SURVEY REPORT

Consumer Trust, Consent and Knowledge in the Age of Digital Identity

Executive summary

- The survey results show that companies should ensure their online interactions with customers are aligned around three key principles: **trust, consent,** and **education.**
- Overall, consumers' knowledge about what they share about themselves online, and who is capturing this information, is low. Around half of adults surveyed (47%) don't feel they know how much information about themselves is available online. Similarly, almost three in five (57%) know "only a little" or "nothing at all" about their rights regarding the use of their personal data. This lack of awareness around data-sharing is significant as those with higher levels of knowledge about their rights are also more likely to be happy with the level of personal information they share with organizations online.
- Some consumers are troubled by what they know they have shared online. About half (53%) worry about how much personal information they have shared online, and a similar proportion (51%) are uncomfortable with the amount of information social media platforms have about them.
- Consumers show high levels of **trust** towards organizations whose contact with customers is formed around a 'transactional' relationship, with a majority saying that they trust banks and credit card companies (79%), utility companies (78%), payment apps (78%), insurance and / or pension providers (77%) and even tech-giant Amazon (74%) to manage their data responsibly.
- **Consent** emerges as a second key principle for building transparent, trusted data-sharing relationships. Those who share personal data with Amazon are most likely to feel in control of what is stored (62%), in line with the level of control consumers perceive themselves to have over the data which is stored by banks and credit card companies (61%), the health service (60%), utility companies (60%) and payment apps (60%).
- Finally, a third element of this relationship is consumers' own **knowledge** of their rights regarding the use of personal data which they have shared online. Those who know at least "a fair amount" about their rights are consistently more likely to say that they feel in control of the personal data they have shared with companies than those who know "only a little" or "nothing at all". Similarly, those with higher levels of knowledge about their rights would be more likely to sell or share their personal information online in return for discounts and personalization.
- Unsurprisingly, with knowledge around online data-sharing relatively low, consumers are more likely to believe that the organizations collecting this data are the main or sole beneficiaries of this (41%) rather than the consumers themselves (17%). In this context, consumers largely think that the organizations that collect and store their personal data should be responsible for its protection. Over half (57%) of adults think that it is mainly or only the company's responsibility to protect the data they have shared with them, while only 9% think that it is their own responsibility.
- Further to this, sharing personal data with a third-party without the consumers' consent is likely to have serious implications for businesses who rely on the sharing of personal data: if this was to happen, respondents are most likely to stop using the company (56%), to remove / delete all the data held on them by that company (49%), and to advise their family and friends against using the organization (46%).

Introduction

Defining 'Digital Identity'…

A person's online presence, the sum of all digitally available data about an individual[1].

'Digital identity', the information that represents an individual, organization or device online, is a concept that has become increasingly complex in recent years. Not only has the number of connected services and devices proliferated, but organizations use technology to capture personal data from consumers during online interactions to target certain groups, personalize their service, and inform their future strategy. Entire markets have been built on the data individuals share with organizations online.

This year, the debate about personal data and its protection is reaching a new peak. In 2018, substantial regulations will come into effect in Europe that will set higher standards and affect businesses and consumers globally. It is particularly important for businesses to understand consumers' perceptions of their digital identity, in order to build strong, positive data-sharing relationships that enhance their ability to profile their customers and maximise the value of their service.

Therefore, the purpose of this survey was to understand consumer awareness of their digital identity, their knowledge of how the information that they share about themselves is used online, their rights regarding that data and their perceptions of the online platforms that collect it. In total, 8,434 adults were surveyed across France, Germany, the US and the UK, with a minimum of 2,000 individuals from each country.

The findings suggest that companies should look to re-align their online interactions with customers with three key principles in mind: **trust, consent,** and **education**. This will help to ensure that consumers see interactions as mutually beneficial, and will help to build confidence and trust in online interactions.

Low awareness: a primary barrier to improved data-sharing relationships

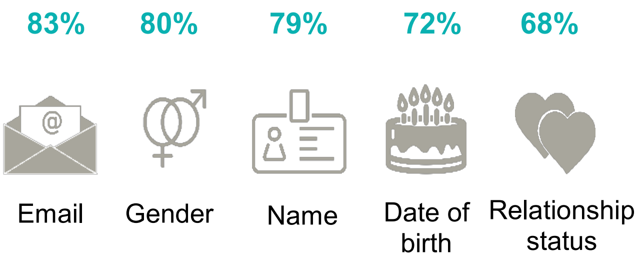
Knowledge and perceptions of transparency are closely linked. The survey finds that over half (53%) of consumers are concerned about how much information they share online, and that this concern may be driven by consumers' lack of awareness of what they share about themselves, and who is capturing this information.

