› Research Paper

Mobility, vulnerability and the state of data privacy

sas
THE POWER TO KNOW.

Contents

About the Research

SAS conducted an online survey among adult consumers yielding 4,368 responses from 15 countries across the globe in North America (30%), Western Europe (42%), the Nordic region (7%), the Pacific region (14%) and South Africa (7%).

We live in a mobile, digital world. Consumers expect and demand that they can connect every aspect of their daily lives to their smartphones and tablets. To live up to this expectation requires organizations to be more intimately aware of consumers' wants and preferences. Without that detailed knowledge, it becomes difficult to offer a truly personalized experience.

And personalization works. No one disputes that. Messages that contain content related to customers' preferences and lifestyle simply perform better. Increasing consumers' connectivity allows marketers to gather and use information that helps provide a more satisfying experience. While many customers are willing to share information, there is a clear give-to-get mentality.

Even as they explore and extend their digital paths, consumers are voicing an uneasiness about the use and control of their personal data. Mobile banking is now commonplace and mobile payments are gaining in acceptance, but people are less willing to share information such as financial details. Trust becomes paramount. Data security breaches at big companies heighten concern.

New technology leaves the public feeling even more vulnerable as inventive information thieves exploit unforeseen security gaps. Consumers also lack trust in the data practices of companies they do business with, despite assurances that data privacy is among organizations' top concerns.

Organizations can better address consumer concerns only if they know where consumers stand on the tradeoff spectrum of personalization and privacy.

That's why for the third year, we have conducted a global consumer survey.

Survey Highlights

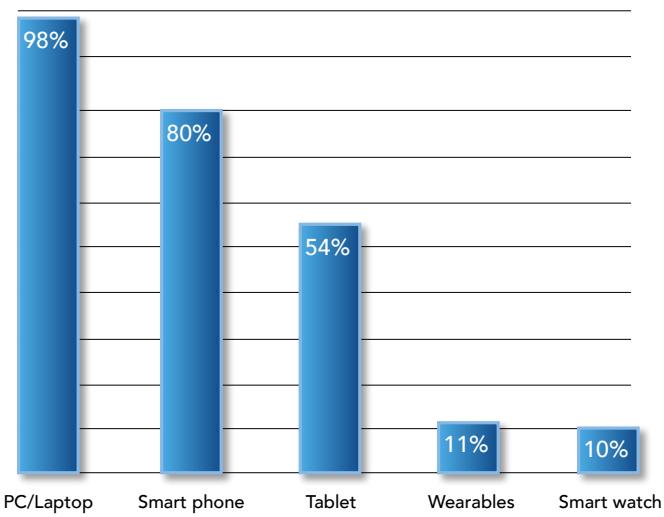
Expanding digital footprints create big shoes to fill

Digital footprints in all parts of the world are expanding. Consumers are on board and logged in. And the use of mobile devices is changing everything. Consider these statistics:

- 45 percent of the world's population uses the Internet.[1]
- At least 5 billion mobile phones will be in use by 2016.[2]
- There are 1.5 billion mobile apps available.[3]
- A third of all web traffic is via mobile.[4]

Our survey results reflect this high level of internet connectivity. While use rates vary by activity, in general, PCs and laptops remain the most heavily used to connect online. But smartphones and tablets have become a permanent part of the digital world. Smart watches and wearables are still fairly new residents of the digital community and, as you can see below, they are at the beginning of their adoption curve among our survey participants. (See Figure 1).

Figure 1: Use of Connected Devices



[1] Internet World Stats, 2015. Internet usage statistics.

[2] Statista, 2015. Number of mobile phone users worldwide from 2012 to 2018 (in billions).

[3] Statista, 2015. Number of apps available in leading app stores as of July 2015.

[4] We are social, 2015. Digital, social and mobile in 2015.

This consumer connectivity and reliance on smart devices has spawned high expectations. Consumers want immediate access and resolution, real-time information and relevant content. In fact, over half of the respondents in our survey expect the companies they do business with to know their preferences and understand their needs.

