The Economist Intelligence Unit

PRIVACY UNCOVERED

CAN PRIVATE LIFE EXIST IN THE DIGITAL AGE?

A report from the Economist Intelligence Unit

SPONSORED BY:

beazley

Contents

About the report

Privacy uncovered: Can private life exist in the digital age? is an Economist Intelligence Unit (EIU) report, sponsored by Beazley. It examines consumer attitudes to the sharing and storage of personal data online as well as the implications for companies.

The report draws on two main sources for its research and findings:

- A global survey of 758 adult Internet users conducted in January and February 2013. Almost all of the respondents (97%) use the Internet daily. Respondents come from across the world, with 32% based in Western Europe, 30% in the Asia-Pacific region, 20% in North America and the remainder in Latin America, the Middle East, Africa and Eastern Europe. Respondents also have a range of ages. Nearly three-fifths (59%) are male and 41% female.

- A series of in-depth interviews with experts and leaders from business, government and the NGO community listed here:
  - Richard Allan, European director of policy, Facebook
  - Richard Baker, EMEA chairman, Aimia
  - Alex Fowler, global privacy and public policy lead, Mozilla
  - Michael Harte, chief information officer, Commonwealth Bank of Australia
  - Nellie Kroes, European commissioner, Digital Agenda for Europe
  - Ponnurangam Kumaraguru, professor, Indraprastha Institute of Information Technology
  - Joe McNamee, executive director, European Digital Rights

We would like to thank all interviewees and survey respondents for their time and insight.

The report was written by Dr Paul Kielstra and edited by Sara Mosavi.

Executive summary

In the world that George Orwell created in his novel *1984*, every word and action is recorded and filmed by a tyrannical government led by Big Brother. The material is then used to indict rebellious citizens. In the fictional nation of Oceania, where *1984* is set, privacy has no place: "If you want to keep a secret, you must also hide it from yourself."

In the real world, we are far from the kind of personal infringement suffered in *1984*, but individual privacy is increasingly at risk. Facebook profiles, Google searches and Amazon purchases can be mined for information with ever more sophisticated tools that help create incredibly detailed pictures of individual users.

In *Privacy uncovered*, we examine the complex relationship that consumers have with their personal data. The research conducted for the report discovers that while consumers have become more liberal in sharing data, they remain concerned—and feel in the dark—about how they will be used and by whom. This has significant implications for how businesses collect and use consumer data. The key findings of this report are:

Consumers don't know how their data is used, and think regulation and data protection are weak. When asked about the security of their personal information held by a number of entities, consumers only rarely said it was very secure. This is particularly the case for online entities: only 3% say that their data is very secure with social networks and 11% say the same about online retailers. Meanwhile, just 26% think that businesses are transparent enough in how they use customers' personal data, and three-quarters of respondents believe that regulation preventing the misuse of such information is too weak.

Although fears of potential abuse abound, they are not stopping consumers from sharing data. Individuals are increasingly willing to share information. Over four-fifths (84%) of survey respondents, for example, belong to social networks, and 34% say that they are more willing to share basic personal information online than they were three years ago, compared with 23% who say the opposite. At the same time, however, well over eight in ten respondents are very or somewhat concerned that such information might be hacked and used to steal their money, or that sharing data might lead to them being targeted by marketers.

Companies' revenues and reputation stand to suffer because of privacy concerns. Sixty-six percent of respondents report sometimes not buying a product or service because of concerns

about the security and privacy of their personal data. Of the 23% of respondents who have suffered a data breach, 46% advised family and friends to be careful when sharing information with the organisation. Moreover, the most active Internet shoppers are also the least forgiving of transgressions. Among those who shop online at least once a week and have experienced a data breach that compromised their personal information, 59% ceased to do business with the organisation in question.

Data security policies are not just about protecting data, but also about building and maintaining customer relationships. Interviewees for this study stress the need to develop trust with customers on data issues, not just for regulatory or ethical reasons, but also because it provides a competitive advantage as it can encourage customers to share more information. A good relationship involves showing respect for customer data. This starts with good practice in areas such as data minimisation. But equally important is regular communication with customers on how their information is being used.

Policies need to recognise cultural differences on privacy issues. The understanding of privacy, and fears of its breach, can vary by country. The EIU survey results indicate, for example, that while Americans and Europeans have similar levels of unease, the former are now less likely to share information than before. Similarly, French respondents are more likely to have suffered a data breach, which may have had an impact on their buying habits. Companies need to understand that what is sufficient in one country might not win trust in another.

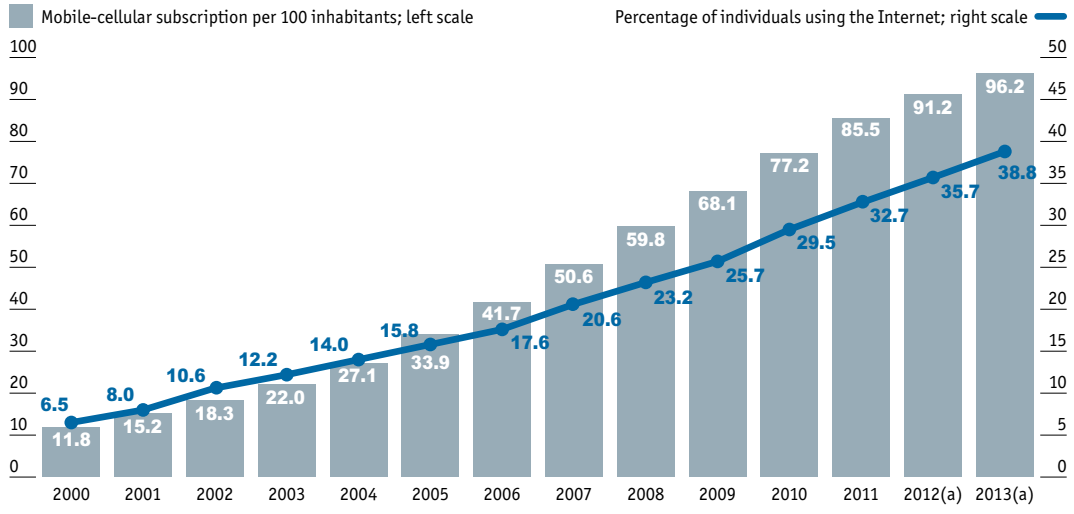
Introduction

Internet and mobile connectivity has increased exponentially over the past decade. While being connected has become more commonplace, individuals have also become more and more comfortable with sharing personal data. In a global survey conducted for this study of over 750 Internet users, 34% say that they are more likely to share basic personal information online now than three years ago, compared with 23% who say the opposite.

These two trends are resulting in staggering volumes of new data. Already, 10bn texts are sent and more than 1bn posts are uploaded online each day, according to the World Economic Forum (WEF). E-commerce volumes tell a similar story: 5% of retail activity in the US and 10% in Britain is now online. By 2016, according to the Boston Consulting Group, online commerce will account for 7% and 23% of total retail activity in the US and the UK respectively.

Chart 1

Ever more connected



(a) Estimate.
Source: International Telecommunication Union.

But with greater sharing comes greater risks. The EIU survey finds a significant minority of respondents have suffered a data breach—an even more common occurrence among frequent online shoppers.

In a digital age where more and more data is created and shared, privacy becomes a concept that is difficult to define and protect. The issue is not only the sheer volume of data available, but also the rapid evolution of tools used to extract information from the data. A recent study of over 58,000 Facebook users by University of Cambridge academics is a case in point. They devised algorithms that in the great majority of cases could accurately predict an individual's sexual orientation, race and political leaning—information that was not explicitly available on the user's profile.