Around half of adults surveyed across all four countries (47%) don't feel they know how much information about themselves is available online. A large majority say they have shared basic pieces of information such as their email (83%), gender (80%), name (79%) or date of birth (72%).

However, when it comes to more personal information, the data shows a perception gap between what consumers believe they have shared online and the personal information their claimed online behaviors suggest may actually be available online. For example, 76% of adults surveyed say that they use the internet to access products and services and make purchases yet only 31% say that they have shared their debit / credit card details online.

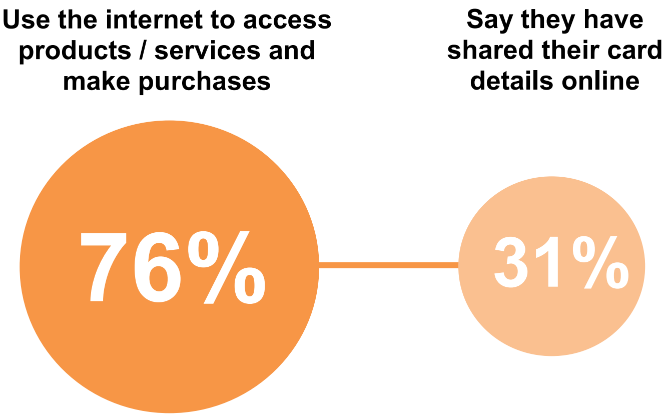
Chart 1: Types of personal information shared online

Showing % who have shared each information online – top 5



D2. To the best of your knowledge, which of the following types of personal information, if any, have you ever shared online? Base: All respondents (n=8434)

Chart 2: Online behaviour compared to information shared online



D2. To the best of your knowledge, which of the following types of personal information, if any, have you ever shared online?; Q1. For which of the following reasons, if any, do you tend to use the internet, either personally or in a professional capacity? Base: All respondents (n=8434)

Similarly, despite around 93% of consumers saying that they use at least one social media platform, between a fifth (20%) and two in five (38%) think that each social media platform tested has no access to any personal data about their users (although it is important to note that users of each platform were more likely to be aware that these have access to their personal data). Differences in awareness are particularly stark at a country level, with German adults being much more likely to think that each platform has no access to personal data about their users.

Social media platforms tested

- Facebook
- Twitter
- Instagram
- LinkedIn
- Xing*
- YouTube

**Only in Germany*

Consumer attitudes towards social media in detail

- Half of consumers (48%) think that Facebook holds information on whether or not users have children
- Just 21% of consumers think Twitter has access to data on users' political affiliations
- A third (32%) of consumers believe that Instagram has access to location data on its users
- 20% of consumers do not believe that Facebook has access to any personal data about its users.

In line with their level of awareness of what they share online, consumers' knowledge of their rights regarding the use and protection of their personal data is limited. Almost three in five (57%) know "only a little" or "nothing at all" about their rights regarding the use of their personal data, while only three in ten (30%) European respondents say they know anything about how the General Data Protection Regulation (GDPR), due to come into effect in May 2018, will affect their rights. Half (48%) do not know who is liable should their data be hacked, even amongst those who have been hacked in the past (49%).

This lack of awareness around data-sharing is significant, as those with higher levels of knowledge about these rights are also more likely to be happy with the level of personal information they share with each organization online. Thus, consumers' low awareness should not be taken as a sign of a lack of engagement with this topic; rather, it should be understood by organizations as one of the primary barriers to improving data-sharing relationships, and moreover a key focus in the drive to improve consumer attitudes towards sharing personal information online.

