The 2017 State of Consumer Privacy and Trust

Consumers Understand They Must Take Control of Their Own Privacy, Yet Concerns Persist in Light of Ongoing Breaches, Risks of IoT

As usual, there's a lot going on in the world of consumer privacy and security, from Yahoo's endless hacking woes to FBI Director James Comey's assertion that "There is no such thing as absolute privacy in America." And with the rise of the Internet of Things (IoT) — which contributes to the interconnectivity of everything — these issues likely won't be on the wane anytime soon. Indeed, it seems that privacy and security are perpetually top of mind for consumers and brands alike.

In an effort to gain additional perspective on attitudes toward security and privacy in the Digital Age, Gigya polled 4,002 adult respondents — one-half from the U.S. and one-half from the U.K. — on their concerns and perceptions. The results yield important insights, including:

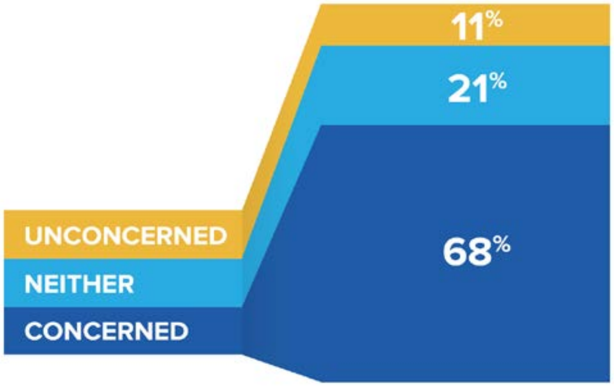
- Sixty-nine percent of consumers are concerned about device security and privacy risks with increased adoption of IoT devices.
- Two-thirds — 68 percent — don't trust brands to handle their personal information appropriately, such as name, email, location or marital status.
- Sixty-three percent of respondents acknowledge they bear some responsibility in protecting their information. After a breach, 62 percent have changed their passwords, 32 percent have added a second factor of authentication, and 18 percent have closed an account.
- In addition, 61 percent of respondents with Facebook accounts have taken advantage of the social network's privacy settings by updating their preferences.
- Despite taking some measures to protect themselves, 70 percent use seven or fewer passwords across their many online accounts, indicating poor password hygiene habits.
- Consumers believe recent changes in national governments will have little impact on their security and privacy, according to 53 percent of all respondents — 41 percent in the U.S. and 65 percent in the U.K.

Consumers Don't Trust How Brands Handle Their Personal Information

Trust is the foundation of any relationship — including the one between consumer and merchant. With the Internet as the great equalizer, the consumer-brand relationship stands to lose a lot if not maintained properly — that is, merchants setting and adhering to strong and easily understood privacy policies and ensuring transparency in how consumer data is handled. Despite brands' efforts to this end, consumers still hold strong in their opinions that brands are not as forthright as they should be in explaining how they handle and protect a customer's information.

Our survey results support this, with 68 percent of respondents either "Very Concerned" or "Concerned" about how brands are using their personal information (i.e. name, email address, location, marital status, etc.). Twenty-one percent are "Neither Concerned nor Unconcerned," and the 11 percent remainder are "Unconcerned" and "Very Unconcerned." This lack of trust has profound implications for the relationship between consumers and brands.

MORE THAN ⅔ OF CONSUMERS DON'T TRUST BRANDS WITH THEIR PERSONAL INFORMATION



Despite rumblings about lax brand privacy policies, the majority of our respondents have not seen any change over the past year. Thirty-six percent report that there has been no change, while 33 percent believe brands' privacy policies in general have become stronger. Interestingly, 31 percent believe they've become weaker. Of the total responses, 41 percent of U.K. respondents have seen no change and 32 percent report weaker policies, despite the European Union's General Data Protection Regulation (GDPR) going into effect next year.