The continued evolution of data-analysis tools has changed the degree to which businesses can understand people. Richard Baker, EMEA chairman at Aimia, a loyalty programme company, explains how it is now possible to get a far more detailed understanding of customers and citizens: "Because you can put so many databases together, you can take the equivalent of a ten-megapixel picture of a customer in real time, when a decade ago you could only do a one-megapixel picture that took a long time to develop."

Individual privacy is therefore being redefined as more and more interactions, commercial or social, become digital. As Richard Allan, European director of policy at Facebook, notes, "if a billion people are sharing information online, it is self-evident that something has shifted. We clearly do have a social norm that most people feel comfortable sharing some data online within certain boundaries." The issue is how to understand and respect those boundaries or, as Joe McNamee, executive director of European Digital Rights—a privacy and civil rights umbrella group for the EU—puts it, to maintain the "established principles of rights over one's own data" in a world where people are "communicating in ways they never did before".

The Atlantic divide: similar worries, different behaviours

Survey respondents from the US and Europe share many common views on privacy. Roughly the same proportion, for example, is very or somewhat concerned about their private data stored online being hacked and used for theft (over 90% in both cases) or for targeted marketing (78% in Europe and 88% in the US). Large majorities in both locations also believe that regulations on the use of consumer data by businesses are not strong enough, and only small minorities—15% in America and 24% in Europe—believe companies are sufficiently transparent about how they use data.

The impact of these similar concerns, however, seems to be different. According to the EIU survey at least, respondents in Europe are much more frequent online shoppers: 22% do so at least once a week compared with just 5% of those in the US.

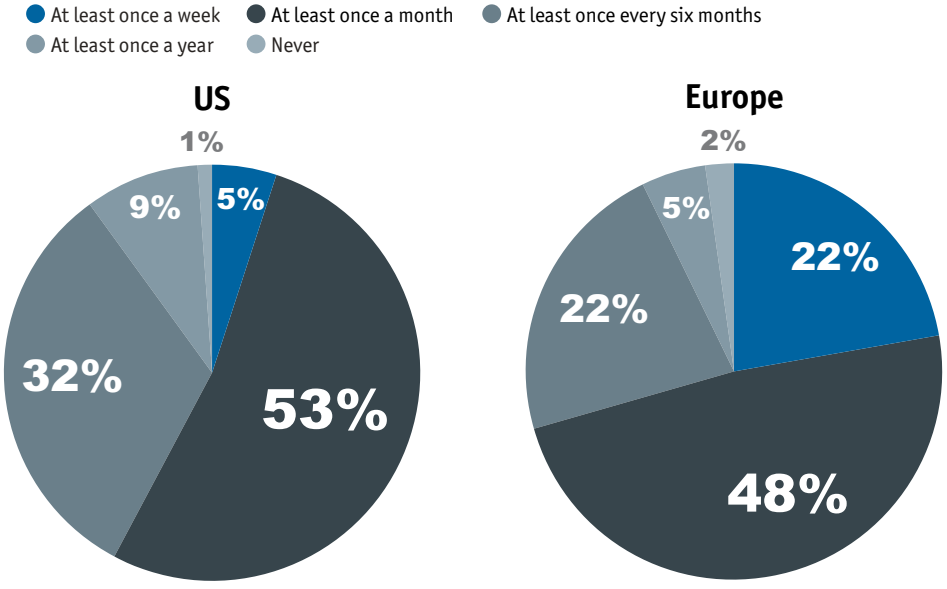
This is the case even though Americans report slightly higher trust levels in the security of data held by online retailers. More strikingly, unlike most of the rest of the world, those surveyed in the US are becoming more reluctant to share basic personal data: 38% say they are less likely to do so than three years ago compared with 14% who are more likely; the comparable figures for Europe—20% and 31%—show the opposite tendency.

Companies need to adjust strategies to take account not only of regulatory differences on use of consumer data across borders, but also of how worries about data safety may have different effects in different national contexts.

Chart 2

How often do you make an online purchase?

(% respondents)



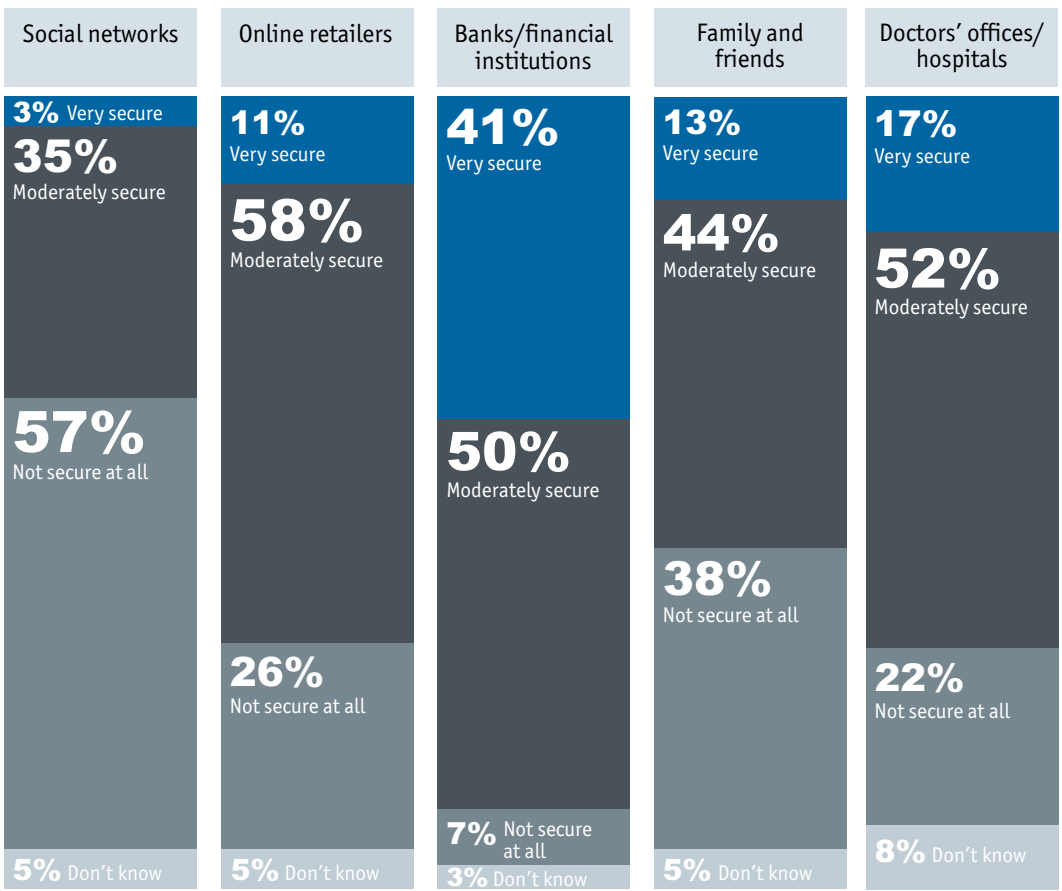
Source: The Economist Intelligence Unit.

1 An air of unease

Although respondents are comfortable sharing basic personal information, the EIU survey finds that they rarely think their data is particularly safe in the hands of others. Only 3% say that their data is very secure with social networks and 11% say the same about online retailers. The mistrust, though, is far wider. Only 13%, for example, say that personal information known to family and friends is very secure.

