CONTAGIOUS

CONTAGIOUS INSIDER / PRIVACY

This article appeared in Contagious issue 39

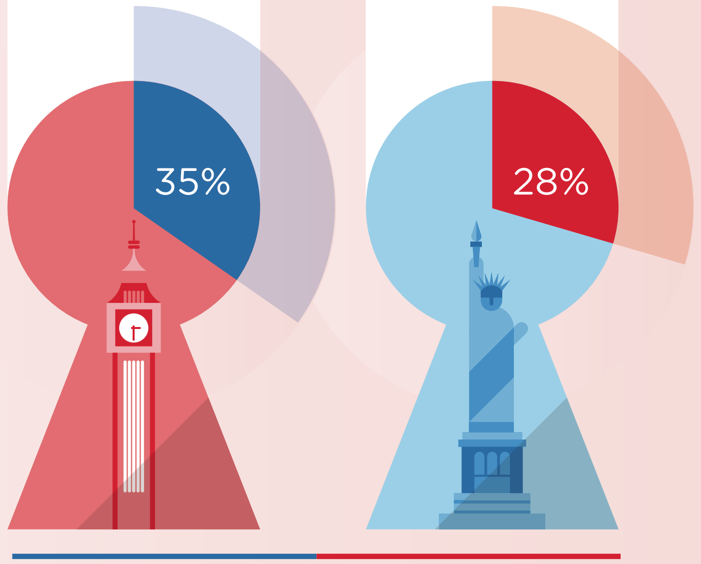
Contagious is a resource for the global marketing community
focusing on non-traditional media and emerging technologies.
www.contagious.com

For more information please contact the team on
+44 (0) 203 206 9266 or sales@contagious.com

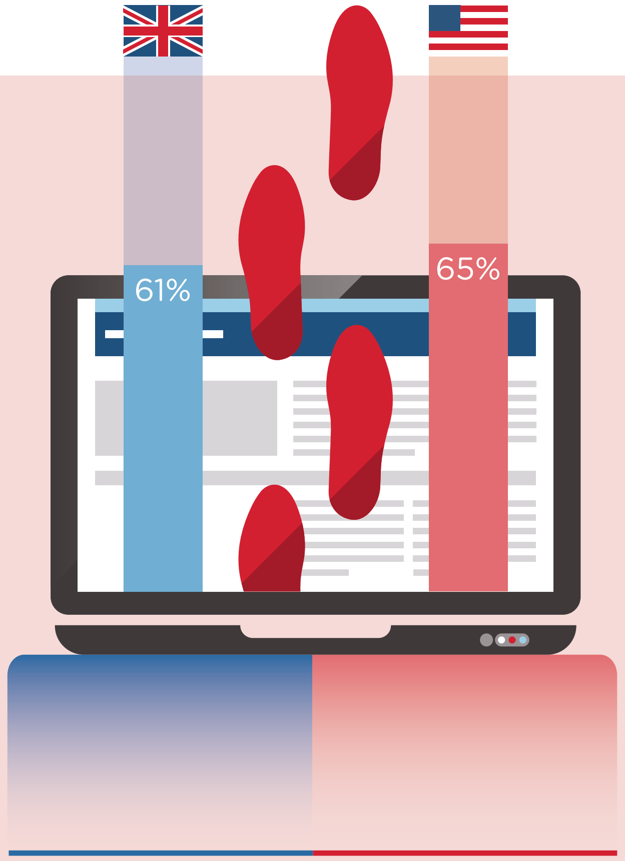
PUTTING A PRICE ON PRIVACY

What privacy means in a digital world, why marketers can no longer afford to ignore it, and how you can turn privacy from a regulatory headache into a competitive advantage

