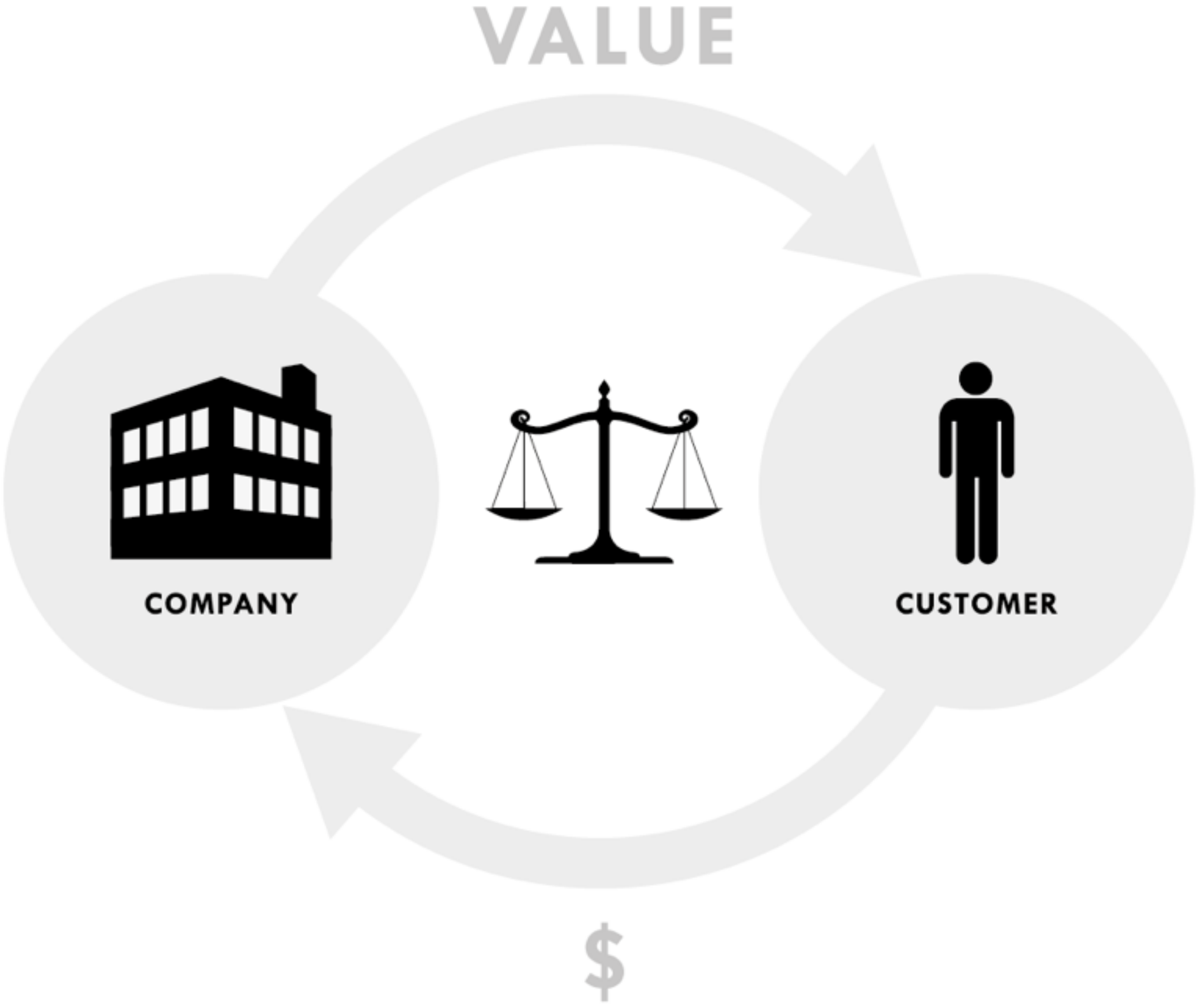
The Data Dilemma: How Can Consumers Trust Brands with Personal Information?

September 22, 2014

IPG MEDIA LAB

You may think of consumer data collection—and the resulting privacy concerns—as “corporate evil-doing”.

