TEALIUM

Trust is Golden:

How Brands Can Prioritize Privacy in the Age of Data

The 2019 Tealium Consumer Data Privacy Report

Introduction

Brands today know more about their customers than ever before, thanks to a massive, technology-driven influx of data. This technology also has forced consumers, in many ways, to give up control over the information they share. But the way brands are collecting, using, and sharing data is changing by the day. In part, that's spurred by evolving privacy regulations. But consumers themselves are also becoming more savvy and educated, and news about data hacks, breaches and misuse are increasing their skepticism.

Many businesses today focus on data governance with the aim of avoiding financial penalties, especially in the face of the California Consumer Privacy Act (CCPA), which goes into effect Jan. 1 2020, and the European Union's General Data Protection Regulation, which went into effect in 2018. These laws regulate, among other things, citizens' access, transparency, and consent surrounding their personal data. They're also helping drive conversations at both a state and federal level.

The trust associated with data privacy has gained so much clout that it's now a competitive differentiator for companies — notably, Apple, which is taking 2019 as an opportunity to go all-in on data protection. So privacy isn't just about avoiding financial repercussions, but also the arguably costlier impact of diminishing consumers' trust and lifetime brand relationship.

In the 2019 Tealium Consumer Data Privacy Report, we surveyed 1,000 consumers about their relationships with brands and personal data privacy. The resulting insights give businesses evidence of the ways their current strategies are impacting customer relationships, as well as concrete directions for changing their practices and policies to meet modern expectations and build trust with consumers.

- Though most consumers (59%) think businesses are doing a good job handling their data, 71% also say they don't think it's possible to have total control over their own online data.
- 40% of consumers also say that, other than themselves, businesses are the most responsible parties for protecting their data — higher even than the federal government.
- Brands have a lot of room to become more transparent about their data policies. Just over one-third (38%) of consumers say they always read a brand's online terms and conditions; the rest rely on brands to do the right thing.
- While trust is the default, it's also tenuous. Just 15% of respondents are more likely to forgive data-use missteps from brands they trust.

Brands must proactively retain consumers' trust or they risk permanently losing these relationships. CCPA is just the tip of the data regulation iceberg, and it's in brands' very best interest to get ahead of the trends.

Section 1

Why consumers default to trust — and how brands can shore up that feeling.

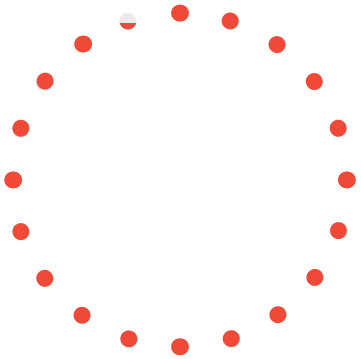
Consumers want data privacy more than ever before, but they simply don't have the time or prowess to educate themselves. Businesses' data practices in general are mired in long, complicated, jargon-filled documents, meanwhile they rely heavily on their consumer data to create relevant experiences. Until there's a problem, consumers trust businesses to do the right thing with their personal information.

Nearly all of consumers are very or somewhat concerned about protecting their data,

and they believe a vast amount of companies have access to their data. Yet, half of them don't feel well informed about how businesses are using their data, and most believe their personal information is being sold online.

97%

of consumers are somewhat or very concerned about protecting their data



39%

More than one-third of consumers believe 20 or more businesses have access to their personal data

Half

of consumers don't feel well-informed about how businesses are using their data

80%

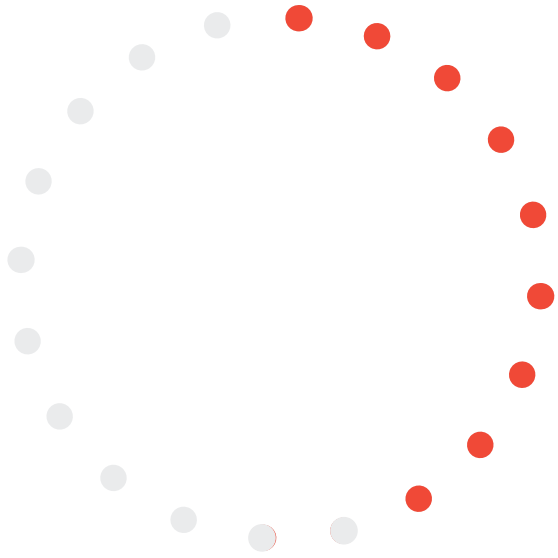
of consumers believe personal information is being sold online

Consumers are right to be wary of companies' approaches to data protection and suspect their data is being sold.