Chart 3

How secure do you believe your personal information is in the hands of the following?
(% of respondents)

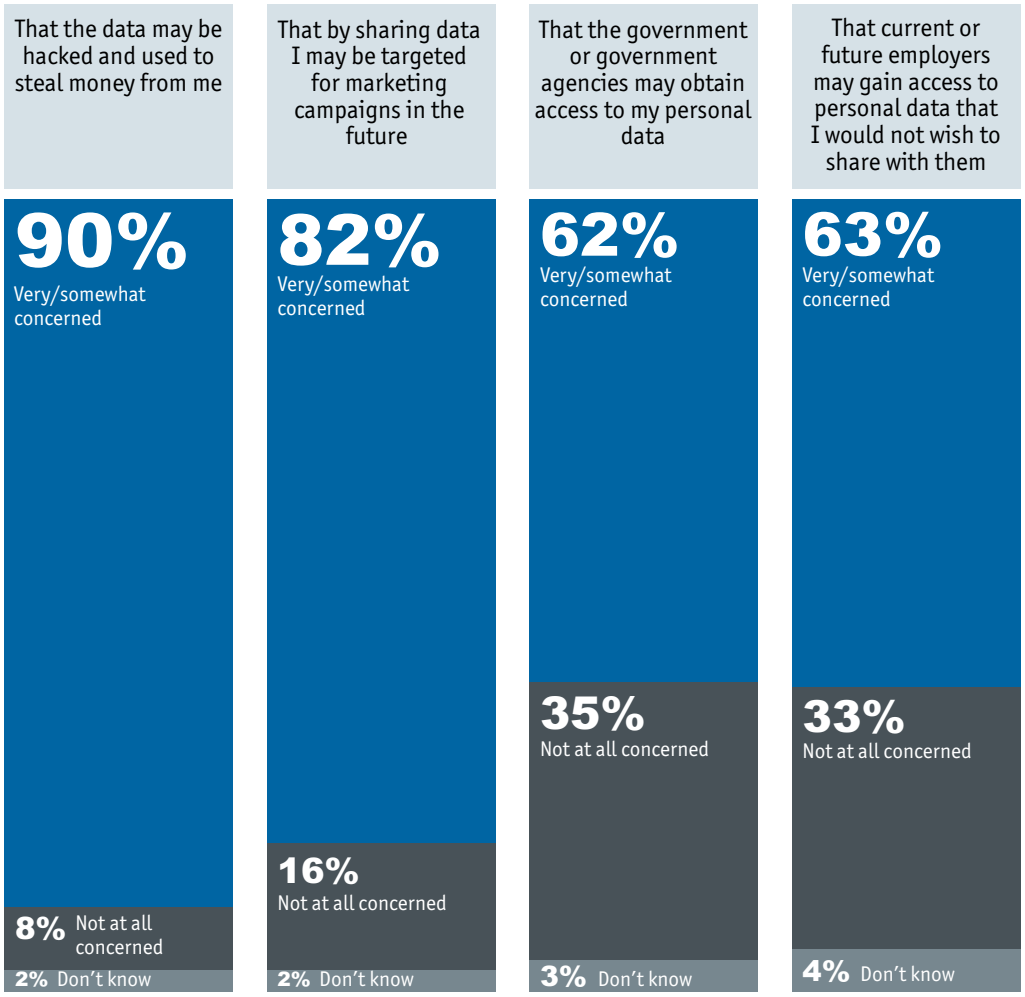


Source: The Economist Intelligence Unit.

Chart 4

To what extent are you concerned about the following risks when sharing personal information online?

(% of respondents)



Source: The Economist Intelligence Unit.

This insecurity about personal data is combined with widespread worry about its potential misuse: 90% of respondents, for example, are very or somewhat concerned that such information might be hacked and used to steal their money, and 82% are concerned that sharing data might lead to them being targeted by marketers. The worry that governments or employers might discover secrets is also widespread. Alex Fowler, global privacy and public policy lead at Mozilla, echoes the EIU findings. "The conclusion we draw from the consumer research that's been conducted over the past decade is that the public is uneasy about all the information collected, used, bought and sold, and lost due to lapses in security or stolen by hackers," he says.

Consumer mistrust appears to be deep-rooted: 70% of respondents believe that businesses do not have a great enough incentive to protect personal data, and only 26% think businesses are transparent enough in how they use such

information. "Many people have a strong reaction when they see their Collusion map for the first time," Mr Fowler says. Collusion is a browser app that creates a real-time map of trackers—the sites that receive information about users depending on the websites they visit. "Often they don't realise that there were so many trackers or that tracking was happening at all," Mr Fowler adds. Michael Harte, chief information officer at the Commonwealth Bank of Australia, sees this issue growing in importance. "Customers increasingly want more control of their data," he says. "They want transparency on where it is, who has it and with whom it will be shared. They want to know what it will be used for."

Consumers also feel unprotected by the authorities: 75% of respondents say that regulation preventing the misuse of personal data is not strong enough. Nellie Kroes, the European commissioner for the Digital Agenda for Europe, is seeking to strengthen legislation in this area, but also recognises that popular concerns are at the very least exacerbated by a lack of knowledge. "It is clear that one of the biggest problems is transparency and complexity," she says. "People may even be protected [legally], but may not know because [the regulations or contracts] are too complex." This is one of the reasons why the proposed General Data Protection Regulation (GDPR) seeks to provide a single law for the EU which would make the rights and protections of citizens clearer.

It does not help that the only form of company communication on transparency and privacy protection—the privacy statement—is notoriously inefficient. A 2008 academic study found that if the average American were to read the privacy statements from all the websites they used during a year, it would take 201 hours—or five work weeks—and would cost the economy $781bn.[1]

Consumers, however, are far from universally negative about sharing data. Despite expressing concerns about the security of data held by social networks, 84% of those surveyed say that they belong to at least one. Similarly, despite the large majority worried about targeted advertising, Mr Baker's experience at Nectar, a loyalty card owned by Aimia, paints a different picture. "At Nectar, our point collectors understand the value exchange in providing their data and are therefore comfortable with receiving targeted adverts," he says. "In fact we are more likely to get complaints if they are not being provided with relevant offers." And Mr Harte adds: "I am sure there are plenty of examples of marketing campaigns that have spooked people, but customers also like it when organisations 'intuit' what they may need. They see this as excellent customer service. The challenge is to keep the balance right." Mr McNamee agrees that consumers are often willing to share information, especially in return for some benefit, but adds that they are only truly comfortable when they understand and approve of the way in which it is being used.

In short, consumers as a whole are uneasy about how their data might be misused, but seem happy, or even want, to have it used in ways they understand and from which they can benefit. How does their attitude impact their behaviour and how can businesses respond?

[1] Aleecia McDonald and Lorrie Cranor, "The Cost of Reading Privacy Policies", *I/S: A Journal of Law and Policy for the Information Society,* 4(2008).

Culture, privacy and trust: an Indian view

Differing attitudes towards privacy worldwide are not the result of happenstance. Instead, they are closely connected to a range of cultural assumptions about what is normal to share and how important it is to guard personal information. Ponnurangam Kumaraguru, professor at the Indraprastha Institute of Information Technology in Delhi, helped lead a recently completed 10,427-person survey in India. He found that despite well-publicised government efforts to improve online privacy protection, the understanding of privacy issues was noticeably lower, and trust in governments and other organisations on such matters higher, than in developed countries. This reflects, Mr Kumaraguru says, the "difference between a collectivist and an individualistic society. The concept of privacy has been widely discussed and understood for a long time in Europe and America, but not much in the culture in India. The concept is unclear and some aspects of privacy awareness are very low."

These differing attitudes have an impact on online behaviour and expectations about online behaviour. Although this makes setting global privacy and data policies more complex for companies, in India it brings some good news as well. Internet users there exhibit a substantial level of public trust around privacy. Even though 77% of Indians in Mr Kumaraguru's study believed that consumers had lost all control over how information about them was used and circulated by companies, 59% still agreed that most businesses use such data in a proper and confidential way, against just 14% who disagreed.