And they should. Consumers are handing over valuable information with each digital interaction. Every online purchase they make, every social site they join, every search they do and every trip to a store that uses Wi-Fi tracking is adding to the stockpile of personal data businesses can mine to understand them better. Geolocation data, diet and exercise routines, sleep habits, and health information are among the many pieces of personal data consumers reveal via mobile devices. Businesses have a tall order –maximize the use of the information customers provide in order create more meaningful customer engagements.

Privacy and security concerns loom large

But there's a flip side. While consumers enjoy many of the benefits of personalization, exposure of so much personal information is causing some to take pause. In fact, our research shows that 62 percent of consumers have some concern about what businesses do with their personal information.

Age, income and gender play a role in consumers' level of concern about their data. More affluent consumers, women and those over 40 are more likely than their counterparts to take issue with how their information is being used. (See Figure 2).

Security concerns over new technology are lower than for technology in use

Based on our survey, consumers are more concerned about data security for those devices that they currently use most. Six in 10 consumers say that have concerns about data being collected via their smartphones or PCs, while significantly fewer express worries about in-store technology and wearables. (See Figure 3).

It's likely that higher levels of concern for more established technology are related to highly publicized security breaches with these devices, while consumers aren't as aware of security risks associated with more recent technology. Or perhaps they feel that the data gathered from wearables and in-store technology is less likely to put them at risk.

In-store technology – using geolocation to communicate to and track customers – while not new, is not yet widespread. But as wearable use and in-store technologies grow, it's likely that security concerns will also increase.

Figure 2: Concerns use of personal data by demographics

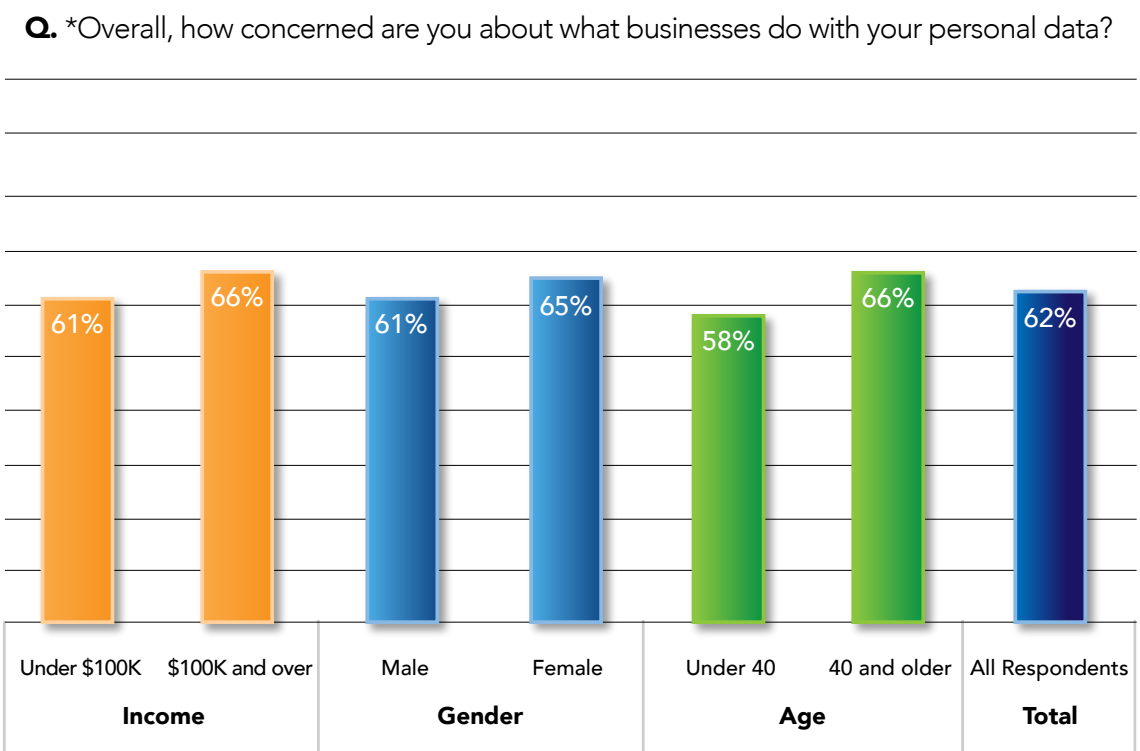
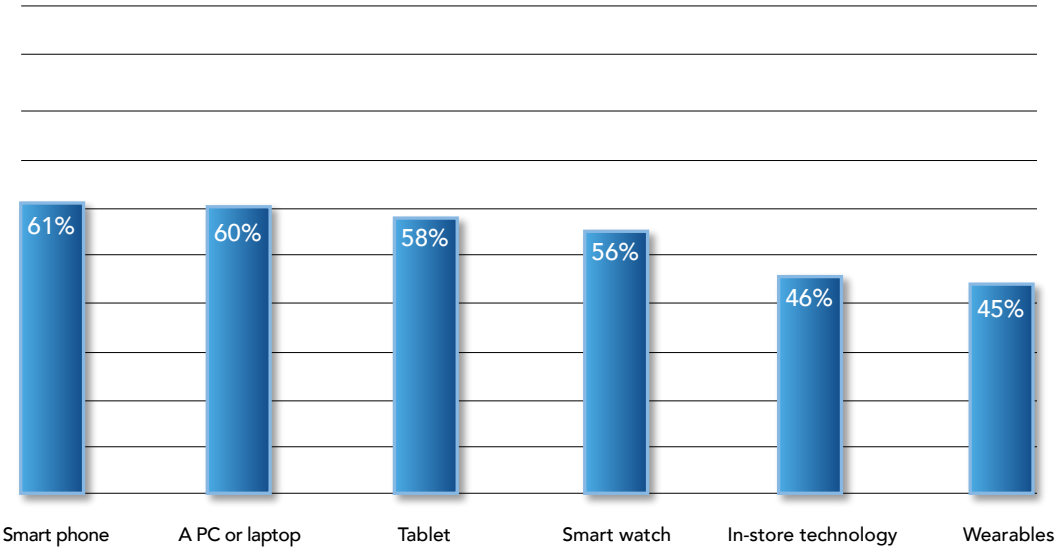