Whether or not data is literally being exchanged for money, consumer information itself is a value-driver. The future of data regulation will prevent data being used as currency, but brands still will need to gather this information to shape personalized experiences. Consumers struggle to see the value behind the data they give up if it doesn't directly result in such experiences.

43%

of consumers would provide detailed data about themselves to a retailer for a discount



32%

would provide this same data in exchange for exclusive benefits or perks

Golden Rules of Data

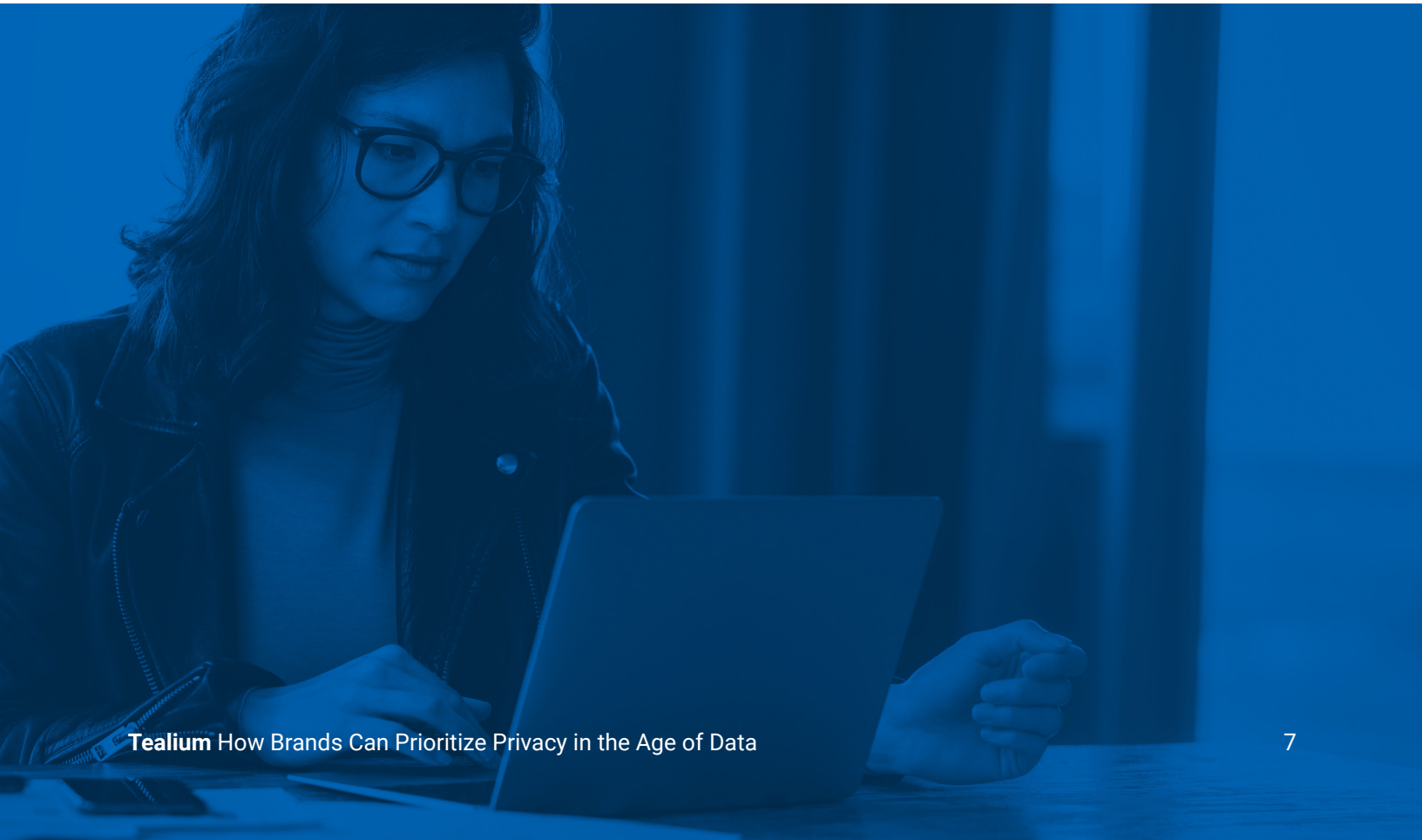
Treat consumers' data as you would want yours to be treated

Think about how your grandmother would react if you explained how your business handles customer data. If this exercise makes you uncomfortable (or if grandma would be appalled) your company likely needs an adjustment in both mindset and practices. It's easy to forget that data represents individual people. Take a step back to reprioritize transparency, communication and trust — in a human way.