Nick Caley, Vice President, Financial Services and Regulatory at ForgeRock, commented:

> *"Given the rate at which the data collection techniques that businesses use have evolved, and the lack of effective tools for consumers to control and manage their data, it is not surprising that nearly half of consumers are unaware of what information about themselves is available online.*

> *With so many active services gathering personal data, there is a limit to the extent to which consumers can be expected to take responsibility for controlling their data. If they want to build consumer trust, organizations need to take these findings onboard and adopt a new philosophy around consumer data, one that involves the customer in their own data and empowers them to control it via consent.”*

Consumers are concerned with data sharing

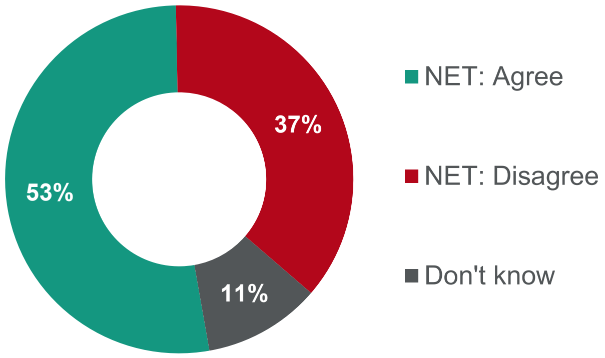
While the data shows that there are gaps in what consumers believe they have shared versus what they have actually shared, the research also suggests that consumers are troubled by what they have shared online.

About half (53%) worry about how much personal information they have shared online, and a similar proportion (51%) are uncomfortable with the amount of information social media platforms have about them. At the same time, a third of parents (30%) are worried about how much information they have shared online about their children. There are clear differences between countries in their attitudes towards data sharing, with Americans being most likely to worry (63%) about the personal data they have shared online – despite the fact that, of the four countries surveyed, they are most likely to engage with online data sharing.

Nick Caley commented:

> *“The fact that Americans are most concerned about the potential exposure of the data they’ve shared online suggests that there is a lack of confidence that major corporations and government institutions will protect the customer data they collect. Many more Americans, compared with Europeans, have experienced some form of data or identity theft and this suggests there has been a greater erosion of trust as a result.”*

Chart 3: ‘I worry about how much personal information I have shared online’
Showing % who agree or disagree



Q20. Thinking about how much you know about how to manage the personal information you share online, to what extent do you agree or disagree with each of the following statements? Base: All respondents (n=8,434)

Interestingly, while Germans are the least concerned about the amount of information they have shared online (43%), more of them are uncomfortable about the information that social media platforms have about them (56%). The reverse is true about the UK and the USA. This points to the differences in expectations and public awareness around data protection in Germany, where it has been a high-profile topic.

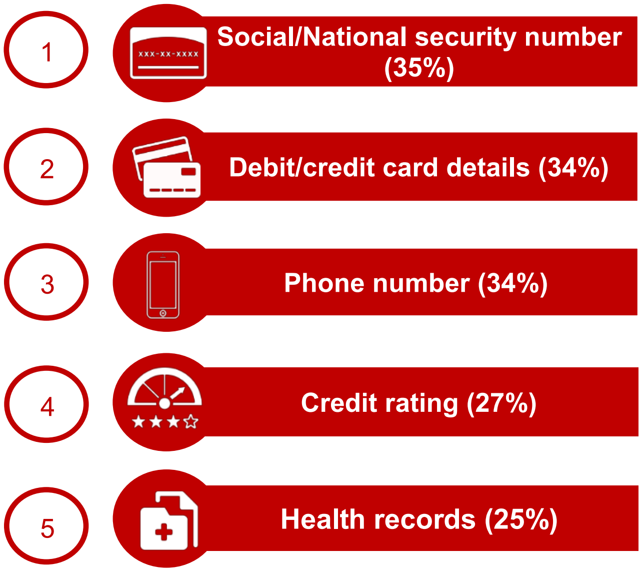
Overall, at least two in five (43%-69%) consumers would prefer to share less information about themselves with organizations online. Consumers are most likely to want to share *less* of their personal data with social media platforms (64%), travel apps (64%), dating apps (63%), online retailers (62%) and news outlets (62%). That some consumers want to share less information with online platforms highlights a distrust over how companies will use their data. Between a sixth (15%) and a third (33%) of consumers would prefer to share less information with companies even if it impacted the service they were offered; this willingness to forgo the standard of the service that companies offer is a clear indication that consumers do not see themselves as the main beneficiary of online data-sharing.

Nick Caley:

"These findings suggest that consumers have become resigned to the fact that their data is being used and misused in ways they don't understand but, given a choice, the majority would prefer to share less. There is sufficient fear, uncertainty and doubt in the relationship between consumers and companies that customers would be willing to tolerate a negative impact to the services provided if could minimise the data they share. There is an opportunity for businesses to build trust and brand loyalty by delivering greater visibility and control of the data being managed, used, processed and shared."