Figure 3: Personal information concerns by device

Q. *How concerned are you about the security of your personal information recorded by your activities on these devices?



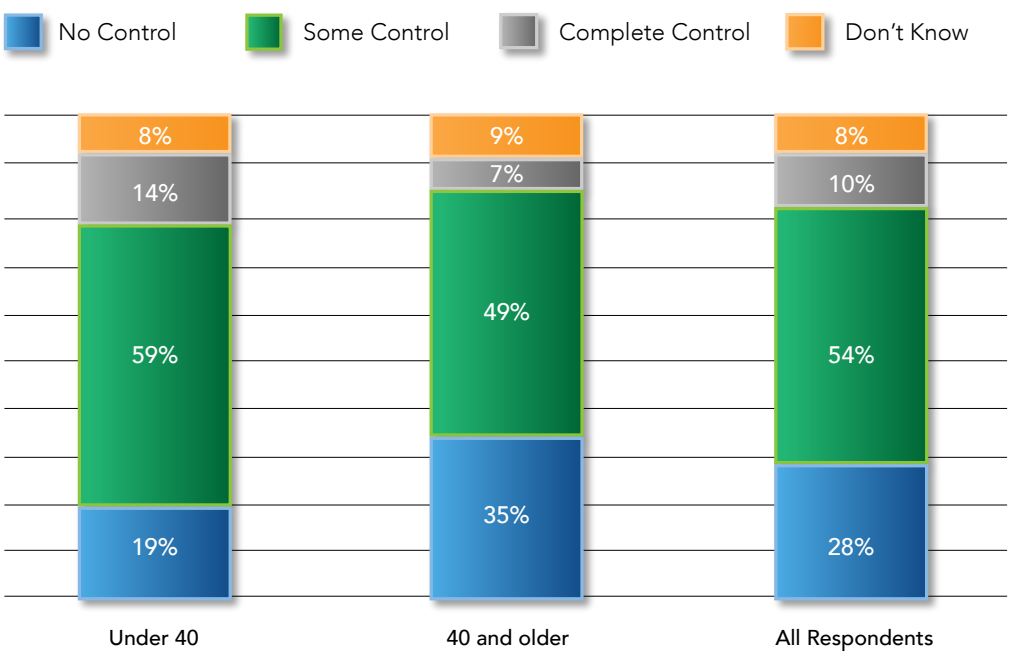
Consumers believe they have little or no control over their own data