Solution 1

Tell the story of how your brand is using data to create a relevant brand experience.

It's an exercise in honesty that shores up consumers' trust in your brand, and helps explain *why* you need their data. Music-streaming giant Spotify is a leader at this practice; it collects data about its 217 million active monthly users every time they listen. But Spotify's customers know the company also is using that data to constantly improve individualized playlists and recommendations, right down to a personalized, year-end microsite.



Solution 2

Rewrite your consumer-facing privacy and data usage policies.

This solution is simple on its face, but it also may be the most difficult one for brands to complete, given the legalese involved. Consumers are starving for companies to explain their practices in concise, straightforward language. Doing so will bolster your company's reputation as trustworthy — the clearer your policies, the less it appears you're hiding something.

- 72% of consumers would be more likely to read these policies if they were shorter
- 61% would read them if they were straightforward
- 45% of consumers want to see examples of how their data is used

Solution 3

Employ tools and eliminate silos to unify your data.

While data silos lead to overall internal inefficiency, they also pose a huge data security risk. Create individual, comprehensive customer profiles for the dual benefit of a unified consumer experience and a lower risk of mishandled data.

Meanwhile, data security and privacy tools ranging from consent and privacy managers to global data centers provide the infrastructure and data governance practices to ensure unparalleled reliability. Your company's use of these tools also should be clearly explained to customers in a prominent place on your website (like your legal and policy page).

Section 2

The brand benefits of maintaining consumers' trust — and the costs of losing that relationship.

When consumers spend money with a brand, they're trusting the service or product they get in return meets certain expectations of quality. Likewise, when a consumer provides data to a brand, they trust the brand will use that data responsibly. But breaking that trust comes with a high price tag: lack of trust cost global companies $2.5 trillion in 2017.

Because companies' products and services increasingly rely on consumer data as the basis of their offerings, a nightmarish future comes into view for those who don't proactively protect data. Consumers want to trust brands they like, and, as our data reveals, they will by default. And once lost, that trust is nearly impossible to regain — 85% of consumers won't forgive a company's missteps, even if they previously trusted the brand.[1]

1 accenture.com

High-profile, high-trust — and high-risk.

Consider two high-profile brands, Amazon and Panera Bread. Both companies have access to an unimaginable amount of consumer data — including payment information — but have handled issues around trust in very different ways.

Continue reading to understand why.

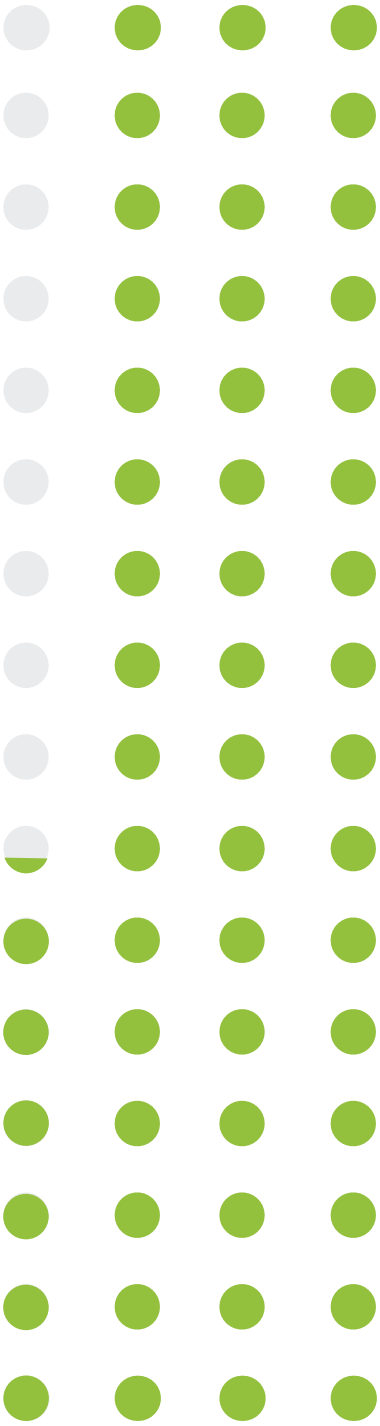
Amazon

U.S. customers: Nearly 100 million

Americans place more trust in Amazon than government, religion, the press, and even Google. Why? Because Amazon delivers on its promises.