Culture, however, is not immutable. When comparing the latest survey with a similar one conducted in 2005, Mr Kumaraguru sees "India becoming more privacy aware and concerned". The two surveys already indicate a noticeable increase in distrust of government in this area. Mr Kumaraguru believes that trust in businesses could also drop, especially if highly publicised data breaches occur.

2 The business implications

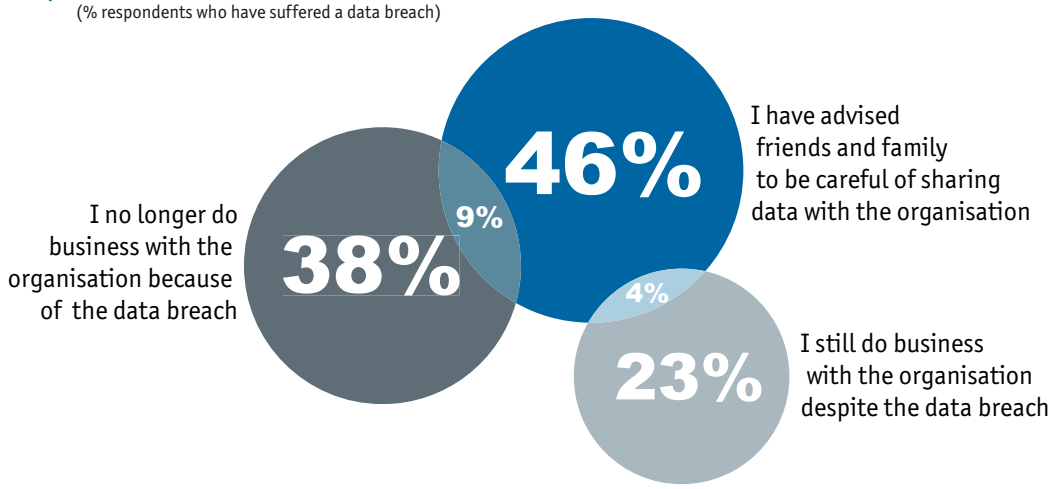
This air of uncertainty among consumers could dampen business activity. Two-thirds of respondents sometimes opt not to buy a product or service because of concerns about the security and privacy of their personal data. And of those in the survey who have experienced a data breach (23% of respondents), 38% no longer do business with the organisation involved and 46% advise friends and family to be careful sharing data with it.

More broadly, the survey suggests a correlation between the level of trust in how data is protected and willingness to engage in online commerce. The most frequent Internet shoppers are more likely to agree that businesses are sufficiently transparent in how they use data—37% compared with 23% for less-frequent shoppers. They are also the only group where the respondents who believe businesses are transparent enough outnumber those taking the opposite view.

These shoppers maintain these views even though they are more likely to have suffered a data breach in the past two years (37% compared with 23% on average). They are also, however, harsher in their reactions: 59% of frequent shoppers hit by a breach have ceased to do business with the organisation in question and only 10% have continued to do so. Rather than putting these high-volume shoppers off online commerce as a whole, such incidents seem to shake trust in individual sites.

Chart 5

Q **Which of the following statements describes the consequences of your data breach?**
Select all that apply
(% respondents who have suffered a data breach)



Note. Overlap percentages represent respondents that ticked both statements.
Source: The Economist Intelligence Unit.

The importance of being trustworthy

"There is a risk of people sharing incorrect or less data than they would have done as a result of a lack of trust," Mr McNamee notes. "That is not helping the amount or quality of the data. Businesses and citizens end up no better off." More broadly, Ms Kroes adds that it is "not a sustainable business approach to trick users into giving data away". Instead, she says, companies need to earn trust.

Corporate and technology leaders interviewed for this study are in complete agreement with Ms Kroes. "We all have to continue our efforts—both big and small—to create a more trustworthy environment of online products that seamlessly integrates ease of use, transparency and user choice," says Mr Fowler. In an atmosphere of consumer unease, maintaining trust is critical. Mr Baker says: "Nectar's business model depends on customers being willing for us to manage data that is attributable to them. We would fail if we violated basic common sense about what is reasonable to do."

This goes beyond ethical behaviour; it makes excellent business sense too. "There is definitely a competitive advantage in having the trust of your customers," Mr Harte says. Risk reduction is an important element of this. Mr Baker notes that "well-run companies understand that if they misuse or lose data in an unprofessional manner, there is a serious downside risk". Similarly, Mr Harte notes that "customer trust is incredibly fragile and once lost, can be hard to regain".

The bigger advantage in the long term, however, is on the profit side. "If our customers trust us to be the guardians of their data, they will in turn give us more to look after," Mr Harte adds. "This will enable us, with their permission, to deliver more value to them by offering them better analytics and insight and, on the back of this, more innovative and tailored products." Trust on data, especially where it is a competitive differentiator, is at the core of mutually beneficial relationships.

First steps

Although the details of how best to build trust can vary by industry and geography, our interviewees point to several universal steps. It is essential to build into business and data storage processes elements such as data minimisation (collecting and retaining only what is needed), the right to be forgotten (deleting what is no longer required), consumer rights to access and, where incorrect, to rectify their information, and portability (the ability to move data around). Crucially, Mr Baker explains that while clear rules and regulations are important, in a fast-changing world value-based guidelines are also essential. "Every day people come up with new ideas on how to use data," he says. "The most important thing is to educate our employees as to the right and wrong of what to do."

Such an attitude will also help to insure that companies value the data they receive. Mr McNamee explains that "because it has been so easy [to collect], businesses can think data is free and that the data subject can be ignored. Citizens, though, will ask if they are getting an appropriate deal if they are paying with their data." Mr Harte agrees. "Customers must believe they are getting some value from the relationship," he says, which he believes means focussing on how to use customer information to create value for them without abusing their trust.

However, the most important starting point, according to many interviewees, is to recognise the need for enhanced interaction, in particular, going beyond ineffective one-off online privacy statements. As Mr Allan explains, because of private statements' ubiquity and length, "companies are technically being transparent, but the cost of reading the information [in terms of time] is too high for individuals". Mr Harte also says that businesses should consider moving towards better and more comprehensible initial statements, and "continuous disclosure, which is about maintaining a dialogue with customers to seek their permission whenever their data is about to be put to a new use". Trust comes

from a relationship and relationships require communication, not one-off statements.

Ahead of the curve

Improved transparency also better prepares companies for the regulatory changes that will accompany the evolution of technology. The most prominent, and controversial, at the moment is the EU's proposed GDPR. Many oppose its implementation, including Silicon Valley technology companies, as it would significantly strengthen consumer protection against tracking and targeted advertising. Companies failing to comply could face fines of up to 2% of their global annual revenues. The core debates surrounding this legislation—in particular on what constitutes personal data in an age where individual snippets can be aggregated into a highly revealing picture—reflect the difficulty in constructing regulation that addresses both current technology and its unpredictable evolution. This leads to, in Ms Kroes' words, a "complex, situational approach" as the price of greater clarity may be complexity.

The final shape of the regulation remains unclear, and corporations, just like consumers and regulators, are wise to fight for their own interests as the process continues. Nevertheless, companies should not lose sight of the bigger picture. In an atmosphere of widespread concern, tighter regulation can help provide reassurance. Moreover, as Mr Harte explains, legal compliance is just the ticket to play. Real competitive advantage comes not only from meeting regulatory obligations, but also from being recognised by customers as fully meeting their expectations regarding their privacy concerns and their relationship with the company. Mr Baker adds that "new rules will have to be created for a new world". The form they will take is hard to predict. Well-run businesses are anticipating these changes in how they behave.