And consumers are feeling a bit hogtied when it comes to controlling their own data. Nearly three in 10 believe they have absolutely no control over what businesses do with their information, while 58 percent believe they have some control. Only 10 percent believe they have total control. (See Figure 4).

Consumers who express concern about what businesses do with their information are worried foremost about data security, but also about businesses sharing their personal information with other organizations. For instance, they don't want to be bombarded with unsolicited marketing messages.

Figure 4: Control of data with businesses

Q. How much control do you feel that you have over the personal information you share with businesses?



Concerns about personal data are also fueled in part by their underlying attitudes about privacy. Seven in 10 survey respondents consider using their personal information without their permission a violation of privacy. If respondents already had privacy concerns, that number rose to 77 percent; it drops to 55 percent among those who are less concerned.

Worldwide news of data hacks and breaches, such as those reported in the last half of 2015 at a number of hotels, government agencies and financial websites, intensify public worries about data privacy and security; 63 percent say events like these have heightened their concerns. The impact of reports like these is significantly higher on those who already have data concerns: 76 percent say their concerns have been increased due to these events, while only 40 percent of those with a lower level of concern say these events have had increased their concerns.

Businesses disappoint when it comes to data practices

Consumers are placing a good deal of responsibility on businesses regarding their personal information. And the survey shows that clearly there's a perception that businesses aren't keeping their end of the agreement. The survey respondents' confidence in an organization's ability to safeguard customer data is low. And consumers don't feel businesses are forthcoming about their policies (and changes to those policies) on use of personal data. (See Figure 5).

But to be fair, consumers are a bit apathetic when it comes to learning about a company's privacy policy. For example, only 13 percent of our survey respondents said that they are very likely to read the terms of agreement and privacy policies before they download new apps or software or make purchases. Most of us check the "I agree" box without clicking on the link that leads to the documentation on what we are consenting to.

On the other hand, companies aren't making the policies and terms of agreement easy to consume. Half of the survey participants have at some time chosen not to go through with a transaction because of the terms of agreement. Two key reasons? Length and complexity. But the primary reason is that consumers still had concerns about privacy even after reading the information.

Data concerns are not a digital deterrent

If you thought the concerns consumers express about their data would make them curtail or at least lighten their use of digital platforms, you would be wrong. We know that use of digital technology continues to grow. And as new devices are introduced, early adopters are out in full force long before security vulnerabilities can be identified.

In fact, data security concerns increase as an individual's online activity increases. The survey participants who reported that they are concerned about what businesses do with their personal information are more likely (than those less concerned) to go online, especially via mobile connections, to:

Figure 5: Agreement with privacy statements

- Search for information.
- Make purchases and reservations.
- Visit leisure and entertainment sites.
- Stay in touch with family and friends.
- Look for coupons and promotions.

It's interesting that concerns about personal data increase the more activities a consumer performs online.

It would be sort of like saying fear of flying increases the more time you spend on a plane. But there's an inherent logic in this – increased exposure raises risk. Probabilities go up. So if a consumer is performing lots of tasks online, he or she is conscious of increased exposure. Data concerns follow activity. They don't curtail it.

One exception is mobile payment systems. Only 30 percent of our respondents indicate that they use mobile payment. A primary reason (cited by 44 percent) for not using this technology is data security. In this case, data concerns appear to be influencing adoption.