"Trust is the function of the promises made and whether they are fulfilled," Brad Stone, a journalist and author, told OZY. "It has promised, very visibly, that when you click and buy something, it will be delivered on a certain date. And it has done an amazing job of fulfilling that promise."

Consumers' trust extends to every aspect of their relationships with Amazon, including data privacy. That remains true even in the face of recent lawsuits surrounding its Alexa voice assistant devices, which underline the evolution of consumer data-sharing to include anything and everything collected via the Internet of Things. And it's likely this trust will continue — so long as Amazon lives up to its core promises.



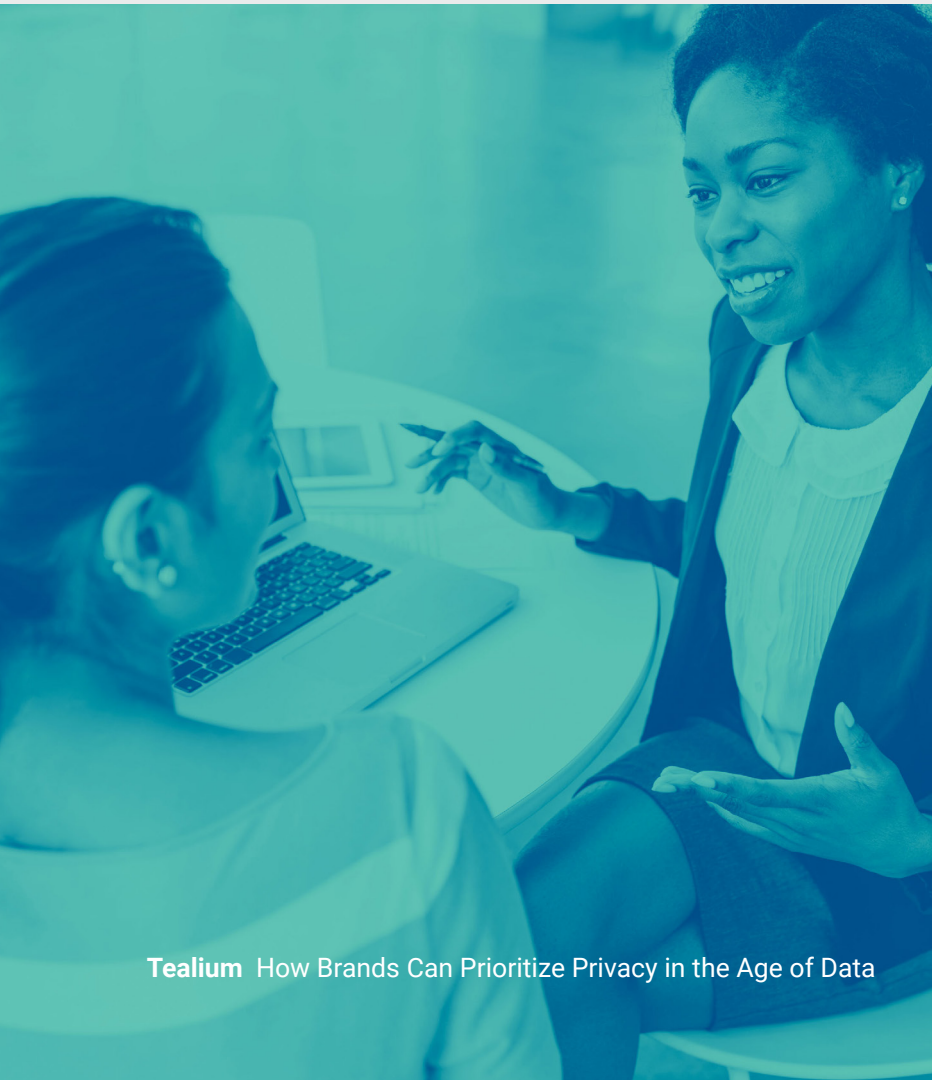
85%

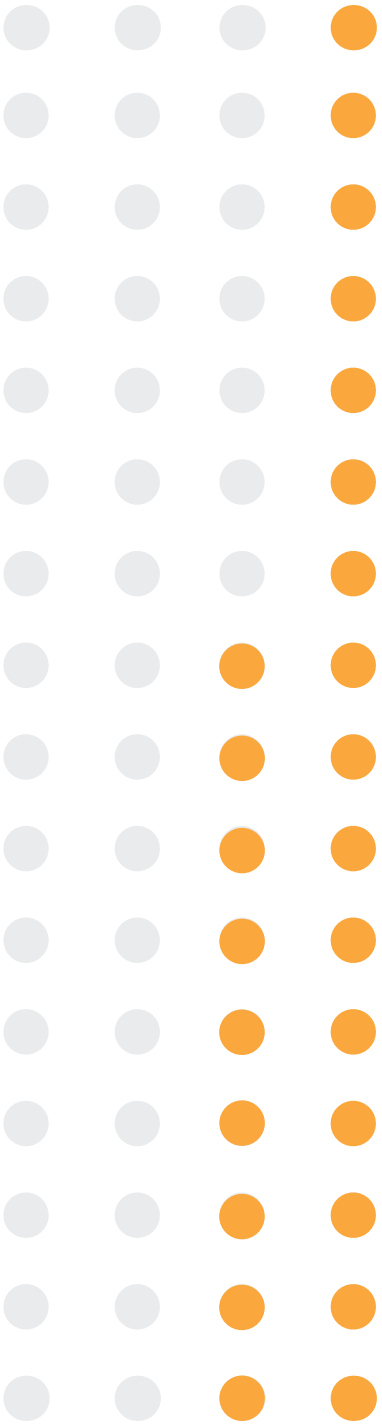
of consumers won't forgive a company's missteps, even if they previously trusted the brand

Panera Bread

U.S. customers affected in online breach: As many as 37 million

Quick service restaurant chain Panera's leak was as obvious as it gets — customer data was available in plain text from the company's website. Yet Panera was aware of the problem for eight months before taking the information offline. A Panera spokesperson downplayed the severity of the leak to Fox News, claiming fewer than 10,000 people had been affected, a number that was quickly refuted by bloggers. The leak may not have been one of the largest to hit the headlines in recent years, but brands and Panera itself still can apply lessons about transparency and reactivity to their future data protection.





39%

of consumers are more likely to rate business's overall data transparency as "fair"

Golden Rules of Data

Transparency, transparency, transparency — throughout the entire customer journey

Consumers are most likely to rate business's overall data transparency as "fair," at 39%. Just 6% thought businesses are doing an "excellent" job.