Brands like Facebook today employ a transparent approach to privacy that empowers consumers to control how much personal information they share and with whom. Since implementing this transparent approach approximately two years ago, Facebook has grown its monthly active users to 1.86 billion as of Q4 2016 (adding 467 million new users since the same time two years ago) and the company market capitalization has grown 167 percent during that same period to about $400 billion today. Facebook's proactive approach to privacy has clearly been a boon not only to their business but also to consumers, who have a clearer understanding of how their data is used on the social network.

CONSUMERS TAKE ADVANTAGE OF PRIVACY CONTROLS

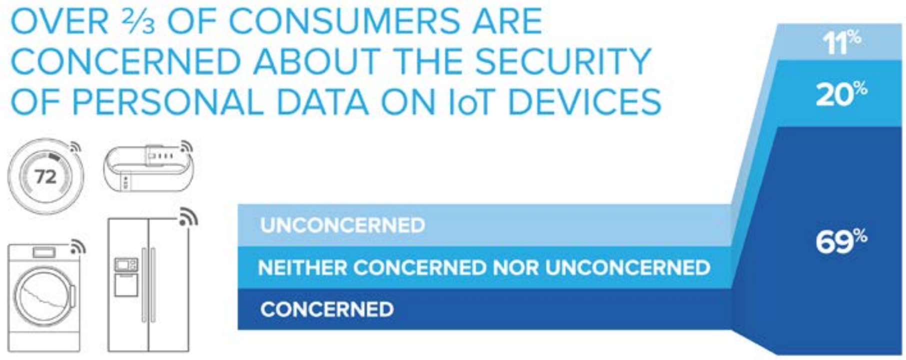
Respondents with a Facebook account who have updated their privacy settings

61%

Our survey results show that of the total respondents that have Facebook accounts, 61 percent have taken control of their privacy settings on Facebook — 40 percent have changed their settings within the past year and 21 percent have changed them at some point more than 12 months ago. Twenty-three percent are aware they can make changes to their privacy settings but rely on Facebook's default settings, while 16 percent were unaware that they could change their privacy settings. Of the 22 percent of total respondents that do not have a Facebook account, 45 percent belong to the silent generation, which preceded the baby boomers.

IoT Sparks Anxiety Over Data Privacy, But Changes in Government Don't

The security of IoT devices has come under scrutiny lately, especially with reports that the CIA has the technology to "spy" on Americans through their smart devices.