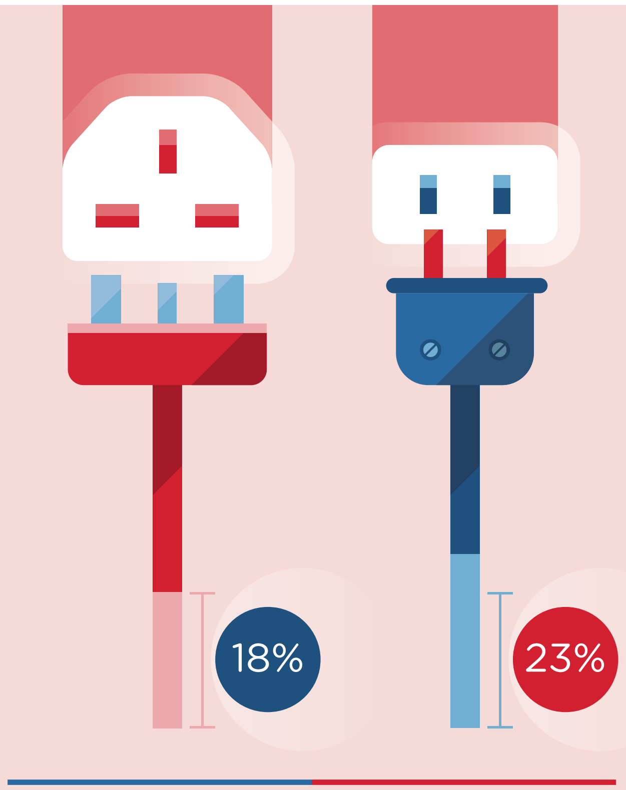
By Arwa Mahdawi



Only 35% of people in the UK and 28% in the US expect that it is realistic for any information about themselves online to remain completely anonymous



61% of people in the UK and 65% of those in the US think all or most of their online behaviour is tracked



18% of people in the UK and 23% in the US think all or most of their offline behaviour is tracked

Illustration / Fernando Volken Togni / YCN

CAREFUL: YOU'RE BEING WATCHED

It's a bright, cold day in April and the internet-connected SmartClocks are striking 13. *Nineteen Eighty-Four* has gone from being a classic work of dystopian fiction to a tired cliché, dredged up by journalists to describe a contemporary reality of overly social media and hyper-targeting. It is 2014 and Big Brother isn't watching you, everyone is.

And that 'everyone' includes you. You might not have 'analyst' in your job title, but I'd be willing to bet that some part of your job involves the collection or application of people's personal information. While data used to be the preserve of number-crunchers in some far-away cubicle, it now sits at the heart of marketing. And for good reason: leveraged correctly, data makes your brand more relevant, more efficient and more effective. Leveraged responsibly, data helps you forge deeper, more meaningful relationships with your customer. Leveraged irresponsibly, however, data can raise privacy issues that erode trust in your brand and make consumers unwilling to transact with you.

Over the past year, a series of high-profile privacy outrages, including, of course, the summer of Snowden, has pushed privacy permanently into the headlines. 'The discussions around government access to public data have triggered a conversation around our privacy that is long overdue,' notes Mary Ellen Callahan, chair of Jenner & Block's Privacy and Information Governance Practice, and the former chief privacy officer of the US Department of Homeland Security. 'Following June 5, I no longer have to explain what I do at cocktail parties,' she adds wryly.

The debate around privacy means that most businesses are well aware that the issue is something they must address. Nevertheless, we're not seeing many of them do much more than simply pay it lip-service. Indeed, there is still a misguided view among marketers that while privacy may be the subject of chatter at cocktail parties, it is not really going to affect their bottom line. But privacy isn't a zeitgeisty talking point people will get bored of: it's an issue that's only going to get more urgent and that will have a major impact on how marketers are able to use consumers' data going forward. Research from GfK found that 80% of consumers surveyed wanted more regulation to protect their data privacy and less than 40% trust marketers with their personal data. Further, 60% said their privacy concerns have risen in the past 12 months. Brands that are myopic about privacy will struggle to establish and keep consumer trust in the not-so-distant future.