Give to get: Consumers are willing to trade information

Despite expressing concerns about use of personal data, a majority of consumers say they are willing to provide businesses with limited personal information – primarily an email address and a name – in exchange for some type of discount or benefit. By limiting contact information to an email address and a name, the customer has control over the invasiveness of communications. Overall, what appeals most for customers is the promise of personalized discounts and promotions and discounts on future purchases.

None of the discounts or special offers tested was successful in getting a majority of the customers to give more than an email address and their name. However, special offers at certain times of the year (such as a birthday) increase the likelihood of getting customers to reveal their birthday month and year. (See Figure 6).

Figure 6: Willingness to trade types of information

Information Consumers Are Willing to Provide for Various Offers

Offer	Email address	Name	Birthday month	Birthday year	Address	Phone number	Credit card/ financial data
Personalized discounts and coupons on a regular basis	72%	60%	30%	28%	28%	25%	5%
A discount that applies to every future purchase	70%	60%	31%	30%	27%	29%	7%
Special offers at certain times of the year (holidays, birthday, etc.)	68%	57%	42%	34%	22%	21%	4%
Store credit/coupons to be used on a single future visit	65%	58%	25%	24%	19%	21%	4%
A one-time discount at time of purchase	64%	61%	30%	28%	19%	20%	7%

Appeal of digital marketing messages varies by age

Interestingly, consumers have lukewarm reactions to various types of marketing messages, with no more than 51 percent of all respondents finding any type of message appealing.

Loyalty program updates seem to hold the most appeal, followed by personalized emails. There is little difference in appeal by age group for these two. However, consumers under 40 respond better to messages relevant to their lifestyle. They are also more receptive to promotional offers via text message. (See Figure 7).

Building trust in a mobile, digital world

As consumers browse the web, post to social media sites, share data from wearables and mobile devices or shop online, they are intentionally – and sometimes unknowingly – giving away digital bits of information about their identities.

Brands can harness petabytes of data to better identify and serve customers. Yet consumers and organizations often unwittingly leave themselves vulnerable to emergent technologies, data breaches, poor data governance and unclear privacy strategies that put a customer's personally identifiable data at risk.

Figure 7: Appeal of marketing messages

Appeal of Marketing Messages

% of respondents who indicated the marketing message is somewhat or very appealing	Under 40	40 and Over	All Respondents
Loyalty program updates and offers from companies I do business with	52%	51%	51%
Personalized emails from companies I do business with	46%	43%	45%
Promotional emails from companies related to my lifestyle and/or interests	45%	38%	40%
Direct mail/catalogs from companies related to my lifestyle and/or interests	41%	37%	39%
Advertisements relevant to my lifestyle and/or interests on webpages I visit	38%	29%	34%
Text messages with promotional offers from companies I do business with	36%	28%	32%
Text messages with promotional offers specific to my location from companies I do business with	36%	27%	31%
Advertisements from mass media outlets (TV, newspapers, etc.)	36%	26%	31%
Messages and advertisements relevant to my lifestyle and/or interests on social media feeds	39%	23%	30%

Vulnerabilities highlight important challenges for brands:

- The complexity and fragmentation of the customer journey due to the expansion of digital channels, platforms, data and content, which has placed enormous burden on marketing to be contextually and personally relevant and responsive.
- While companies that deliver a more personalized experience tend to achieve higher customer satisfaction and increased revenue, they are struggling to engage customers without giving the perception that they are infringing on the customer's privacy.
- Failure to incorporate privacy into a personalization strategy can have consequences such as increased regulatory scrutiny and damage to brand reputation.

In today's world, you need to be digitally trusted – by customers, partners, suppliers and all the other stakeholders in your business (sales, marketing, service and support, operations, product teams, etc.). Regardless of where you start, your organization can lead in this latest, expanded digital trust ecosystem and bolster your trust advantage by focusing on three things:

Start trust conversations in the boardroom

As digital opportunities and threats become critical to business strategy; boards and C-level executives must have the digital expertise to balance between protecting the business and enabling profitable digital growth through personalized brand experiences.

They must be able to ask the right questions and hold management accountable. Executives also must gain commitment and support from the board to implement a long-term strategy for privacy protection.