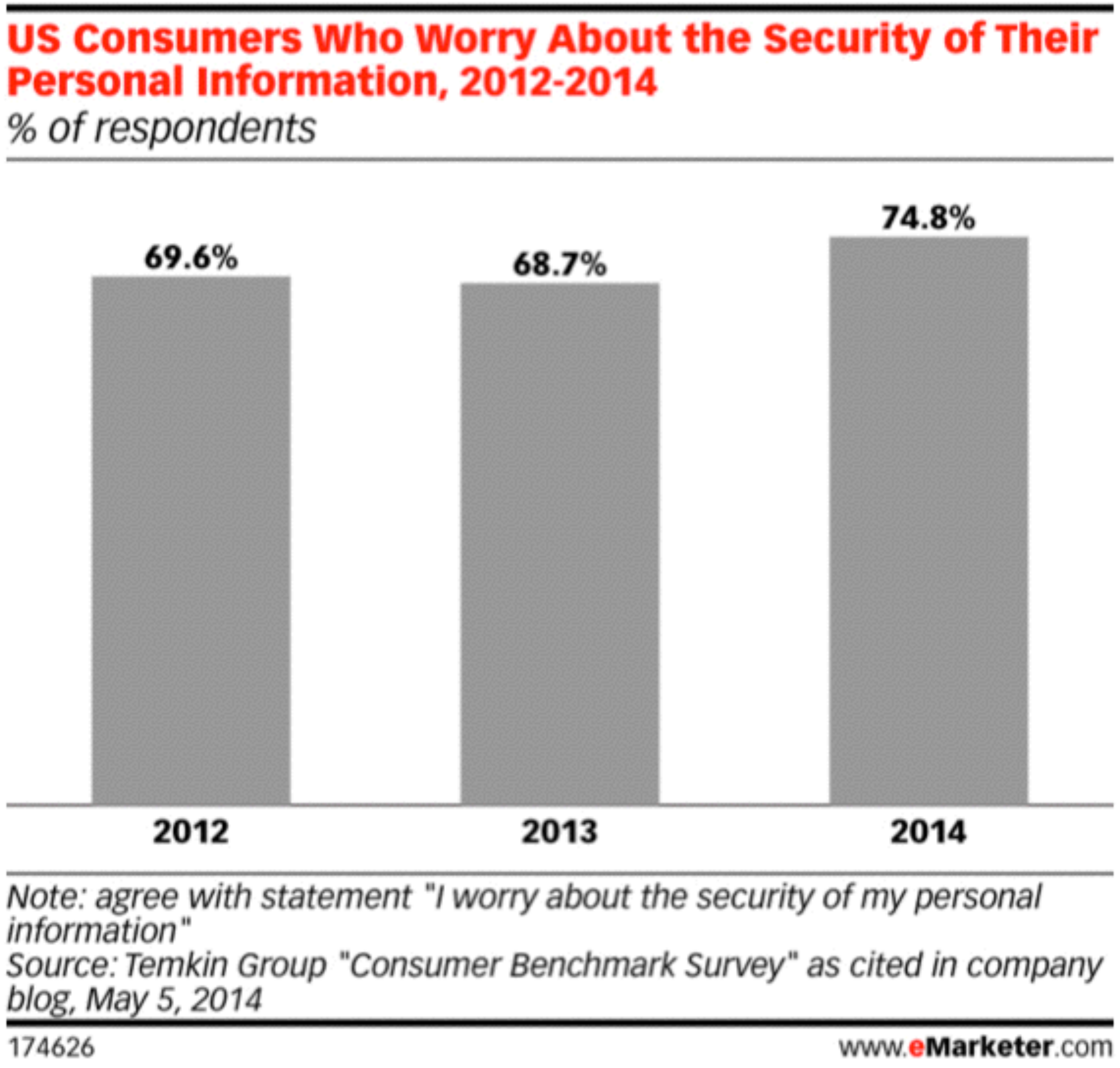
But really, it's just a delicate value exchange that most brands have yet to figure out how to manage



Consumers conflicted over personal information

Even though 75% of U.S. consumers report security concern about their personal data, , 80% of U.S. consumers are willing to give personal info to *certain* brands.