Under CCPA, GDPR and other potential regulations, such transparency will be the letter of the law rather than the exception. But brands looking to responsibly maintain customer trust now should be upfront about data use, as well as next steps in case it is handled incorrectly. And in order to truly ensure accuracy, companies must maintain a single source of truth for customer data.

One company that could not exist without consumer data, Fitbit, prioritizes transparency around its use of such information. While the company's privacy policy page is lengthy, it's topped by a list of broad topics so consumers can skip directly to an area of interest. Users also can access archived policies and a reader-friendly legal page.

Solution 1

Abide by a new definition of privacy.

During the height of its power, Myspace employees accessed a secret “Overlord” tool that allowed them to spy on other users of the social media network. The tool’s abuses underline an antiquated, all-or-nothing definition of privacy: By sharing information, users have forgone any expectation of protection.

This definition is absolutely counter to the current reality of personal privacy, which contains all shades of gray. Companies need to adjust internal mindsets, then set and abide by their own rules. If a social network user sets a photo to be visible only with his or her friends, that’s exactly what should happen; the same goes for any other private information shared online.

Solution 2

Draft a privacy manifesto.

In the 1990s, Congress modernized the flow of healthcare information with the Health Insurance Portability and Accountability Act of 1996, commonly known as HIPAA. Instead of leafing through inconsistent policies at each provider's office, patients now are met with a universal, one-page consent form. HIPAA turned trust into the letter of the law.