CONSUMERS CHOOSING CONFIDENTIALITY

Quantitative and qualitative research commissioned by Contagious in March 2014 makes it clear: privacy concerns are beginning to encroach on how consumers interact with brands. Some 49% of respondents in the UK and 57% in the US stated that they invest time and money in protecting their online privacy, while 33% of people in the UK and 42% in the US have stopped using a product or service because they were worried about how it was using their personal data. Brands with particularly affluent consumer bases should take note: privacy worries are especially prominent among the wealthy in Britain, with 68% of people who earn more than £90,000 ($151,000) per year having switched brands due to privacy concerns.

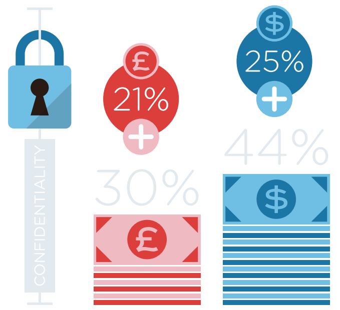
External research provides further evidence that the debate around privacy is affecting our behaviour and buying habits. A Harris Interactive study carried out in April 2014 found that more than a quarter of the 2,000 people surveyed in the US were doing less banking online following the news about the US National Security Agency's snooping, and 24% were less inclined to use email. Millennials appear to have changed their behaviour the most, with a third of people aged 18 to 34 saying they were doing less shopping online compared with 26% of the public at large. The conventional wisdom that states 'millennials don't care about privacy' is being exposed as a myth. If marketers don't adapt their businesses to this changing landscape, their customer base will go elsewhere.

And, with the market for privacy-protecting alternatives to traditional products and services expanding every day, there are now a lot more places for customers to go. If you're worried about the security of WhatsApp or iMessage, you'll soon be able to opt for Heml.is, a secure message service (see Small But Perfectly Formed, page 52). If you're concerned about potential data leaks from your smartphone, you can trade it in for a Blackphone, a pro-privacy handset that uses a customised version of Android called PrivatOS. The privacy industry is booming: the market for mobile security management products alone was estimated to be worth $560m in 2013 and is expected to rise to $1bn a year by 2015.

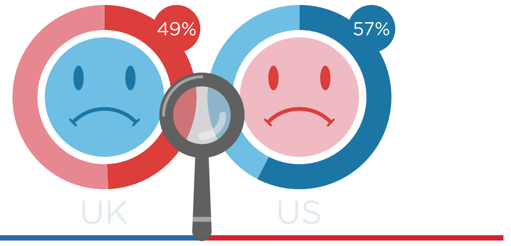
One upstart brand that has found favourable footing in these shifting sands is DuckDuckGo, a search engine that emphasises protecting searchers' privacy. Founded in 2008 by Gabriel Weinberg, DuckDuckGo received funding from Union Square Ventures, backers of Twitter and Tumblr, in 2011 and reached 1 million direct searches a day in February 2012. Use of the platform skyrocketed post NSA-revelations. In June 2013, it reached more than 3 million direct searches a day and, almost a year later, the search engine's traffic figures show that it wasn't a temporary hike.

Explaining the surge in interest in DuckDuckGo, Weinberg says: 'People don't want to be tracked. That hasn't changed. What's changed is two-fold. First, the extent of the tracking, both public and private, has become more clear, and it is unsettling enough to make people seek out alternatives. Second, alternatives like DuckDuckGo now exist where you can get both great results and privacy. What we've seen in our numbers is that a lot of people would gladly choose to switch to a private alternative without sacrifice.'