Why? Because certain brands have earned their **trust.**



US Consumers Who Worry About the Security of Their Personal Information, 2012-2014

% of respondents

Note: agree with statement "I worry about the security of my personal information"
Source: Temkin Group "Consumer Benchmark Survey" as cited in company blog, May 5, 2014

174626 www.eMarketer.com

How to win consumer trust

In order for consumers to trust brands with their personal data, brands must actively take steps to ensure that:

- Consumers **consent** to data collection
- Once collected, data remains **secure**
- Data proves **helpful** to both the brand *and* the consumer

It's simple enough, but as the next cases illustrate, some brands fall short of these principles.

No consent, no trust

Facebook recently received a considerable amount of criticism for manipulating 690,000 users' Facebook experiences in order to see if a more positive news feed affected user behavior without ever informing the users nor getting their consent to participate.

Though this "psychological experiment" only affected a limited number of news feeds, it was met with a wave of indignant backlashes, severely damaging the trust of all of its users. Some users even publicly quit Facebook in protest.

In fact, Facebook is now the least trusted social media platform among U.S. college students, according to an eMarketer survey.

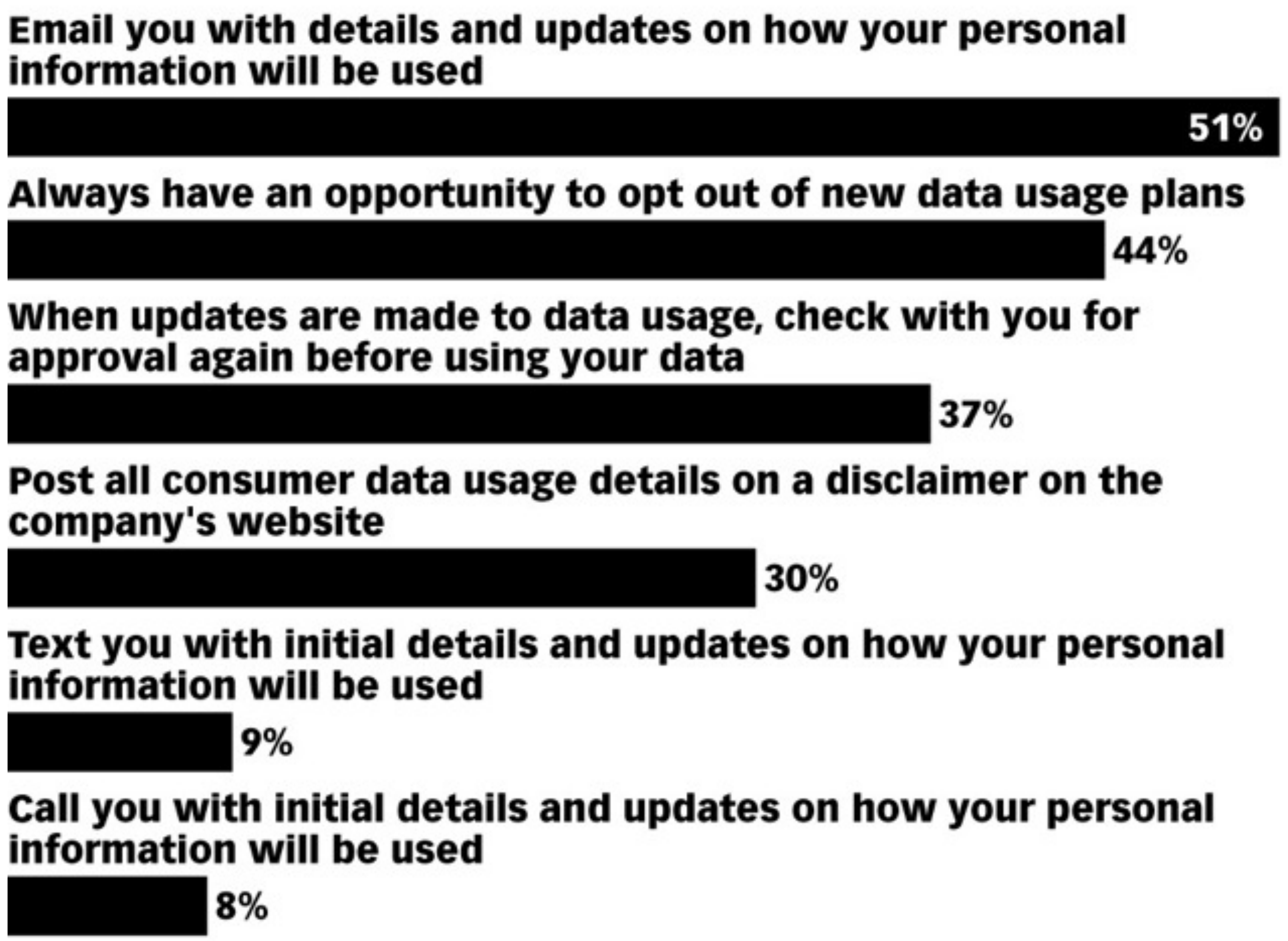
FACEBOOK SHOULDN'T CHOOSE WHAT STUFF THEY SHOW US TO CONDUCT UNETHICAL PSYCHOLOGICAL RESEARCH.
THEY SHOULD ONLY MAKE THOSE DECISIONS BASED ON, UH...
HOWEVER THEY WERE DOING IT BEFORE.
WHICH WAS PROBABLY ETHICAL, RIGHT?