Internet privacy desperately needs a HIPAA form of its own. Most consumers find brands' data security notifications bafflingly complex; fewer than two in five (38%) say they always read a company's privacy policy and online terms and conditions before agreeing to them. As we've discussed, state governments will continue to develop their own data protection laws similar to CCPA. But companies can't wait for Congress to develop a solution that crosses borders and empowers consumers — they need to take the reins and create their own.

On the next page, we'll spell out the ideal features of such a universal data policy.

Designing Your Own Policy for the Future of Data Privacy

While the Obama administration took steps toward a Privacy Bill of Rights in 2012, supported by the Federal Trade Commission, the proposal eventually lost momentum. Since then, little has been done on the federal level to move toward universal data protection for Americans.

But companies can't sit by and wait for Congress to act — such a policy, which we'll call the Consumer Data Accountability Act, is desperately overdue. It needs to be simple and standardized so companies can easily comply, and consumers can easily understand it.

When drafting such an internal policy, include these features:

Employ transparent language to talk about transparency.

Your privacy policy doesn't just apply to your most well-read, tech-savvy customers. So the language you use in your bill needs to be accessible to people from every walk of life. Complicated legalese is not only a turnoff, it's a turn-away.

Allow for access, deletion and correction of data.

To promote consumers' control, ensure the right to access data about themselves, to correct this data, to have it deleted and to take it to another provider. Include these tools in your policy, while also collecting, using and sharing information in ways that protect individuals.

Bake in future flexibility.

The types of data companies are able to collect are evolving on a constant basis, and it's impossible to guess what your company's policy will need to cover in five years. Allow room for changes to be made that reflect politics, consumer demand, and new technologies, and apply a universal approach to the way you handle your entire company's data set.

Use consistent language around privacy, transparency and consent.

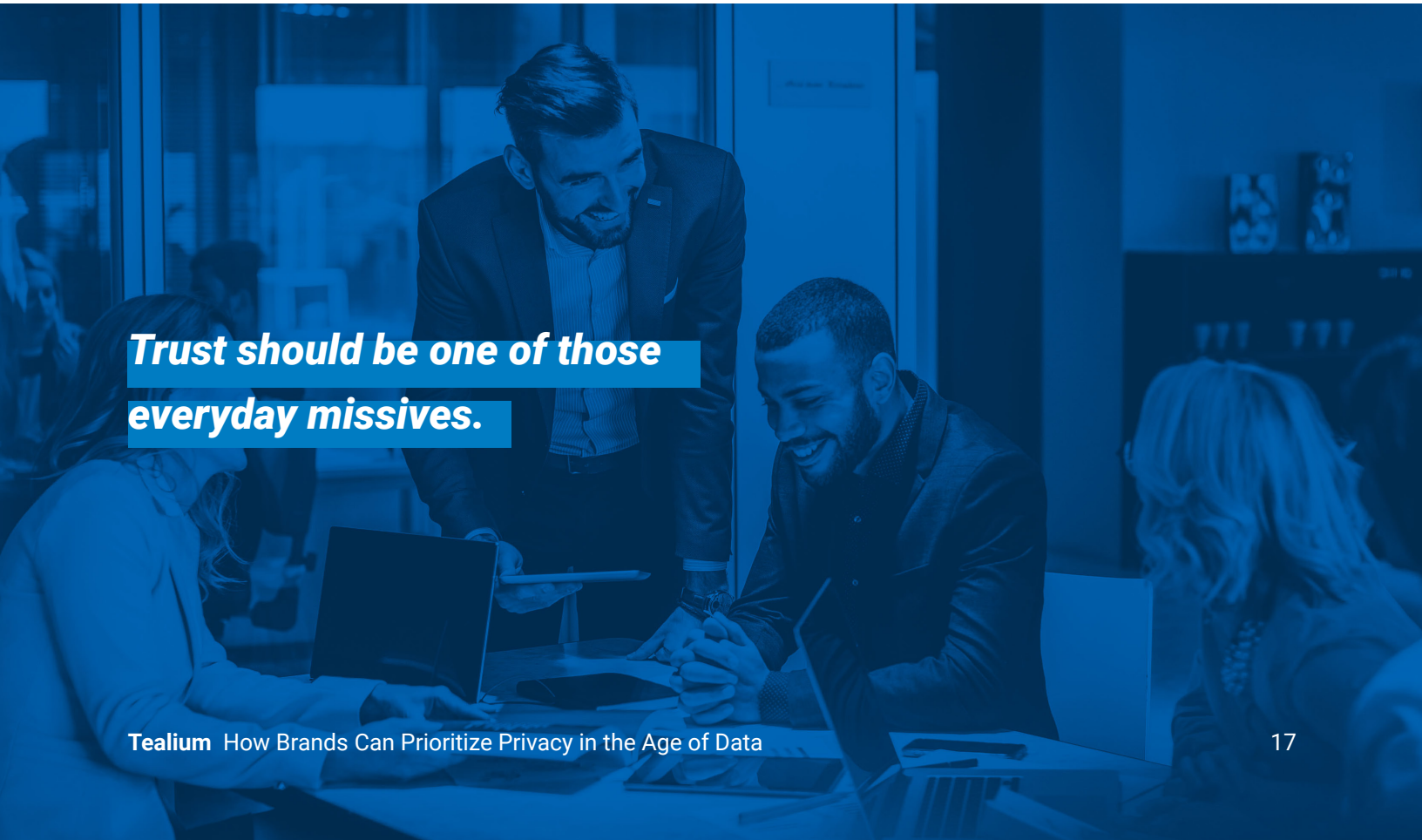
Applying strict, clear guidelines around consent requirements, access rights, and security protections will go a long way toward eliminating confusion.