France, the UK and China: insecurity and its varying costs

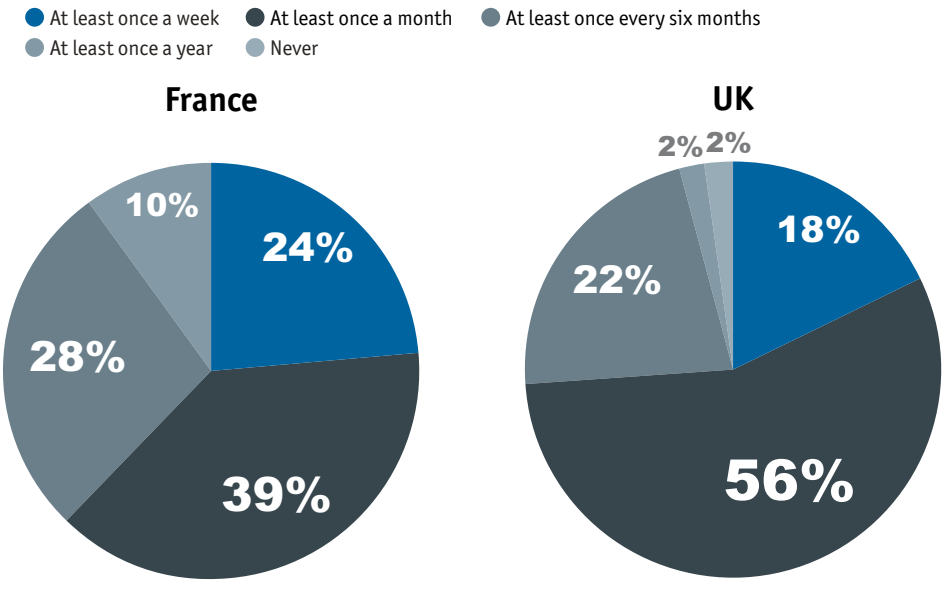
Despite geographic proximity, French and British respondents have had different experiences of information security. Nearly one-quarter (24%) of the former report suffering a data breach in the past two years, involving the loss or theft of personal data, compared with just 10% of those in the UK. This probably accounts for why French respondents show less confidence in the security of their data in the hands of every type of holder covered in the survey. It may also explain why they shop online slightly less frequently overall than their British counterparts, and why they are so much less likely to share personal data online than three years ago compared with respondents in the UK and the rest of Europe.

A look at China, however, shows that the impact of insecurity is far from straightforward. An alarming 58% of Chinese respondents have experienced a data breach in the past two years. Nevertheless, they have become more open: 58% of Chinese respondents say that they are more willing to share basic personal information now than three years ago, compared with only 12% who are less so. This may arise from a lack of consumer choice as Chinese retail markets tend to be under-served, especially in tier three and tier four cities which are seeing faster Internet sales growth than their larger counterparts. Underlying attitudes to what is acceptable may also be an issue. Chinese respondents have slightly lower levels of concern than French ones about hackers and companies misusing their personal information, even though the Chinese have much more experience of data breaches. Similarly, 46% of Chinese respondents agree that companies are transparent enough in their use of customers' personal data, compared with just 14% of French respondents.

Chart 6

Q **How often do you make an online purchase?**

(% respondents by country of origin)



Source: The Economist Intelligence Unit.

The Facebook experience

Facebook, the social networking site, is no stranger to privacy-related controversies. Most recently, a string of concerns has led to major revisions of the site's privacy policies and the enhancement of user control over privacy settings.

The biggest issue for the company has been understanding consumer demands. Richard Allan, the company's European policy director, notes that the vast majority of data put on Facebook by users is supposed to be shared with other individuals. Here, he adds, privacy questions revolve around "whether that service is behaving in the way you anticipated". Because the medium of the social network is still relatively young, however, meeting these expectations—or even understanding what they are—is still a matter of network companies and customers learning what the latter want.

This has not always been a smooth process. Mark Zuckerberg, chief executive officer of Facebook, has more than once publicly admitted to making mistakes relating to privacy, but the end result seems to have been successful. A recent academic study found that changes to privacy settings and policies led to an increase in the willingness of users to share certain data on the site.[2]

Facebook's experience holds a number of lessons for companies dealing with online customer data. "The critical issue is not to surprise the people using your service," Mr Allan says. "When designing updates, think hard about whether you are going to cause surprises and a backlash. We have launched hundreds of updates—most have met these criteria but a few have failed."

Another important element of avoiding surprises is finding more meaningful ways to communicate with users. Privacy statements and terms of service remain important, says Mr Allan, but these often go unread. Accordingly, Facebook has adopted a policy of using dialogue-box warnings to explain to members using certain features for the first time exactly who will be able to see any information transmitted.

The most important change Facebook has made, says Mr Allan, is incorporating privacy by design into new features. "Social networks are designed for sharing, but this approach [privacy by design] means that when we create a feature we ask, 'Will the privacy settings work in the way people anticipate?'" This, he believes, rather than guaranteeing complete privacy, is the proper role for the provider of a social network. "If you share a photo with 150 people, absolute security is unlikely" he says. "Our job is to make sure it is shared only with the people you want to share it with. It is for the individual then to consider, 'If I am sharing with all my friends what are the implications of that?'"

[2] Fred Stutzman et al., "Silent Listeners: The Evolution of Privacy and Disclosure on Facebook", *Journal of Privacy and Confidentiality*, 4(2012).

Conclusion

The amount of data, including personalised information, in the world is continuing to grow exponentially and improved technology is making it ever easier to draw from it increasingly detailed pictures of individuals. This is causing unease among consumers about how their information will be used and by whom.

If a company is unable to engender confidence—or has lost trust through negligence—its business inevitably suffers. On the other hand, consumers also reward firms that use data about them to provide personalised services in a way with which they feel comfortable. Companies therefore need to treat customer data as a building block in their relationships with consumers rather than as a purely low-cost asset. This is not just an exercise in ethical behaviour, but also a propeller of competitiveness. To this end, several steps can be taken.

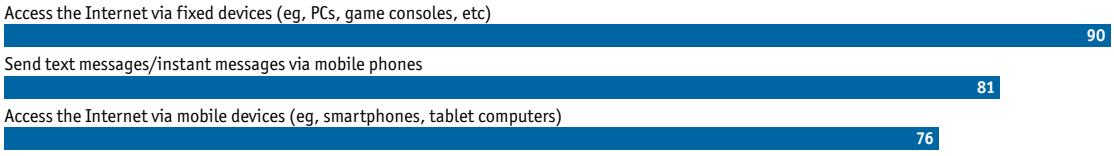
- *Legislative compliance and strong security are essential, but are only the beginning:* Obeying the law on data provides a ticket to play and in the long term customers simply will not maintain ties with businesses that are constantly leaky with their data or that misuse it. As almost every firm will, or should, be covering the basics, though, this will not be a differentiating factor.
- *Treat customers with respect in the use and storage of their data*: Data minimisation, customers' access to their data, the right to be forgotten and to rectify errors, and other elements of best practice not only improve the relevance and accuracy of the information companies hold on customers, but are also testimony to a company's trustworthiness.
- *Educate employees on how to treat consumer data*: As the tools for data analysis continue to evolve in unforeseen ways, employees at all levels must be clear about the limitations in the uses of consumer data. This will help companies to build relationships with consumers and avoid reputation-damaging data-breach scandals.
- *Pay fairly*: If consumer data is such an economically important asset, it should be fairly priced. Compensation need not be monetary, but may involve a free or enhanced service, or even superior customer service. Skimping on this in a data-driven economy could mean losing your competitive edge to rivals.
- *Communicate properly on privacy*: Website privacy statements are frequently a legal requirement and can help to answer the questions of interested individuals, but as a communication tool with the vast majority they are nearly worthless. Because customers are wary about privacy, finding ways to communicate relevant elements of privacy policies effectively will be a key element in building trust and relationships.