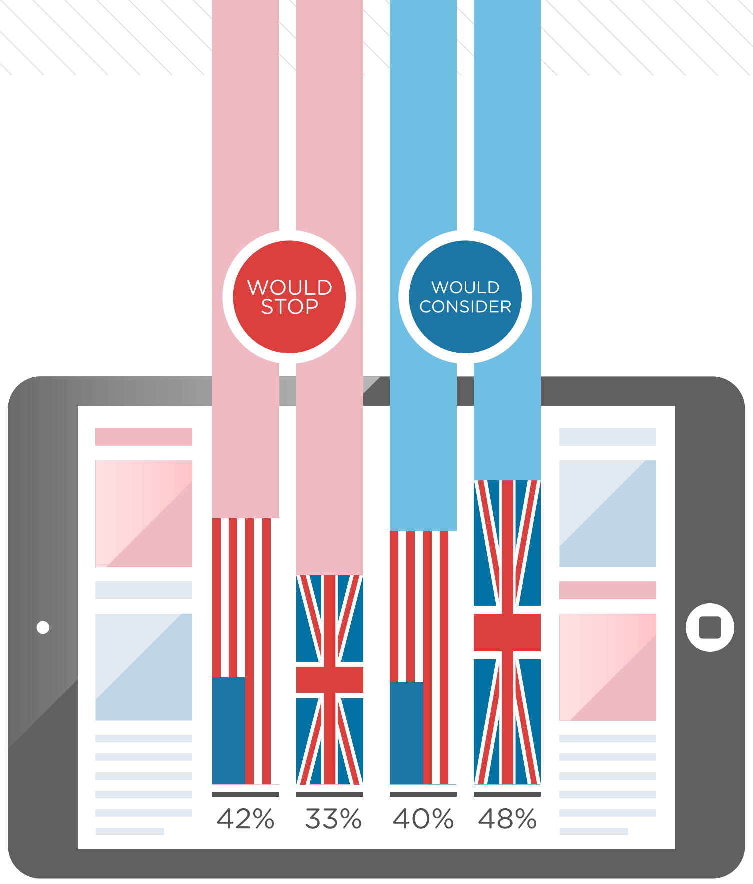
In some cases it seems that people are even willing to switch to a private alternative when there is a sacrifice. Contagious' quantitative research, conducted by Opinium, found that 30% of people in the UK and 44% of those in the US would be willing to pay something in exchange for total confidentiality when buying products and services online. Of these, respondents in the UK would pay an average of 21% extra, while those in the US would pay 25% extra. In both countries the younger generations are more likely to be willing to pay something, and of those that would, they would pay proportionately more. Again, the myth that millennials don't care about privacy is quickly being overturned.



30% of people in the UK and 44% of those in the US would be willing to pay something in exchange for total confidentiality when buying products or services online. Of these, those in the UK would pay an average of 21% extra, while those in the US would pay 25%



The fact that we're used to our information being tracked, doesn't mean we like it: 49% of respondents in the UK and 57% in the US say that protecting their online privacy is something they invest time and money in.



42% of people in the US and 33% of people in the UK have stopped using a product or service because they were worried about the way it was using their personal data, and another 40% in the US, and 48% in the UK would consider doing so.

PRIVACY BY DESIGN

DuckDuckGo, Heml.is, and Blackphone can all be considered examples of 'privacy by design', a philosophy in which privacy provisions are embedded into products, marketing strategies and business practices from the beginning rather than as an afterthought. Coined by Ann Cavoukian, the privacy commissioner for Ontario, Canada, back in the 90s, the principle has been embraced by both the European Union and the Federal Trade Commission as a critical part of their revision of privacy laws.

While it might be tempting to dismiss privacy by design as only really relevant to regulators and niche brands that have privacy as one of their main propositions, this would be a mistake. As data and analytics become increasingly important drivers of modern marketing, the smartest brands are those that realise that a privacy-by-design approach to tech systems, marketing strategies and business practices is going to be a critical element to long-term success.

Even Big Tech has made a recent volte-face towards privacy by design. Only a few years ago, Google CEO Eric Schmidt suggested that anyone concerned about online privacy was trying to hide something, and Mark Zuckerberg claimed that privacy was no longer a social norm. However, both Schmidt and Zuckerberg appear to have changed their tune. At SXSW this year, Schmidt was unequivocal about the importance of privacy, stating: 'In hawks versus doves, hawks win. Fight for your privacy or lose it.' And, in March, Facebook started testing a new feature called 'privacy checkup', which takes the form of an illustrated dinosaur that pops up when a user posts something publicly, reminding them about their option to keep the post limited to a smaller circle of friends.