Chart 4: Regret over sharing different types of personal information online – top 5

Percentage who say they wish they had not shared each type of information online



Q4. You said that you have previously shared the following types of personal information online. Which of these do you wish you had not shared online? Base: All who have shared this type of personal information online (n=variable)

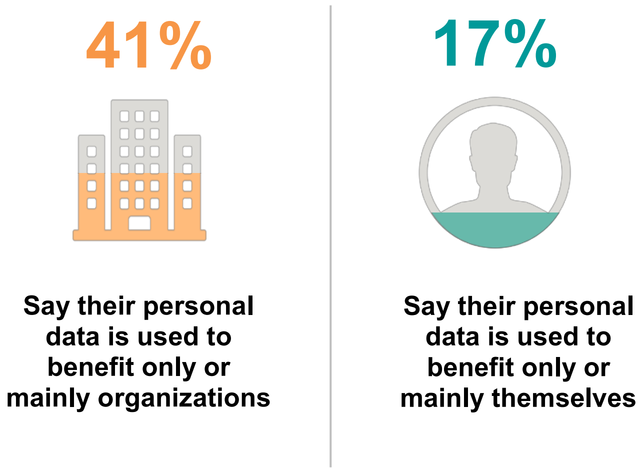
Of course, consumers' sensitivity towards the sharing of personal data varies across different types of personal information. For example, while nearly all consumers who have shared information about their gender (94%) do not regret sharing this online, they are most likely to regret data which could be most damaging if misused or stolen such as financial information, as shown by chart 4. While consumers' willingness to give up the most sensitive pieces of personal information is unlikely to shift considerably, reassuring customers about online data-sharing could help businesses to get closer to their customers.

Levels of trust and willingness to share vary across platforms

Despite relatively low awareness among consumers around the data they share online, the survey shows that they have clear perceptions of who benefits from this data-sharing relationship, and which online platforms can be trusted with their information.

In the minds of consumers, the benefits of sharing personal data online are clearly weighted in favour of the organizations who collect this data. While three in ten (29%) say that both themselves and organizations benefit equally, more than twice as many consumers believe that their personal data mainly or exclusively benefits the organization (41%) as opposed to themselves (17%).Most respondents say that they would be unlikely to sell personal data (79%), share it in exchange for discounts (64%), or share it so they could be offered a more personalized service (60%).

Chart 5: Perceived beneficiary of personal information shared online



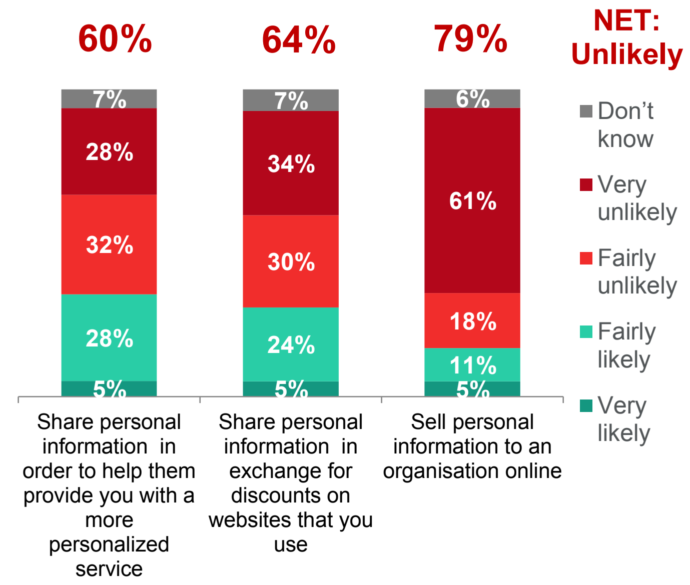
Q13a. Which of the following statements do you think best describes who you think benefits from the personal information which you share online? Base: All respondents (n=8,434)

Nevertheless, discounts and personalization do still incentivize consumers to share personal data, indicating that consumers do recognize the benefits of a data-sharing relationship. Similarly, although half (51%) would never be happy for their data to be shared with a third party, a significant minority would be happy for their personal data to be shared with a third party so they can be kept up to date with relevant discounts and offers (20%) or to improve the service offered to them by companies (17%).

The survey suggests that trust in brands and organizations is critical to consumer attitudes towards sharing personal data. Consumers show high levels of trust towards organizations whose contact with customers is formed around a 'transactional' relationship. This is arguably linked to the tangible benefits of data sharing which certain platforms can offer to their users, with consumers more likely to be willing to share personal information in return for specific benefits, rather than simply selling their information online.