Source: xkcd.com

Give consumers more control

A corollary of consent is control—if consumers can manage their data, they will feel more comfortable sharing information.

Ways in Which US Internet Users Want Companies to Be Transparent About Using Personal Data, April 2014
% of respondents



Source: Accenture, "Eighty Percent of Consumers Believe Total Data Privacy No Longer Exists" conducted by Coleman Parkes Research, May 28, 2014

174525 www.eMarketer.com

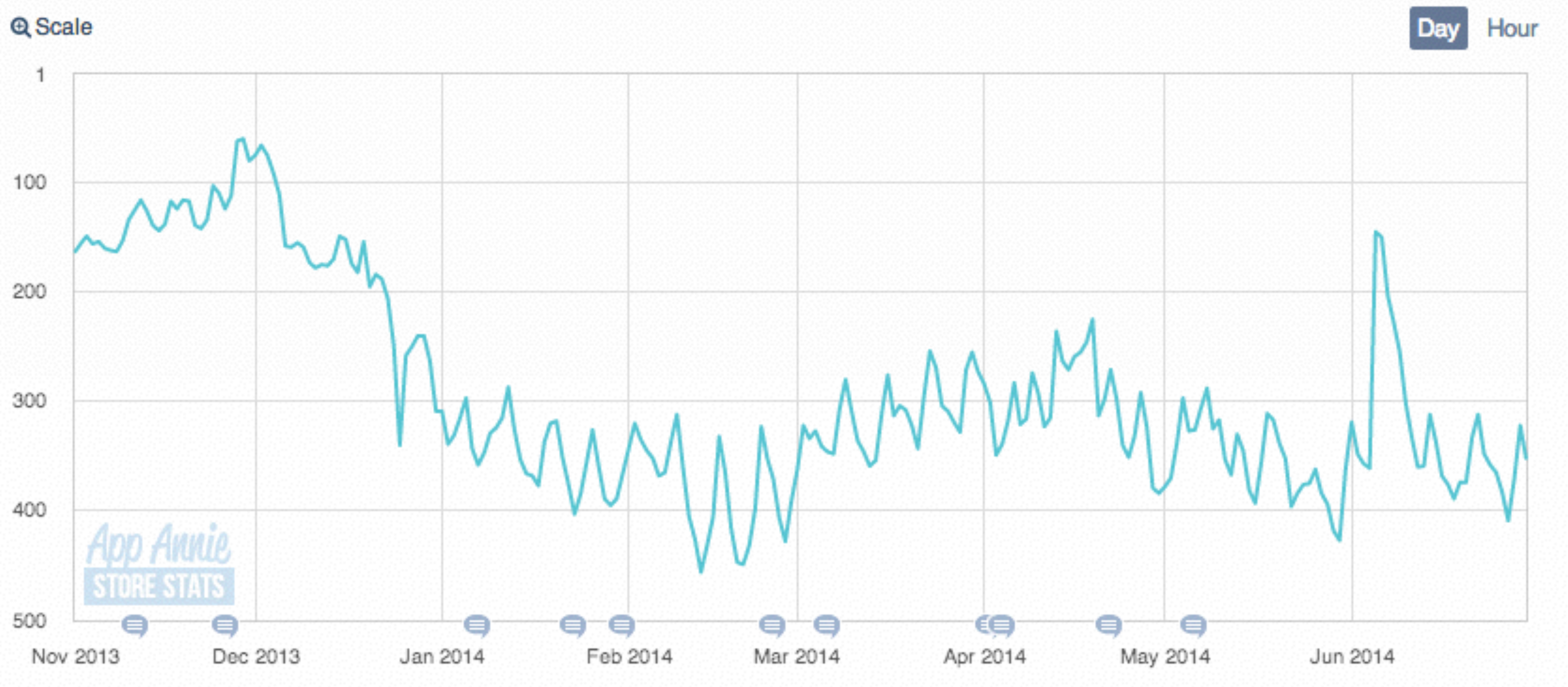
Once collected, keep data safe

Target was caught in a comprising position last December, when a widespread credit card data breach affected over 110 million Target shoppers.

The incident alarmed a lot of previously unsuspecting customers and severely damaged Target's reputation, causing its profit to plunge nearly 50% in its fourth fiscal quarter of 2013, according to Forbes.

Furthermore, data breaches have a ripple effect: if consumers can't trust a brand with their payment data, why should they trust the brand with the personal data that can be used for marketing? Note that Target's iOS app downloads suffered a sharp decline after the news broke (see chart at right).