Facebook may have chosen to represent privacy as a dinosaur but the very introduction of the feature is a clear acknowledgement that privacy isn't extinct. Around nine out of ten people in the UK and US believe their privacy should be protected online automatically, according to Contagious' qualitative research, carried out by global insight and brand consultancy Flamingo. Brands that can provide peace of mind will engender consumer trust and find themselves with a competitive advantage. The fact that the world's most enthusiastic advocate of uninhibited sharing has recognised this and is scrambling to stay relevant by openly addressing privacy concerns should be a major wake-up call for marketers who still believe that privacy is simply a short-term trend.

HOW TO PRIVACY-PROOF YOUR BRAND

A key step toward embedding a privacy-by-design ethos in your business is to incorporate privacy considerations into your user journey mapping. This involves looking at each consumer touchpoint through the lenses of data context, collection, exchange and storage:

1) Contextual privacy: incorporate this into the user journey

It can be helpful to think about people's trust as concentric circles. We go from private circles (friends, families, colleagues) to global ones (government, brands, everyone else). Expectations of privacy depend on which circle we're in – we choose what to share, and control the integrity of each of these discrete environments. And we pick and choose different communications tools depending on these needs: Snapchat when we want to share privately with a friend, Tumblr when we want to project publicly to the world.

Context was a major theme in the ethnographic research we commissioned. 'I think there's a big difference in terms of the expectation of privacy between Netflix and Gmail,' explained one Gen X male. 'Obviously it makes sense to me that Netflix is going to have a record of what DVDs I've watched. But it is off-putting to see a targeted ad based on an email I have sent – it makes me think my email is being read by someone.' While email was in his private circle, his Netflix history wasn't, leading to very different privacy expectations.

> ***Companies need to think more strategically about what data they really need***
>
> Mary Ellen Callahan, Jenner & Block

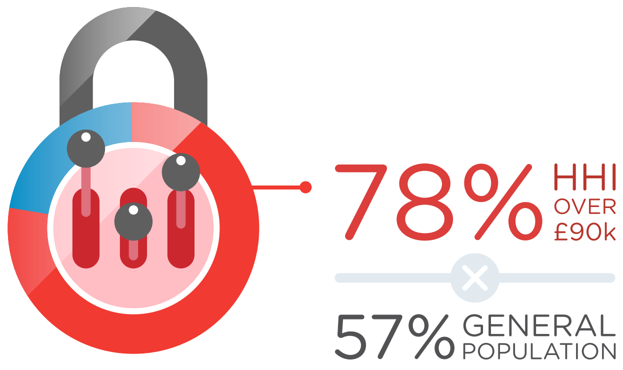
Privacy today isn't about anonymity and it's not a binary on and off switch. Rather, the contemporary understanding of privacy is based on maintaining the integrity of context. Privacy should be worked into how you approach the modern consumer journey. What is the different privacy need-state at each stage and across each touchpoint?

2) Collecting data: transparency and control are key

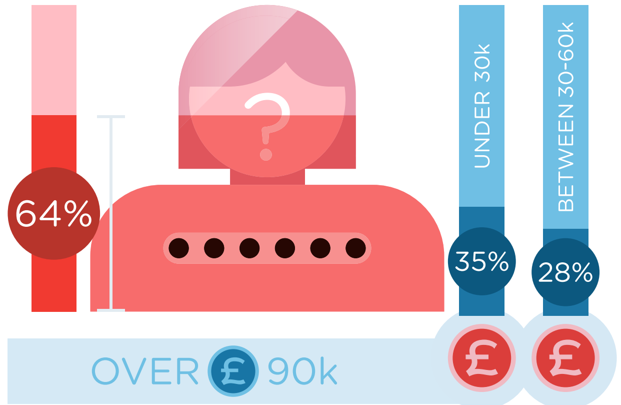
When looking at the sort of data that can be collected at each consumer touchpoint, brands need to think harder about how they're collecting it and why. To begin with, brands should make a distinction between 'earned data' and 'extracted data'. What data will people give you and what data can you extract using analytical tools? Data that people offer you freely is often more valuable than data you grab by stealth. Not only is the transaction transparent, but it can be more relevant.