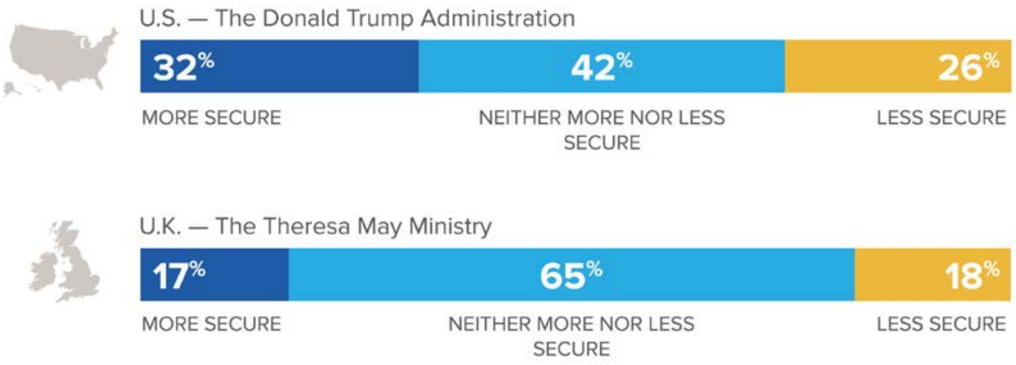


OVER ⅔ OF CONSUMERS ARE CONCERNED ABOUT THE SECURITY OF PERSONAL DATA ON IoT DEVICES

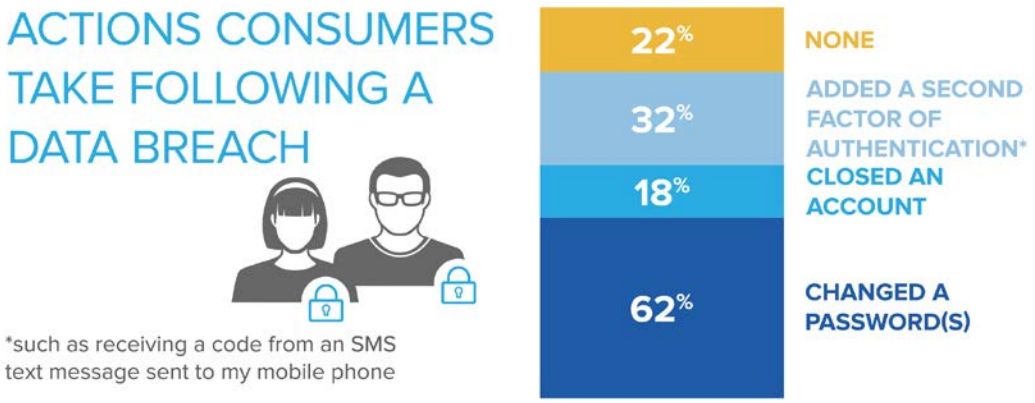
Our survey results indicate some apprehension over the security of IoT devices, with 69 percent of respondents either "Very Concerned" or "Concerned" about the security of their personal data on devices like smart watches, connected cars, fitness trackers and home appliances. Twenty percent are "Neither Concerned nor Unconcerned," while 11 percent are "Unconcerned" or "Very Unconcerned."

Regionally, it seems Americans are somewhat more concerned overall about IoT security than their U.K. counterparts, with 73 percent "Very Concerned" or "Concerned" vs. the UK's 66 percent.

CONSUMERS DON'T FEEL NEW GOVERNMENTS WILL MAKE THEIR PERSONAL DATA MORE SECURE



Changes in government, meanwhile, do not appear to have a major impact on consumers' expectations and attitudes about the security of personal data overall, although recent changes in the U.S. may have had a more polarizing effect according to our survey. In the U.K., a clear majority of 65 percent of respondents felt that the May ministry will not have an effect on the security of the data. By contrast, 42 percent of respondents in the U.S. felt the Trump administration would have no impact on the security of their data, while 32 percent of respondents felt their personal data will be more secure and 26 percent felt their personal data will be less secure.