Chart 6: Willingness to sell or share personal information to organizations online

Showing % who say they are likely or unlikely to do each of the following



Q12. How likely, if at all, would you be to do each of the following? Base: All respondents (n=8,434)

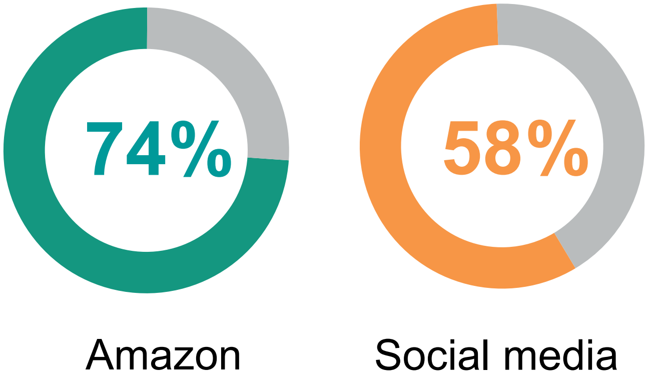
Eve Maler, Vice President of Innovation & Emerging Technology in ForgeRock's Office of the CTO, commented:

> *"Our research shows that people do now understand that 'If you're not the customer, then you're the product'. With Amazon for example, consumers purchase goods or services for money, so they are a defined customer. Social media companies offer them experiences without any financial payment– instead consumers pay in data. If companies were more transparent about how their business models rely on purchases, attention or data, consumers would have a much stronger understanding of what their privacy risks are and could tailor their behaviors and trust levels accordingly."*

For example, a clear majority of consumers who have shared personal data with banks and credit card companies (79%), utility companies (78%), payment apps (78%) and insurance and / or pension providers (77%) say that they trust these organizations to manage it responsibly. Particularly interesting is the strength of Amazon's reputation; overall, three quarters of consumers (74%) trust it to store and use the data they have shared responsibly, in-line with levels of trust in more traditional organizations.

Chart 7: Level of trust in different online platforms – Amazon vs. social media

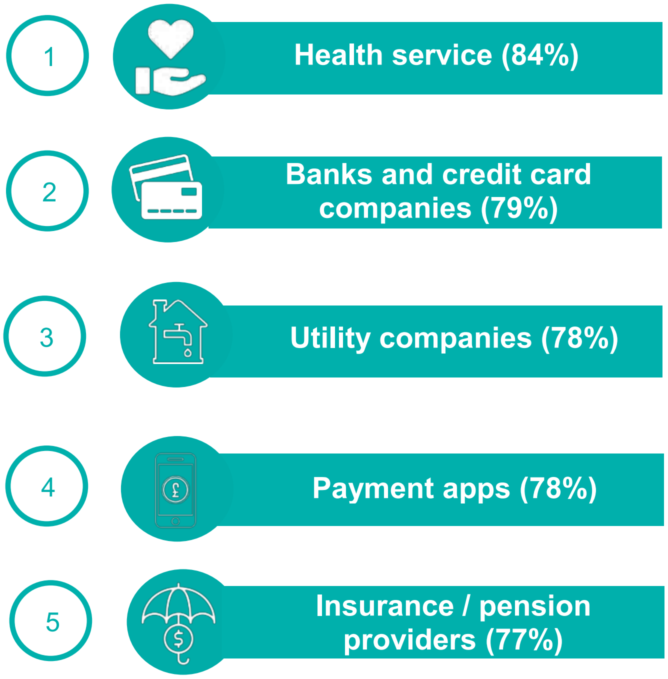
Showing % who say they trust each organization to at least some extent (NET)



Q9. To what extent, if at all, do you trust each of the following organizations to ensure that any personal information you have shared with them online is stored and used responsibly? Base: All except those who don't share personal information with relevant organization / don't know how it is stored (n=variable)

Chart 8: Level of trust in different online platforms – top 5

Showing % who say they trust each organization to at least some extent (NET)



Q9. To what extent, if at all, do you trust each of the following organizations to ensure that any personal information you have shared with them online is stored and used responsibly? Base: All except those who don't share personal information with relevant organization / don't know how it is stored (n=variable)

Engendering confidence that an organization will store and use personal data responsibly is one element of encouraging consumers to share data online more freely, and this should be complemented by a commitment to give the consumer more control over their data. Consent, therefore, emerges as a second key principle for building transparent, trusted data-sharing relationships.