Solution 3

Remember that trust is a company-wide effort.

Your company likely has a mission statement and a set of core values for employees to rally around. Trust should be one of those everyday missives. Get all your teams, from IT to marketing, on board with your company's stance and messaging around your customers' data and its security from day one.

If trust hasn't previously been a messaging priority, identify internal leaders who can act as a council of data stewards, including security, architecture management, database operations management, data warehousing, and business intelligence management. Also, host internal trainings as needed. Like a strategy to unify siloed data, a company-wide plan to ensure consumer data protection and trust keeps your team on the same page while rallying support.



Section 3

Consumers aren't up to speed yet — but that doesn't mean brands are off the hook.

Trust aside, there is an incredible appetite from consumers for more stringent privacy regulations. In fact, 91% of consumers say they want their state or federal government to adopt strict regulations to protect their data.

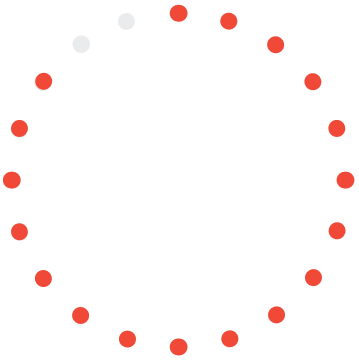
But many consumers also genuinely do not know how data protection works in the U.S., despite having major concerns about data privacy. Two-thirds of consumers haven't heard of any regulatory changes, current or upcoming, that would help protect online privacy, though nearly the same amount also say potential privacy regulations affect the way they vote.

While government regulations are on the rise, consumers still aren't familiar with them.

More than two thirds of consumers have not heard of CCPA or GDPR, and just one in 10 have heard of both. So right now, it's the responsibility of the businesses to educate consumers, manage and communicate data privacy practices and protect consumer data.

91%

of consumers say they want their state or federal government to adopt strict regulations to protect their data

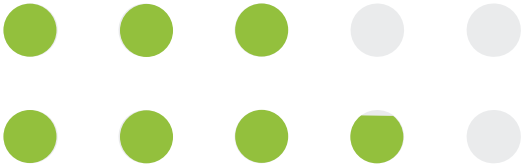


Nearly two thirds

also say potential privacy regulations affect the way they vote

Nearly 70%

of consumers have not heard of CCPA or GDPR



Just 1 in 10

of consumers have heard of both CCPA or GDPR

More data privacy regulations are inevitable in the United States, and brands need to future-proof themselves. And it doesn't matter if customers read your policy page or understand your business's practices — you'll be held financially responsible in the case of mishandled data, no matter what.

Data regulations absolutely aren't going away, and will only grow more complicated before they're universally streamlined. With a strong foundation in place, brands will evolve along with regulations instead of playing catch-up every time.