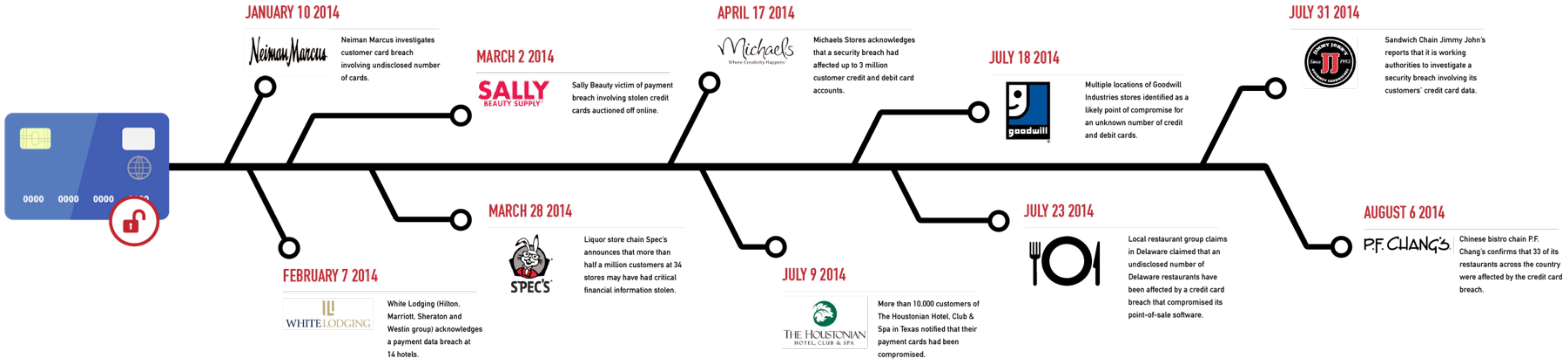
Target iOS App Downloads



Source: App Annie

Don’t be complacent about security

Given how well-publicized the Target breach was, you’d think businesses would learn to be more careful with consumer data. Yet at the timeline shows, businesses continue to breach consumer trust.


0000 0000 0000
Neiman Marcus
SALLY BEAUTY SUPPLY
WHITE LODGING
SPEC'S
Michaels Where Creativity Happens
THE HOUSTONIAN HOTEL, CLUB & SPA
goodwill
JIMMY JOHN'S Since 1983 GOURMET SANDWICHES
P.F. CHANG'S

JANUARY 10 2014

Neiman Marcus investigates customer card breach involving undisclosed number of cards.

FEBRUARY 7 2014

White Lodging (Hilton, Marriott, Sheraton and Westin group) acknowledges a payment data breach at 14 hotels.

MARCH 2 2014

Sally Beauty victim of payment breach involving stolen credit cards auctioned off online.

MARCH 28 2014

Liquor store chain Spec's announces that more than half a million customers at 34 stores may have had critical financial information stolen.

APRIL 17 2014

Michaels Stores acknowledges that a security breach had affected up to 3 million customer credit and debit card accounts.