Those who share personal data with Amazon are most likely to feel in control of what is stored (62%), in line with the level of control consumers perceive themselves to have over the data which is stored by banks and credit card companies (61%), the health service (60%), utility companies (60%) and payment apps (60%).

Indeed, Americans are more likely to feel in control of information shared with Amazon (67%) than they do banks and credit card companies (60%). On the other hand, on average only half of those who share personal data with social media companies feel in control over what is stored (48%). With feelings of control so closely aligned with the levels of trust expressed in each organization, enhancing the sovereignty users have over their own data will give them more confidence to engage further with the online world.

Eve Maler:

> *"In simple terms, if consumers are paying a brand for goods or services then they are more likely to have confidence in how that company will use their data. For those businesses that do not have this transactional relationship, it means they need to do more to build trust. Providing greater control and visibility of how data is being used will allow businesses to go beyond the information of transactions and to add value for consumers in other ways."*

A third element of this relationship is consumers' own knowledge of their rights regarding the use of personal data which they have shared online. Those who know at least "a fair amount" about their rights are consistently more likely than those who know "only a little" or "nothing at all" to say that they feel in control of the personal data which is stored by each of the companies with whom they've shared this information. This applies not only to those who have shared data with Amazon (72% vs. 55% respectively), but also to social media (59% vs. 38%). Similarly, those with higher levels of knowledge about their rights are also more likely to not only be happy with the level of personal information they share with each organization, but also would be more likely to sell or share their personal information online in return for discounts and personalization.

Nick Caley:

> *"As new data services appear, brands will need to be much more transparent with consumers about how data is being shared and, often, explicit consent will need to be granted by the user. Inevitably, this will give individuals more leverage and they will be able to seek more, and higher value, rewards in exchange for the data they share. To succeed in this environment, businesses therefore need to find ways to maximise the value they deliver to customers through context driven, relevant insights while also delivering greater transparency, greater control and choice for consumers."*

Consumers believe businesses are primarily responsible for protecting their personal data

In the context of their current attitudes towards data-sharing and who benefits most from it, consumers largely think that organizations who collect and store their personal data should be responsible for its protection. 57% of adults think that it is mainly or only the company's responsibility to protect the data they have shared with them, while only 9% think that it is their own responsibility. In line with these opinions, most (68%) would not be willing to pay anything to retrieve their data if it was lost or stolen and around three quarters (71-78%) would not be willing to pay to ensure that their data was not shared with a third party without their permission.

Further illustrating this are consumer behaviors to protect against data breaches. While the majority of adults surveyed have used anti-virus protection on their computer (72%), cleared their web browser's cache, cookies and / or search history (61%) in the last six months, more complex or time-consuming data protection methods, such as encrypting information online (28%) or using a VPN (19%), are less common.

Nick Caley:

> *"Complex trade-offs between convenient access to services and appropriate security measures mean consumers continue to rely on the business or service provider to take care of this on their behalf. Consumers today are not informed about managing their personal data and there are few or no trusted ways to find out about personal data management and protection online. This highlights a clear need for consumer education and easy-to-use tools for managing personal data."*

Despite limited knowledge of their rights regarding the protection of their personal data and somewhat limited action to protect themselves, consumers are nevertheless sensitive to their data being shared with a third party. Half of those surveyed (51%) would *never* want their personal information to be shared with a third party. If a company was to share their information without their permission, the results show the serious implications for businesses who rely on the sharing of personal data: of the actions tested respondents are most likely to stop using the company (56%), to remove / delete all the data held on them by that company (49%), and to advise their family and friends against using the organization (46%).

However, more serious actions are considered by a significant minority: a third would take legal action (32%), while a quarter would contact the police (27%) or request financial compensation (26%).

Nick Caley:

> *"Our survey shows there is a clear expectation that the companies that profit from the relationship with the customer should be ultimately responsible for protecting customers' personal information. This is now firmly backed up by new and developing national laws, in Europe and in countries like Singapore, Canada, Australia, South Africa and China. As the awareness of new consumer rights regarding personal data becomes an expectation of a different experience, the businesses that have put the customer in control of their data will stand to gain once these new laws take hold."*

> *"As organizations are tasked with processing and storing personal data, they need a single view of the customer to give users a single place to view and manage their profile data, no matter where it is stored; a comprehensive set of end-user privacy capabilities that allow for self-service of the new Data Subject Rights."*

Conclusions

Despite online interactions with organizations being widespread, many consumers are concerned about the amount of data they share on these platforms. Moreover, the majority of consumers have limited knowledge of the digital identity they are presenting online, who has access to their underlying personal information, and what they can do to protect it.