How? The C-suite and board should address these questions:

- Is privacy a board-level priority within your organization?
- Is privacy a consideration when acquiring and implementing new business processes and technologies?
- Do you have privacy governance and operating models in place?
- Do you continually monitor and evaluate data privacy performance?

Build trust by mastering data management and stewardship

When different systems capture the same information, it's seldom consistent. And inconsistency can lead to errors, which often results in unnecessary lapses in privacy and damage to the brand. Data management solutions identify, link and reconcile different pieces of data across business processes, providing a single view of information available for improving business operations and analytics for decision making. Here are some considerations:

Set policies and guidance for collecting, sharing and using data. Organizations should create a high-level statement of values concerning their use of personal data, arrived at through a process that creates common understanding and internal commitment. Here's how:

- Formalize and document your policy for using customer data for personalization.
- Clearly articulate your rules and practices for using customer information to personalize the customer's experience.
- Incorporate privacy by design into business processes that balance business requirements with privacy expectations.

Develop processes to ensure compliance. Codes of conduct need to be embedded in operations. Organizations should design processes and systems that restrict data access to approved uses only, with feedback mechanisms and monitoring capabilities to measure performance and identify breaches if they occur. Some guidelines include:

- Using anonymous data whenever possible.
- Abiding by data-retention rules if data is not anonymous.
- Obtaining informed consumer consent when collecting personal data.
- Being transparent about the reasons for collecting data.
- Ensuring data is accurate and secure – at all times.

Incorporate trust when engaging with customers

Given the importance of trust, companies must create an open, ongoing dialogue with customers so customers understand how brands will safeguard personal data. You can enhance trust in customer engagements in several ways.

Communicate how data stewardship is being implemented. Consumers need to be clear on the company's position on personal data and privacy. This goes beyond publishing a privacy policy. Consumers must see how a brand has embedded its privacy principles into everyday operations. This must be an ongoing and transparent process that applies not only to company's normal business practices but also to those times when a data breach or privacy violation occurs. Two best practices are:

- Communicating often and seeking customer feedback on how well you are doing.
- Explaining the value to customers.

Clarify how data is being used. Many consumers don't realize the myriad ways their personal data is used including the legal agreements and disclaimers they must sign in order to download a mobile app, access a social media platform or sharing on mobile apps. All businesses must strive to create clear and simple communications on how they use the data that consumers either implicitly or explicitly agree to provide. Three ways you can make sharing information more appealing:

- Make tools available to consumers that offer them more control over their data.
- Don't assume that you can use data that seems freely available without analyzing the legal risks.
- Don't use third-party database content without authorization.

Provide transparency into new uses of personal data. Organizations must be transparent in their communications to consumers about the ways they use personal data. Different countries have different requirements governing the use of personal data. Consumers' concern about data privacy also varies depending on demographics and type of industries. Companies will need to tailor the approach – implied consent, opt in or opt out – to each customer context. Here are some guidelines for providing personalization without invading your customers' privacy:

- Base the degree of personalization on how well you know the customer.
- Use only explicit information shared with you by the customer for personalization.
- Continually align personalization to the customer's purchase journey.
- Don't use personalization in sensitive situations.

Trust is a competitive asset in today's digital landscape. Use it to build an organization that recognizes it value, and you will outperform your competitors. You will gain an advantage in brand differentiation.

Gaining this advantage will require leadership and a shifting of responsibility for privacy-related issues from regulatory staff to the C-suite. Organizations that can transparently steward consumer information – restricting its use to mutually beneficial and agreed-upon scenarios – will encourage customers to share more data to create better experiences, products and services and generate more value for consumers, leading to meaningful shifts in market shares and faster growth.

Learn More

To learn about SAS® Customer Intelligence solutions, visit sas.com/en_us/software/customer-intelligence.html.

Explore hot topics in marketing at Marketing Insights. sas.com/en_us/insights.html

For fresh perspectives from other marketers, read our Customer Analytics blog. blogs.sas.com/content/customeranalytics

To contact your local SAS office, please visit: sas.com/offices

108097_S151781.0316