Appendix : Survey results

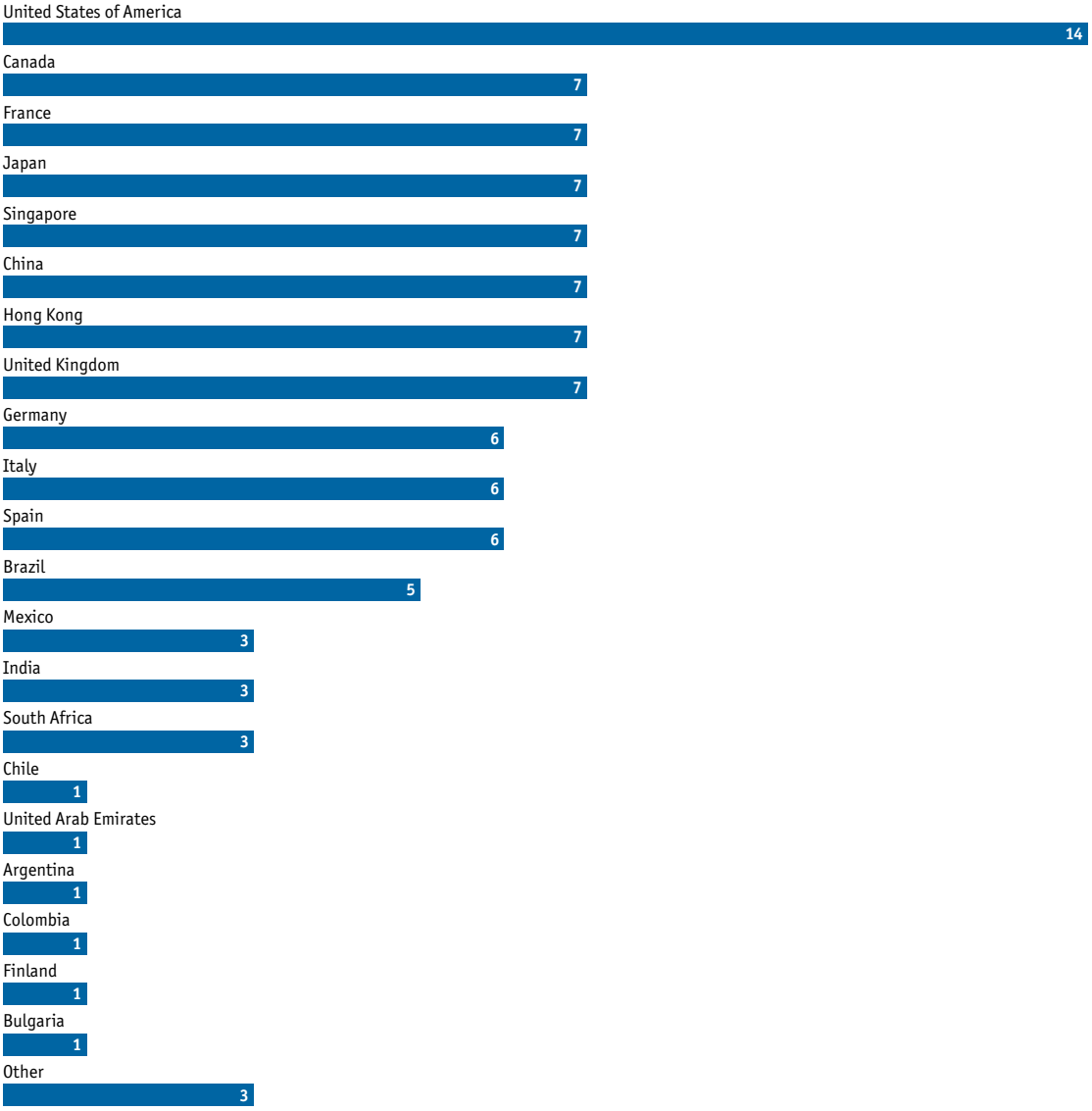
The EIU conducted a global survey of 758 adult Internet users in January and February 2013. Our sincere thanks go to all those who took part in the survey.

Please note that not all answers add up to 100%, either owing to rounding up or because respondents were able to provide multiple answers to some questions.

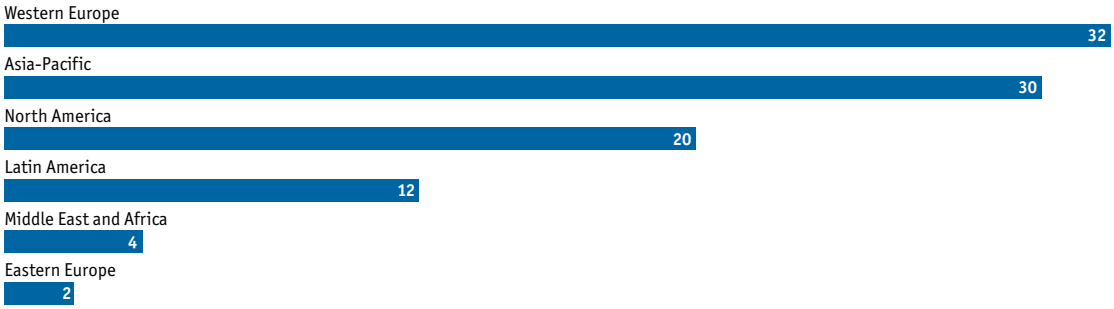
Do you do any of the following? Please select all that apply.
(% respondents)



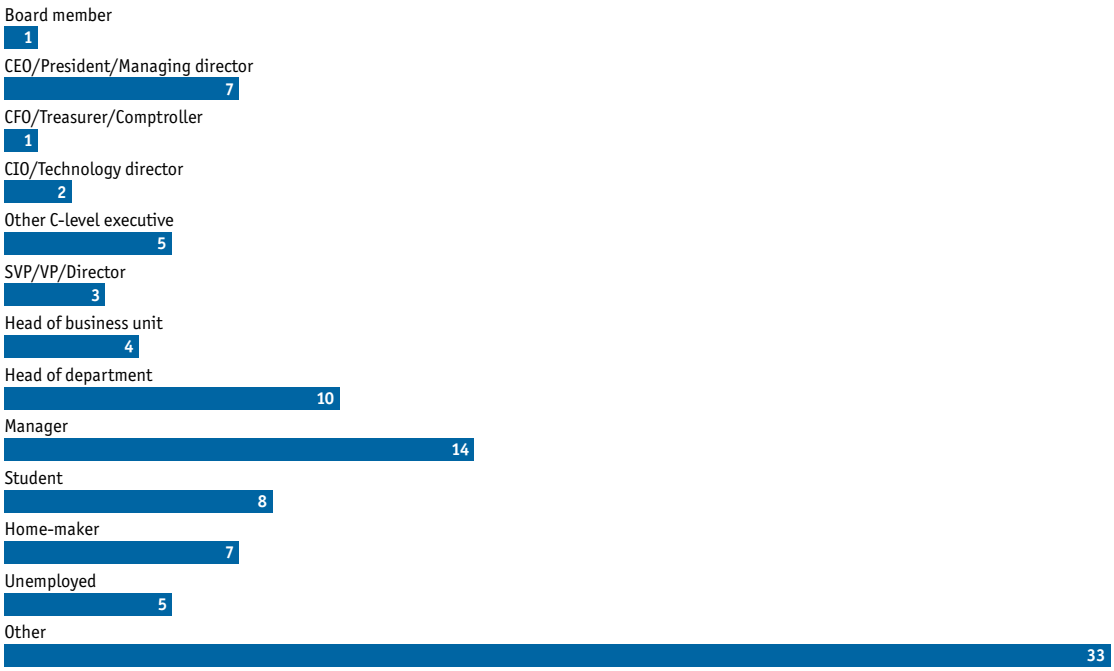
In which country/region are you personally based?
(% respondents)



