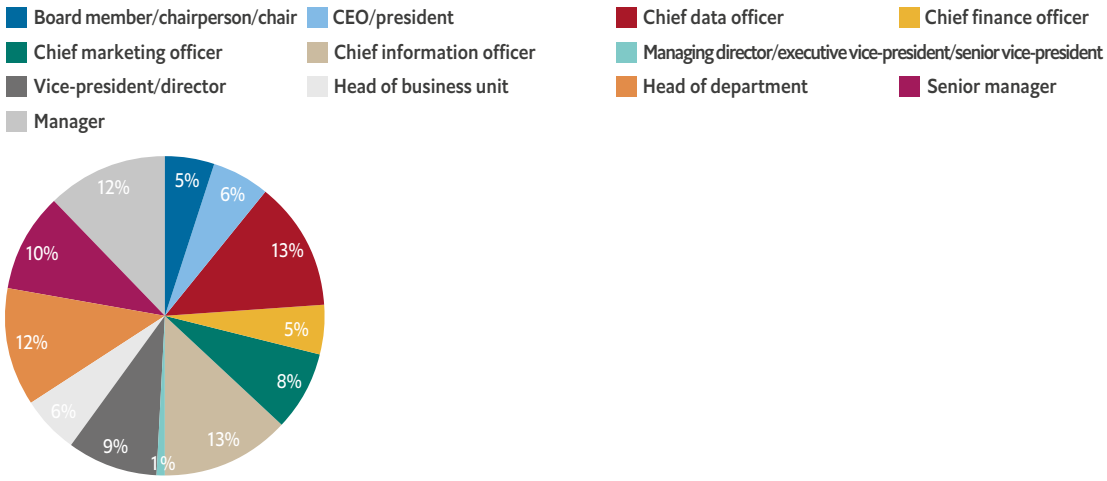
> **If you have privacy by design, you have a trusted relationship.**
>
> *Ann Cavoukian, Privacy by Design Centre for Excellence, Ryerson University*

Appendix I. Survey demographics*

D1. In which country/region are you personally located?



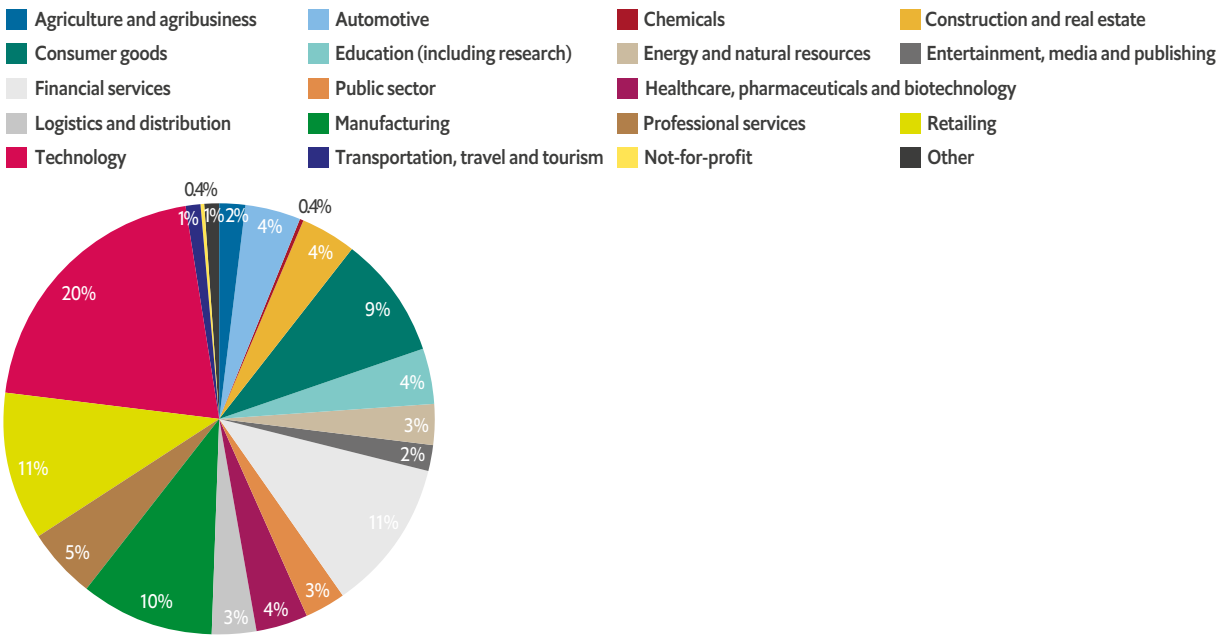
D2. Which of the following best describes your title?