JULY 9 2014

More than 10,000 customers of The Houstonian Hotel, Club & Spa in Texas notified that their payment cards had been compromised.

JULY 18 2014

Multiple locations of Goodwill Industries stores identified as a likely point of compromise for an unknown number of credit and debit cards.

JULY 23 2014

Local restaurant group claims in Delaware claimed that an undisclosed number of Delaware restaurants have been affected by a credit card breach that compromised its point-of-sale software.

JULY 31 2014

Sandwich Chain Jimmy John’s reports that it is working authorities to investigate a security breach involving its customers’ credit card data.

AUGUST 6 2014

Chinese bistro chain P.F. Chang’s confirms that 33 of its restaurants across the country were affected by the credit card breach.

Sources: Business Insider; Chron; Delaware Online: Krebs On Security: Neiman Marcus & Sally Beauty & Goodwill & Jimmy John’s; Mashable; SCMagazine; PFChang.

IPG MEDIA LAB

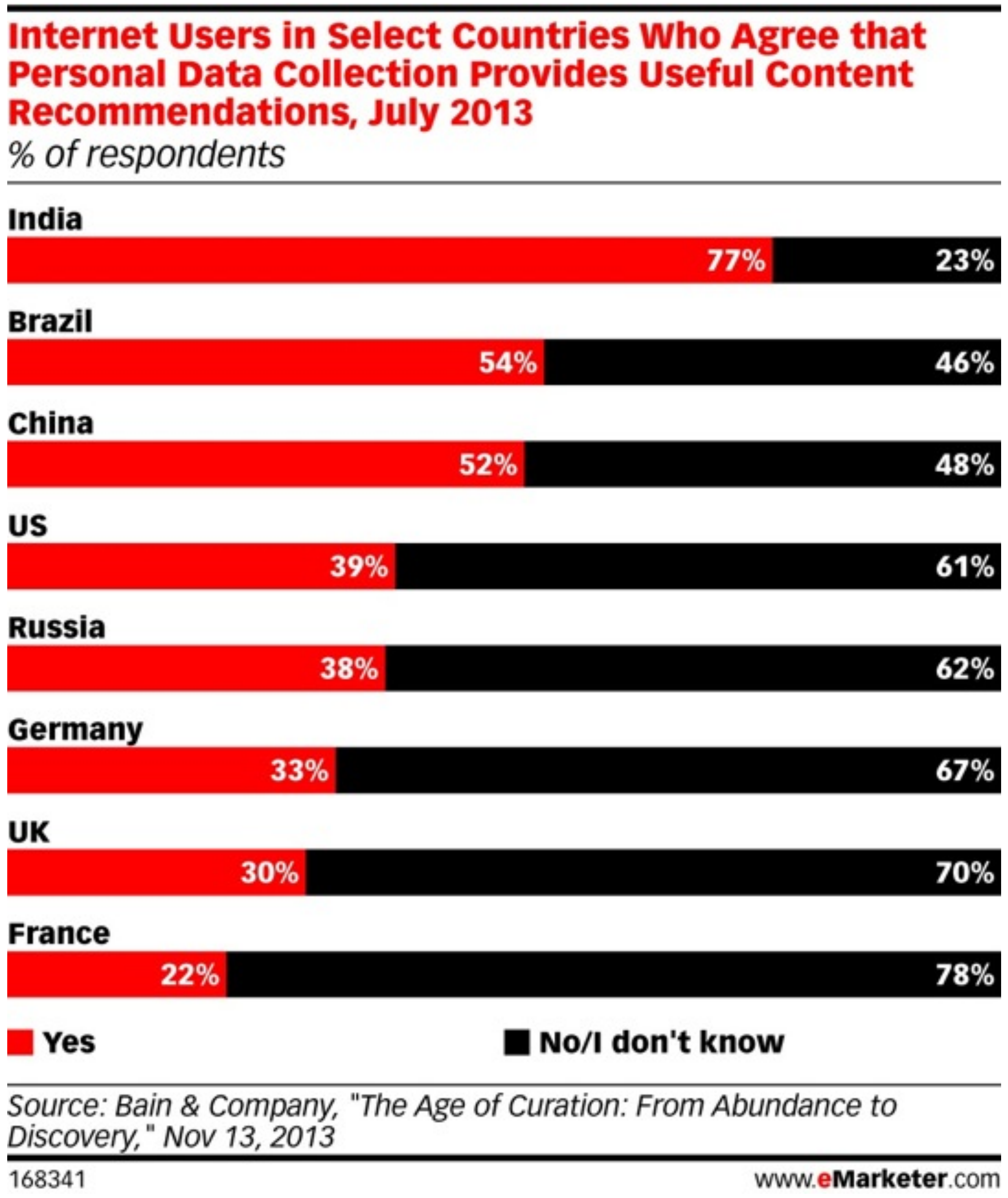
Provide real value in exchange for data

Even if they have technically consented, consumers may not realize exactly how much personal information they are giving away.

For instance, online quizzes popular on websites like Buzzfeed and Zimbio raised concern this year since the seemingly harmless questions actually collected substantial data around buying and technological habits, travel interests, political stances, and more. Although the quiz may provide a moment of fun, the value exchange is highly weighted towards the companies.

There’s plenty of room for improvement

Again, customers don’t mind being tracked if they receive some benefit in return. And these benefits don’t have to be exclusively monetary—“value” can include more personalized recommendations or time savings. According to a 2013 research report by Bain & Company, though, only 39% of U.S. consumers believed they were benefiting from the information exchanged.



Internet Users in Select Countries Who Agree that Personal Data Collection Provides Useful Content Recommendations, July 2013

% of respondents

Source: Bain & Company, "The Age of Curation: From Abundance to Discovery," Nov 13, 2013

168341 www.eMarketer.com

What’s a brand to do?

So, how can conscientious brands make the data-value exchange worthwhile for both sides?

1. Be transparent and get informed consent.
2. Protect data with proper security measures
3. Use data to provide timely and personalized offerings

1. Be transparent and get informed consent

Only informed consent, with the option for customers to opt out, builds trust. Make clear—upfront—exactly what data you intend to collect from consumers, as well as what that data will be used for.