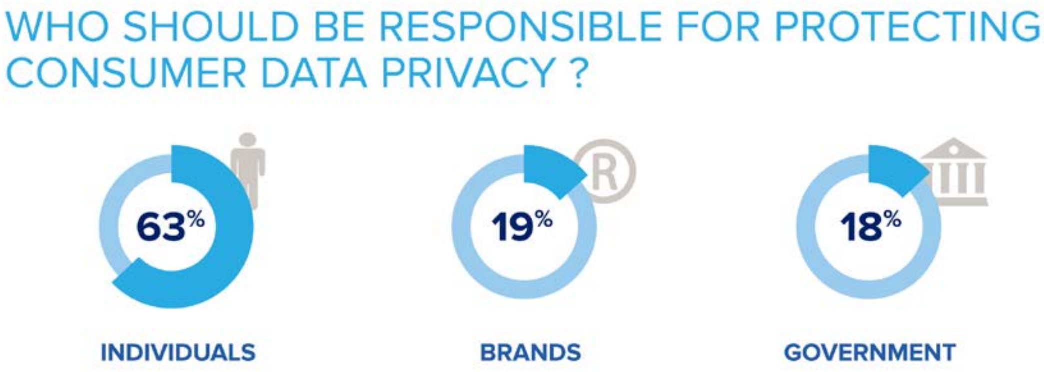
ACTIONS CONSUMERS TAKE FOLLOWING A DATA BREACH

*such as receiving a code from an SMS text message sent to my mobile phone

Data breaches reported by the likes of Yahoo, Target, LinkedIn and others illustrate the need for consumers to be better educated and more vigilant when it comes to securing their personal information. In light of widely reported breaches, the majority of our respondents have taken steps to better protect themselves: 62 percent changed their passwords, 32 percent added a second factor of authentication — such as receiving a code from an SMS text message sent to a mobile phone — and 18 percent closed an account. Consumers' willingness to be accountable for their data security and not relying on companies and governments represents an opportunity for forward-looking brands to provide proactive privacy and security measures that increase their trustworthiness in the eyes of consumers. As the Facebook example illustrates, brands that get this right can reap some big rewards.

Consumers Assume Accountability for Data Privacy, Yet Don't Follow Best Practices

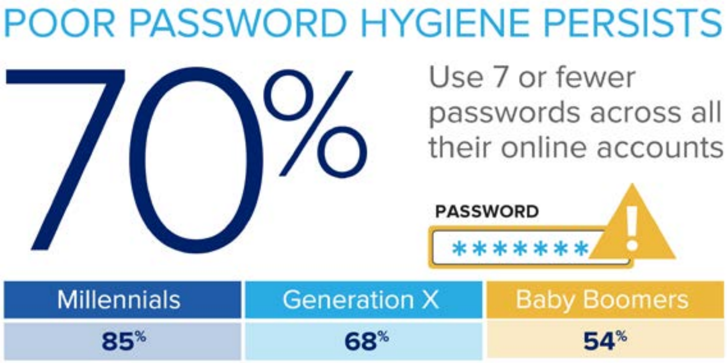
When asked whose responsibility it is to protect their information, an overwhelming number — 63 percent — believes the onus is on themselves. Only 19 percent think brands should assume responsibility, and 18 percent believe it's the government's responsibility.



WHO SHOULD BE RESPONSIBLE FOR PROTECTING CONSUMER DATA PRIVACY ?

The findings point to a need for brands to adopt a platform that provides consumers with greater control over how their data is protected and visibility into how a brand will utilize this data, essentially enabling customers to choose their level of security and privacy settings.

The results also uncover a conundrum. Despite many consumers feeling accountable for their data's protection, most still don't follow best practices with their passwords. Seventy percent of respondents use seven or fewer passwords across all their online accounts. And, it seems to be a generational issue: millennials are the worst offenders at 85 percent, Generation Xers follow at 68 percent and baby boomers at 54 percent.



As new devices emerge and interconnectivity pervades the technology landscape, it will become increasingly critical for brands to rebuild consumer trust in how their personal information is handled. This mistrust has only been exacerbated by the explosion of personal data produced by consumers, especially with the rise of smart devices and IoT. Even with the adoption of consumer privacy laws, such as GDPR, consumers still have little confidence in the impact governments can have in changing the practices and safety of their data. However, brands like Facebook have demonstrated that putting consumer privacy top of mind can engender a great deal of trust, and brands stand to gain tremendously.

Brands can start by putting forth clear privacy policies and gathering consent for how they are using consumer data to provide greater transparency. Brands that can provide a great customer experience and provide the customer with ways to view, edit and delete the data collected and used give consumers both control and a great customer experience. In addition, deploying platforms that will strengthen security around consumer data and help protect consumers from their own poor password practices an also boost confidence. While hacking and breaches may always be part and parcel of the Digital Age, a partnership between brands and consumers can also have a significant positive impact.

Methodology

Sponsored by Gigya, this survey was conducted online in March 2017 by Arlington Research. The 4,002 respondents were surveyed from a nationally representative sample of adults — age 18 and older — in the UK and the Republic of Ireland (2,001) and the U.S. (2,001). Quotas were applied to the sample to ensure that it represented each country's overall population based on gender, age and region.