As data considerations start to become incorporated into product design, having control over what data you choose to share is going to become even more salient. John Foreman, MailChimp chief data scientist, notes that data collection and analysis is going to affect product design in myriad ways. He cites Disney's RFID-equipped MagicBands, which are monogrammed with each family member's name, as an example 'where the product itself has been designed to ensure data purity (prevent switching between users). Alternatively, we'll see a lot of products that are designed to add in some data-gathering component even if data gathering isn't necessary for their operation (much like you have with smartphone apps and games these days). Data has become indispensable for improving and expanding a product, and so people are going to bake in data gathering even if they don't exactly know how to use it at the outset.'

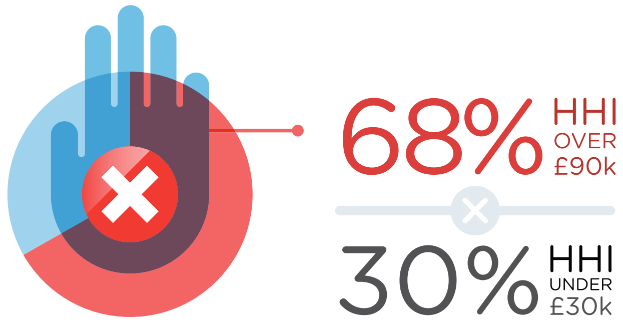
While baking in data-gathering abilities may be important, brands should remember that more is not necessarily more when it comes to data collection. Try to get people to give you information you can use to provide them with a better product or service rather than continually extracting reams and reams of data you might never need. As Jenner & Block's



78% of those with a household income (HHI) of more than £90,000 in the UK think they have some or total control over their personal data, compared with 57% of the general population.



64% of those with a household income in excess of £90k in the UK believe it is possible for their information to remain completely anonymous compared with 35% of those with a HHI of less than £30k and 28% of those earning between £30,000 and £60,000.



68% of those with a HHI over £90,000 in the UK have stopped using a product or service because of privacy concerns compared with just 30% of those with a HHI less than £30,000.

Callahan notes: ‘Companies need to think more strategically about what data they really need. Do they really need to collect precise geolocation to serve a targeted ad? And if they do need to collect the data, do they need to store it? And if they store it, how do they store it? How much detail do they really need to keep?’

3) Exchange: establish a Return on Personal Information (ROPI)

People are often happy to give up their personal data if they get something in return. According to a study by Research Now, 47% of women would willingly share their mobile phone location with a retailer in return for a $5 credit and 83% would do so for a $25 credit. Privacy can be bought: but you need to give people a fair price. Think of it as ROPI – return on personal information – and work this metric into your brand planning. Ensuring there is a fair value exchange whenever a consumer provides their personal information not only helps to keep you accountable, but means you can better communicate that value exchange to your consumers.

One of the best examples of balancing data and privacy via a transparent and meaningful value proposition comes from the Dallas Museum of Art (DMA). Last year the museum set up an innovative initiative that offered free lifetime membership (known as being a ‘DMA Friend’) to any visitor who provides their name, email address or phone number when entering the museum. Paying for a service with data is something we’ve grown used to in the online world, and projects like this suggest the model may be growing in popularity offline. Since the data-for-membership programme was introduced in January 2013, the museum has registered more than 50,000 DMA Friends and continues to add more than 1,000 Friends per week. Before free memberships were introduced, the museum had 18,000 paid members.

The DMA programme provides an ROPI that goes beyond free membership. Maxwell Anderson, director of the DMA, says the data the museum is getting about its visitors allows him to prove to donors that their gifts aren’t just subsidising wealthy visitors. Anderson claims this information has helped the museum attract more than $5m in new giving since the policy change. Checking in to activities also earns Friends points they can use for perks like free parking and gift shop discounts. They can earn additional points by identifying works of art they like or bringing friends along to the museum.