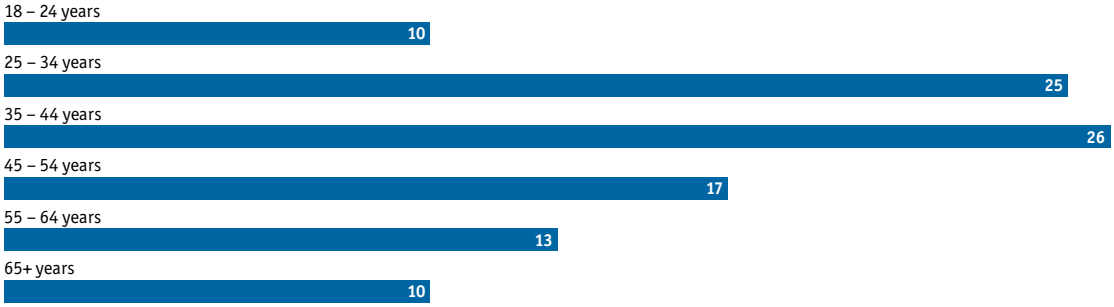
In which region are you personally located?
(% respondents)



What is your job?
(% respondents)



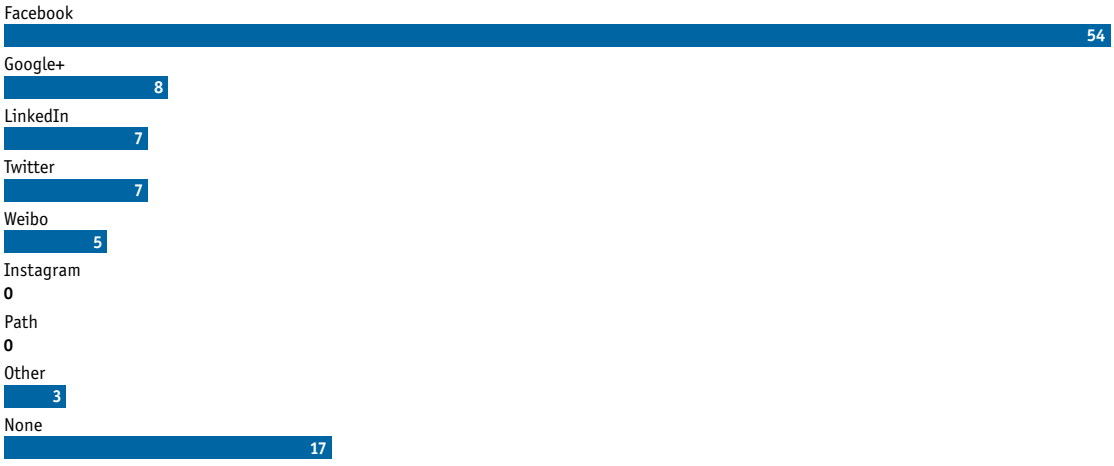
How old are you?
(% respondents)



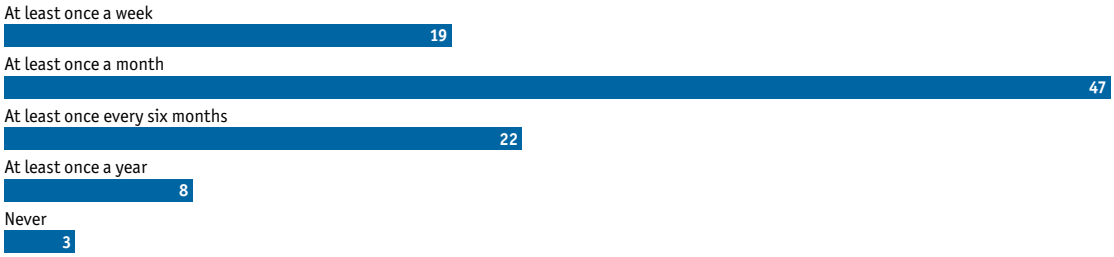
Are you male or female?
(% respondents)

How often do you use the Internet, using either fixed or mobile devices?
(% respondents)

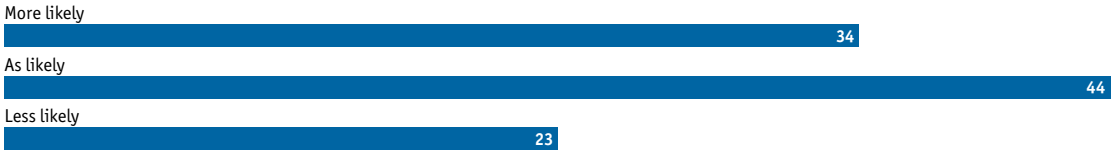
Which of the following social networking sites do you use the most?
(% respondents)



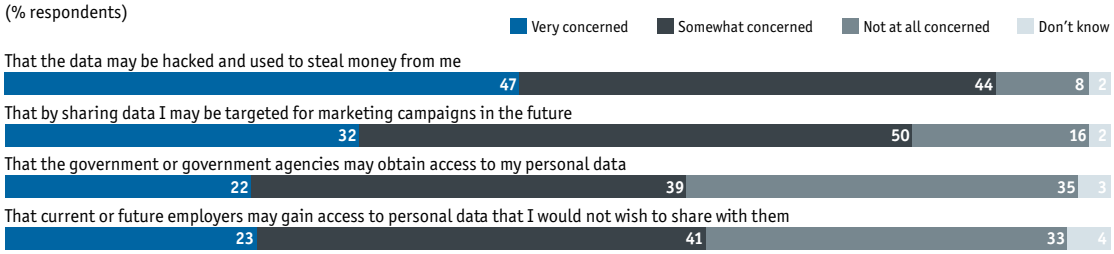
How often do you make an online purchase?
(% respondents)



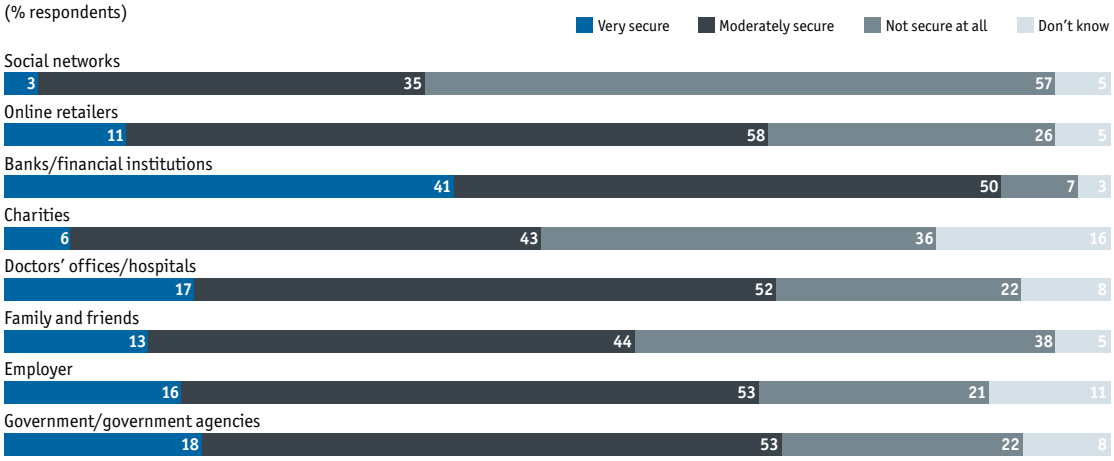
Are you more or less likely than three years ago to share basic personal data online (eg, date of birth, home address, employment status)?
(% respondents)