To address these consumer concerns, businesses should focus on three key principles: **trust, consent,** and **education**.

When it comes to protecting the personal data that they share online, consumers believe that responsibility clearly lies with the companies who collect this data. Trust is therefore vital, with the research showing that failing to manage users' digital identities appropriately can significantly impact on a platform's reputation. Moreover. the level of control consumers feel they have over the personal information they share closely aligns with their likelihood to trust different organizations, demonstrating that prioritising the principle of consent in online interactions is also key in promoting data-sharing among consumers.

It is also important to note that concerns over data sharing does not apply to all organizations equally; rather, consumers are far more likely to trust organizations with whom they have a 'transactional' relationship to store and use this data responsibly.

The research suggests that educating consumers about online data sharing, and the benefits of this, is likely to facilitate, rather than restrict, data sharing since those with higher levels of knowledge about their rights are more likely to be happy with the level of personal information they share. Therefore, above all, the results of this research indicate that companies must educate consumers about data-sharing and protection and manage their digital identity in a way that prioritises consumers' control over their own personal data – doing so will help instil confidence in their users in order to build a strong data-sharing relationship and drive future online interactions.

Recommendations

Recommendations for business

Organizations have a strong opportunity in the face of GDPR and other data privacy mandates to approach their relationship building with consumers with fresh eyes:

- Trust: Identify where digital transformation opportunities intersect with user trust risks. For instance, a location service requires a user's location while the service is being used, but everything beyond that point might count as a risk to be mitigated. Be clear with why certain pieces of personal data are being collected, and how they will be used.

- Education: Conceive of personal data as a joint asset and make this a mindset shift within your business. Not every unit within an organization will have the incentive structures to be mindful of data subject rights and is focused on the same goals.

- Consent: "lean in to consent". It is one of six lawful bases for processing personal data defined by the GDPR. Consumer consent gives an organization various freedoms and responsibilities and is the basis for building trusted, transparent digital relationships.

Recommendations for consumers

- Recognize that each of your login accounts represents a whole new opportunity for hackers to cause mischief when it comes to your personal data. You have a strategy for keeping your home and valuables safe, so why not your data?

- If your digital life threatens to be overrun with passwords, consider using a quality password manager (look for "encryption on the device"), using a strong passphrase to unlock it, and letting it generate and remember strong account passwords for you.

- Many businesses are making it possible for you to turn on account features such as "two-factor authentication" and notifications of suspicious account activity to help you become a partner in keeping your own valuable digital assets safe. Easy-to-use strong authentication methods are a good sign that a business has a good understanding of what it takes to become trustworthy.

- Finally, when assessing whether apps are safe for yourself or your children to use, it's valuable – if frustrating – to read the privacy policy but even more valuable to ask yourself just how the company makes its money. "Free" sites and apps still require payment in attention (ad viewing) or data (your personal data or user-generated content, such as status updates), or more likely both – and they might have in-app purchase features too. You need to decide what you're up for, with eyes wide open.

References

[1] Boston Consulting Group, "The Value of Our Digital Identity", *Liberty Global Policy Series* p. 35-36. http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf

Methodology note

ComRes interviewed a total of 8,434 adults online across the USA, UK, Germany and France between the 3rd and 12th of January 2018 (2,091 American, 2,093 UK, 2,151 German and 2,099 French adults). Data were weighted to be representative of each country by gender, age and region. ComRes is a member of the British Polling Council and abides by its rules. Full data tables can be found at www.comresglobal.com

About ForgeRock

ForgeRock® is the Digital Identity Management company transforming the way organizations interact securely with customers, employees, devices, and things. Organizations adopt the ForgeRock Identity Platform™ as their digital identity system of record to monetize customer relationships, address stringent regulations for privacy and consent (GDPR, HIPAA, FCC privacy, etc.), and leverage the internet of things. ForgeRock serves hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, TomTom, and Pearson, as well as governments like Norway, Canada, and Belgium, securing billions of identities worldwide. ForgeRock has offices across Europe, the USA and Asia.

Get free downloads at forgerock.com and follow us @ForgeRock