4) Storage: end-to-end privacy is vital

On (a virtual) stage at SXSW this year, NSA whistleblower Edward Snowden maintained that even tech firms with business models built on collecting data about their users can operate in a responsible way. ‘It’s not that you shouldn’t collect the data,’ he said. ‘But you should only collect the data and hold it as long as necessary.’

Holding people’s data longer than necessary isn’t just encroaching on their privacy, it’s exposing you to major liability. In 2013, there was a 62% increase in the number of data breaches from the previous year, resulting in more than 552 million identities exposed, according to computer security company Symantec. A major data breach can be crippling for a business, as can be seen from the theft of millions of customers’ payment information from US retail giant Target last December. So far, the company has spent $61m to cover costs associated with the breach, and the cyber attack helped drag the retailer’s fourth-quarter profit down 46%. When the final tally is in, Target’s breach will probably eclipse the data theft at TJX, the parent company of T.J. Maxx and Marshall’s, in 2007, which cost the company more than $250m. The data breach also led to Target’s CEO, Gregg Steinhafel, stepping down in May.

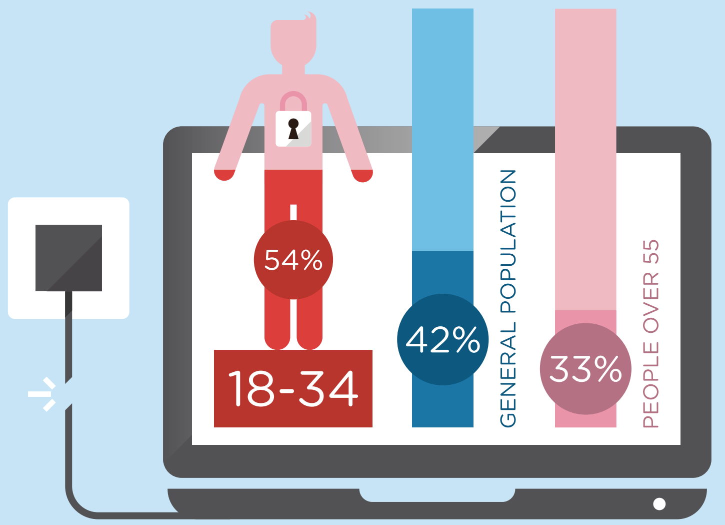
Storage consideration is something secure messaging service Heml.is is thinking carefully about from the outset. The company isn’t just providing encrypted messaging, it’s building its own server software to ensure that privacy considerations are built in end-to-end. ‘One of the biggest problems with mass surveillance is that it surveils everything that pulses through the net,’ notes Heml.is co-founder Linus Olsson. ‘As long as something pulses through the net it tells stories, even though it’s encrypted… That’s the reason we are not doing a federated, distributed system [ie the cloud]. Because giving away that data to either federated servers or distributed servers is, to us, the opposite of privacy. Sure, you need to trust us for not being sociopaths. But if you have a federated or distributed system you have to trust everyone.’

THE FUTURE OF PRIVACY

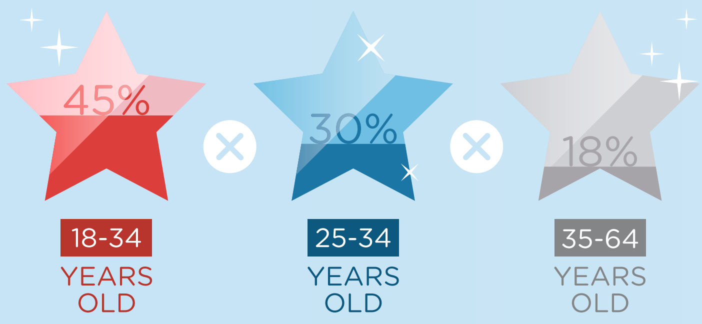
The explosive growth in wearable technology and connected objects is adding increasing layers of complexity to the data/privacy trade-off. Cisco expects that the Internet of Things will result in 50 billion objects being hooked up to the internet by 2020. It won’t be long until the internet-connected SmartClocks in your home really are watching you.