It's not just about using long and complicated Terms and Conditions, but providing information customers can act on. For instance, 500px offers a simplified version of its Terms & Conditions in layman's terms, side by side with the official one written in legal language, to help its users better understand what they are consenting to.

Last but not least, inform customers of updates to your privacy policy. These guidelines are especially relevant for **market research, newsletters, and social media.**

For Your Consideration:

- Are you getting informed consent from your consumers?
- Is your data collection policy sufficiently transparent?
- Can users opt in or out at will?

2. Protect data with proper security measures

To put data security first, brands need to be mindful about what data they collect, and only gather the minimal amount necessary to address their needs. Once gathered, brands must make sure they have enough resources to manage the collected data with proper encryption and other up-to-date security measures.

It is also crucial that brands keep a close eye on relevant legislation and familiarizes themselves with the evolving industry standards regarding privacy, such as the self-regulatory code of conduct issued by the Digital Advertising Alliance (DAA) and the Network Advertising Initiative (NAI). Maintaining high privacy standards is particularly important for **loyalty programs, mobile and location apps, and payment systems.**

For Your Consideration:

- How does your brand address privacy, and is there an internal process to make sure the company is compliant?
- What are the key data points you need to provide value? What extraneous data are being captured that can be eliminated?
- Are you storing the data with up-to-date encryption measures?

3. Provide timely and personalized offerings

Personal data is valuable—otherwise, brands wouldn’t spend so much time and effort collecting it! Put customers’ data to work for them, not just to benefit you. Take Amazon for example. The online retail giant utilizes its data on purchasing behaviors to provide its users with a better online shopping experience with targeted recommendations and personalized offerings. As a result, only 7% of American consumers regard Amazon as a threat in privacy terms.

As in any other marketing effort, think of what problems your customer is encountering, and find ways to make their own data useful. Be particularly mindful when applying this to proximity marketing, loyalty programs, and mobile ads.

For Your Consideration:

- What does “value” mean to your customer?
- Are you collecting data purely for the sake of big data, or is there a true benefit to both the brand and the consumer?
- Are customized offerings being presented in a timely manner?

Thanks!

We hope you've found this POV interesting and provocative. If you have questions or want to talk more about the future of media, please contact us:

ipglab.com
info@ipglab.com
212.833.4751
@ipglab