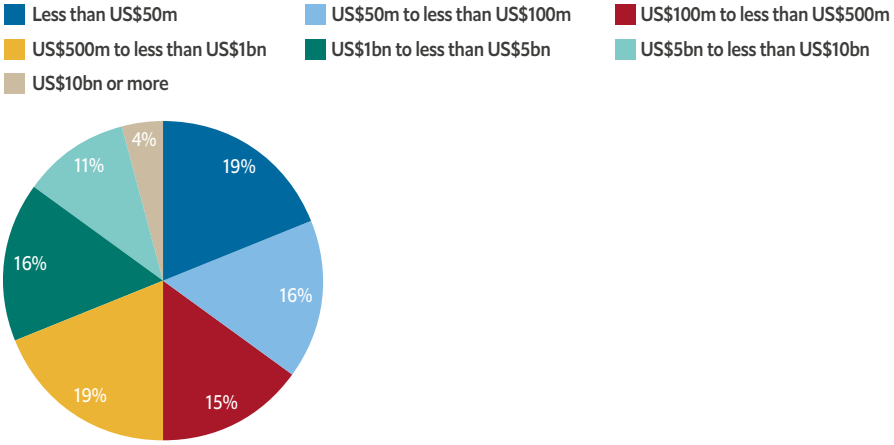
*Not all questions may add up to 100 due to rounding
^Encompasses Indonesia, Malaysia, the Philippines, Singapore, Thailand and Vietnam
†Encompasses Belgium, France, Germany, Luxembourg, the Netherlands and the UK

D3. What is your main functional role?

D4. What is your company's primary industry?



D5. What is your company's annual global revenue?



Appendix II. Barometer readings

By region

	Country or region				
Question	China	US	Western Europe	South-east Asia	Total
How prepared is your organisation to deal with regulation that might restrict your organisation's ability to gather data directly from consumers?	7.26	8.11	6.82	7.35	7.37
How prepared is your organisation to deal with regulation that might restrict your organisation's ability to view or analyse consumer data?	7.20	8.03	6.76	7.47	7.35
How prepared is your organisation to deal with regulation that might restrict your organisation's ability to buy or sell consumer data with other companies?	7.51	8.23	6.66	7.45	7.44
How prepared is your organisation to deal with regulation that might restrict your organisation's ability to leverage consumer data to target customers more effectively?	7.44	8.05	6.79	7.60	7.45
How prepared is your organisation to deal with regulation that might restrict your organisation's ability to transfer consumer data across national borders?	7.33	7.75	6.43	7.25	7.17
Readiness average	**7.35**	**8.04**	**6.69**	**7.42**	**7.36**
Looking ahead, how likely is it that stricter data-privacy regulations at the national or international level will cause your organisation to withdraw operations from certain countries/ jurisdictions where data-privacy regulations are too strict?	6.46	7.00	5.62	5.75	6.19
Looking ahead, how likely is it that stricter data-privacy regulations at the national or international level will cause your organisation to change your business model to reduce reliance on consumer data?	7.26	7.43	6.01	7.15	6.94
Looking ahead, how likely is it that stricter data-privacy regulations at the national or international level will cause your organisation to lobby government at a national or international level to change data-privacy regulations?	6.02	7.05	5.38	6.77	6.28
Likelihood average	**6.58**	**7.16**	**5.67**	**6.56**	**6.47**
Overall average	**7.06**	**7.71**	**6.31**	**7.10**	**7.02**

By company size

Question	Annual revenue: Less than US$500m	Annual revenue: US$500m or more	Total
How prepared is your organisation to deal with regulation that might restrict your organisation's ability to gather data directly from consumers?	7.17	7.58	7.37
How prepared is your organisation to deal with regulation that might restrict your organisation's ability to view or analyse consumer data?	7.11	7.58	7.35
How prepared is your organisation to deal with regulation that might restrict your organisation's ability to buy or sell consumer data with other companies?	7.16	7.72	7.44
How prepared is your organisation to deal with regulation that might restrict your organisation's ability to leverage consumer data to target customers more effectively?	7.20	7.70	7.45
How prepared is your organisation to deal with regulation that might restrict your organisation's ability to transfer consumer data across national borders?	6.79	7.54	7.17
Readiness average	**7.09**	**7.63**	**7.36**
Looking ahead, how likely is it that stricter data-privacy regulations at the national or international level will cause your organisation to withdraw operations from certain countries/ jurisdictions where data-privacy regulations are too strict?	5.58	6.80	6.19
Looking ahead, how likely is it that stricter data-privacy regulations at the national or international level will cause your organisation to change your business model to reduce reliance on consumer data?	6.43	7.44	6.94
Looking ahead, how likely is it that stricter data-privacy regulations at the national or international level will cause your organisation to lobby government at a national or international level to change data-privacy regulations?	5.62	6.94	6.28
Likelihood average	**5.88**	**7.06**	**6.47**
Overall average	**6.63**	**7.41**	**7.02**

The Economist INTELLIGENCE UNIT

LONDON

20 Cabot Square
London, E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8500
Email: london@eiu.com

GENEVA

Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
Email: geneva@eiu.com

NEW YORK

750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
Email: americas@eiu.com

DUBAI

Office 1301a
Aurora Tower
Dubai Media City
Dubai
Tel: (971) 4 433 4202
Fax: (971) 4 438 0224
Email: dubai@eiu.com

HONG KONG

1301 Cityplaza Four
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
Email: asia@eiu.com

SINGAPORE

8 Cross Street
#23-01 Manulife Tower
Singapore
048424
Tel: (65) 6534 5177
Fax: (65) 6534 5077
Email: asia@eiu.com