We have grown used to our personal information being the price of access to digital services online, but the proliferation of smart devices in personal spaces like our homes and vehicles is going to spark a new privacy debate that was foreshadowed in part by the anger stirred in some quarters by Google’s acquisition of Nest at the beginning of this year.

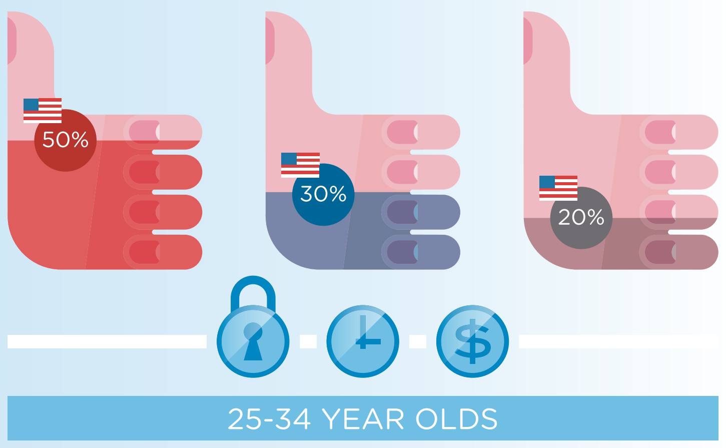
An Englishman’s home might be his castle, but in the future it’s going to resemble something more like a data scientist’s lab. If we’re going to be prepared to navigate the sort of privacy issues this will raise, it is crucial that brands adopt a privacy-by-design ethos sooner rather than later.



54% of people aged between 18 and 34 in the US have stopped using a product because they were worried about the way it was using their personal data. This is compared with 42% of the general population and 33% of people over 55.



Young people are much more willing to pay a premium to ensure their privacy. In the UK, 45% of people aged 18-34 would pay a premium, compared with 30% of the population. In the UK, 25- to 34-year-olds would pay a privacy premium of 30%: a lot more than those 35-64, who would pay 18% more.



In the US, 25- to 35-year-olds are 50% more likely than people over the age of 45 to strongly agree that protecting their online privacy is something they invest time and money in. (30% of 24- to 35-year-olds in the US strongly agree that protecting their online privacy is something they invest time and money in. Only 20% of over 45s say the same.)

TAKEOUTS

MEASURE ROPI

People are often happy to give up their personal data when they’re getting something in return. Privacy can be bought: but you need to give people a fair price. Think of it as ROPI – return on personal information – and work this metric into your brand planning.

MAKE THE VALUE EXCHANGE TRANSPARENT

Having an ROPI established ensures that everyone within the organisation is clear about the value exchange involved in dealing with people’s data. Ensure that this value exchange is effectively communicated to your customers and they are given the option to opt in or out.

DON’T BE AN ASSHOLE

Set your own code of conduct when it comes to protecting consumers’ privacy. When collecting data, focus on earned rather than extracted, and don’t store data just because you can. As John Foreman notes: ‘If as a company all you look at are laws to determine how you treat privacy, you’re going to end up looking like assholes. Legal, maybe, but assholes nonetheless.’

PRIVACY BY DESIGN

Be proactive rather than reactive when it comes to protecting consumer privacy and embed privacy-protecting measures into the design and architecture of your tech systems and business practices. Weaving privacy need-states into the user journey is a key part of this. While it may involve rethinking and redesigning your current systems, adopting a privacy-by-design strategy will prove a competitive advantage in the long term.

Qualitative research was carried out by Flamingo, a global insight and brand consultancy. Research was conducted through an online community of 40 people, 10 each from four generational cohorts (Post Millennial, Millennial, Gen X, Boomer) in the US and UK. This was followed up by eight in-depth face-to-face interviews.Quantitative research was carried out via online surveys conducted by Opinium in March 2014. A nationally representative sample of 2,000 people was surveyed in each of the US and UK.