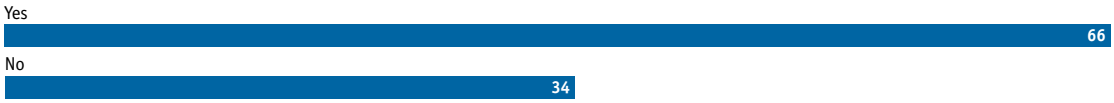
To what extent are you concerned about the following risks when sharing personal information online?
(% respondents)



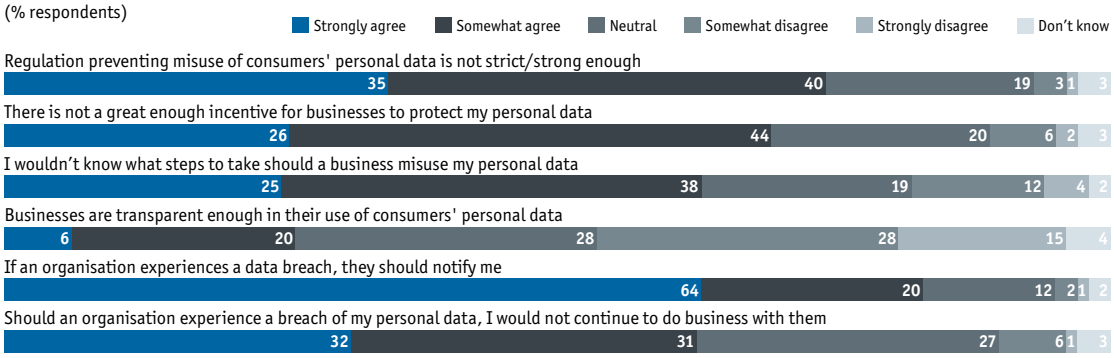
How secure do you believe your personal information is in the hands of the following?
(% respondents)



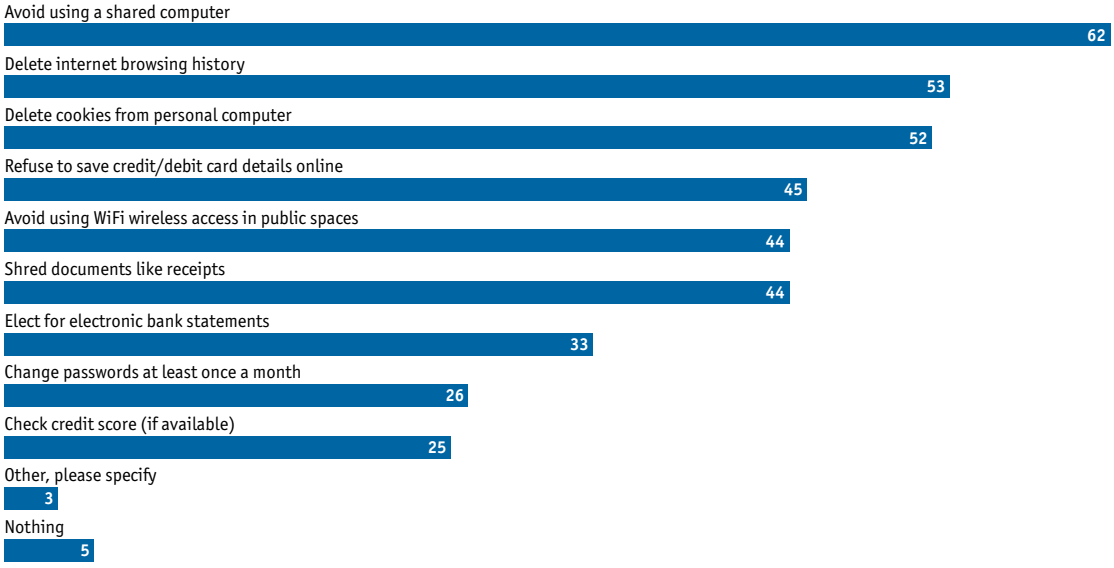
Do you ever opt not to buy from a product or service provider out of concerns for the security and privacy of your personal data?
(% respondents)



Do you agree or disagree with the following statements?
(% respondents)



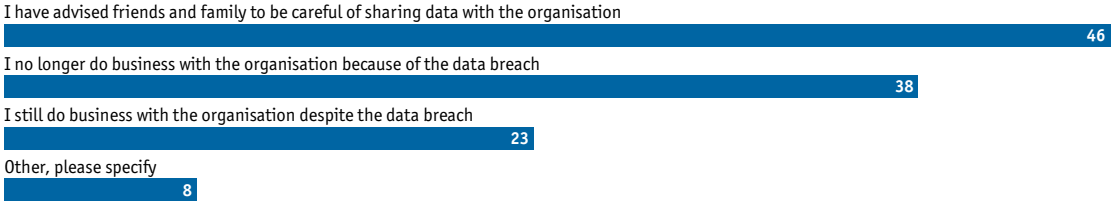
Which of the following do you use to safeguard your privacy? Select all that apply.
(% respondents)



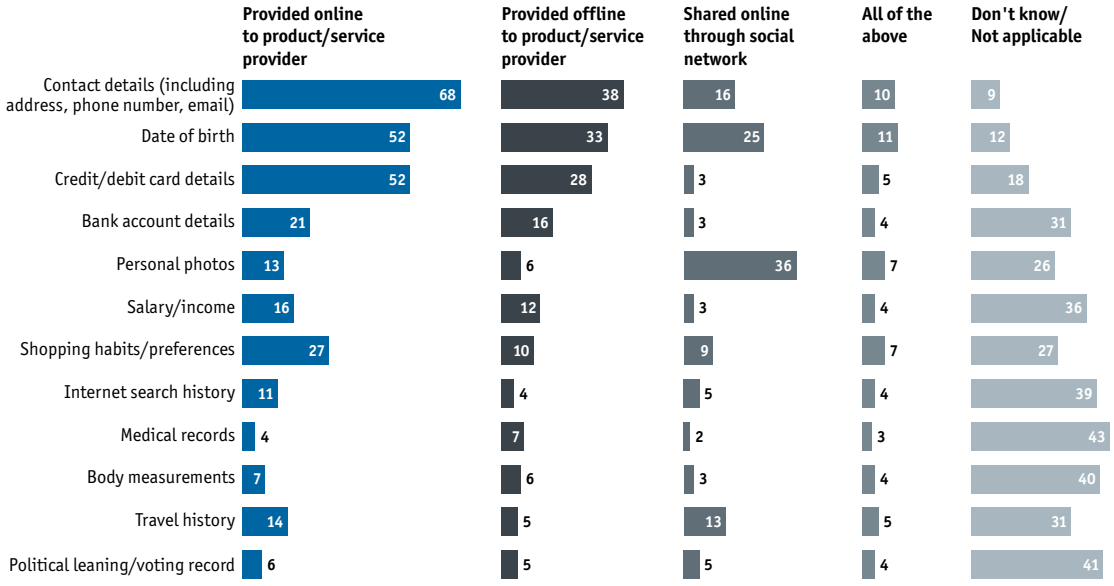
Do you believe that personal information held in the "cloud" is more secure or less secure than information held on the local systems of service providers?
(% respondents)

Has your privacy been breached in the last two years, involving the loss or theft of your personal data?
(% respondents)

Which of the following statements best describes the consequences of your data breach? Select all that apply.
(% respondents who have suffered a data breach)



Which of the following categories of information have you knowingly supplied to a product or service provider, online or offline, or shared with a social network over the past year. Select all that apply.
(% respondents)



LONDON
20 Cabot Square
London
E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8500
E-mail: london@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
E-mail: newyork@eiu.com

HONG KONG
6001, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: hongkong@eiu.com

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