Nearly two thirds

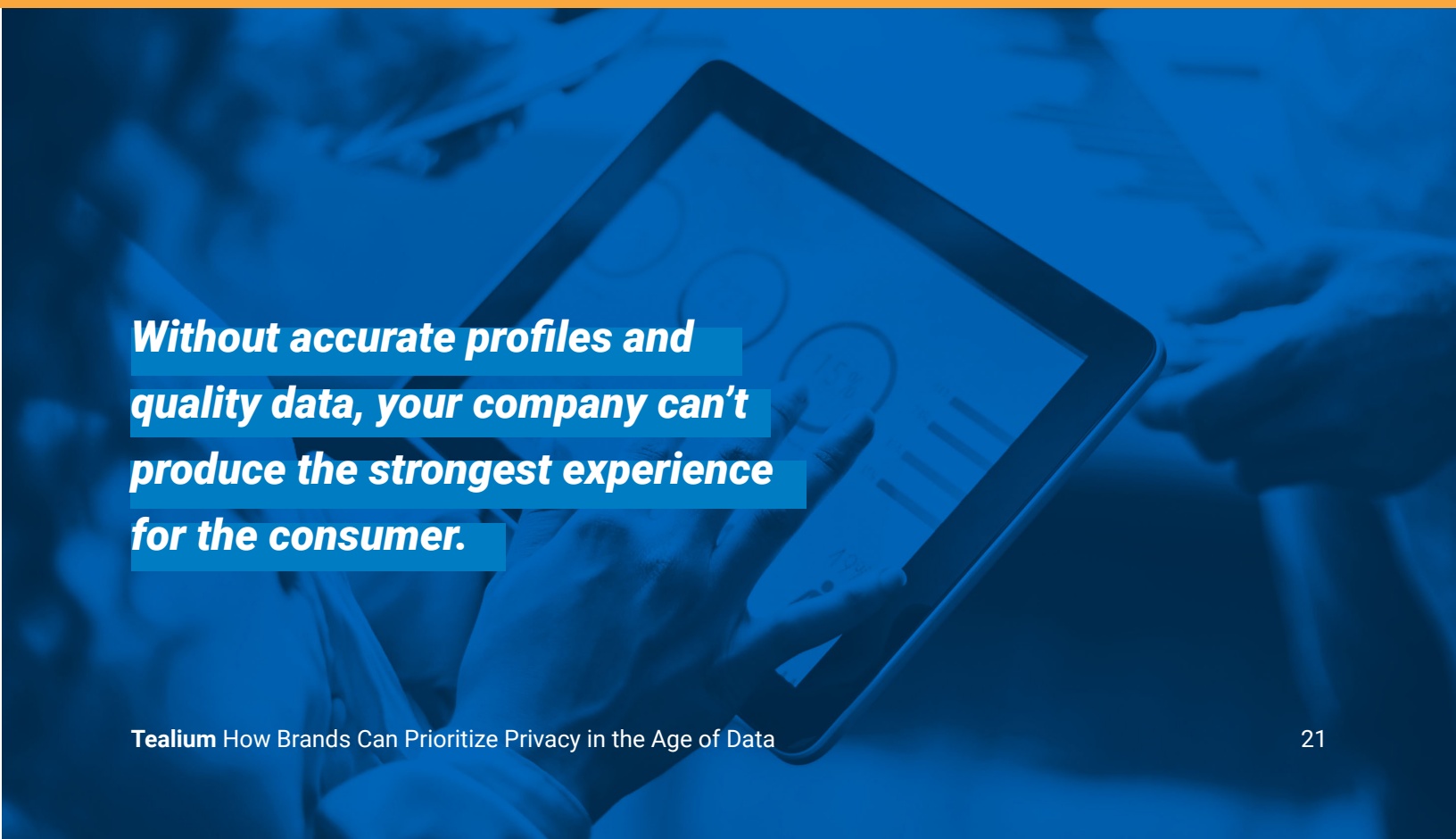
of consumers haven't heard of any regulatory changes, current or upcoming, that would help protect online privacy

Golden Rules of Data

If you can't verify the accuracy or completeness of your consumer data, it isn't reliable.

Disparate data living across technological and departmental silos can create incomplete customer profiles. Without accurate profiles and quality data, your company can't produce the strongest experience for the consumer.

Consumer privacy trends for web browsers will also shape the way your company interacts with consumer data. With access to third-party data sources being phased out by features like Apple Safari's Intelligent Tracking Prevention, first-party data will be the backbone of your consumer profiles. This may make it harder for some companies to create personalized experiences, but it simplifies data privacy practices in the long run.

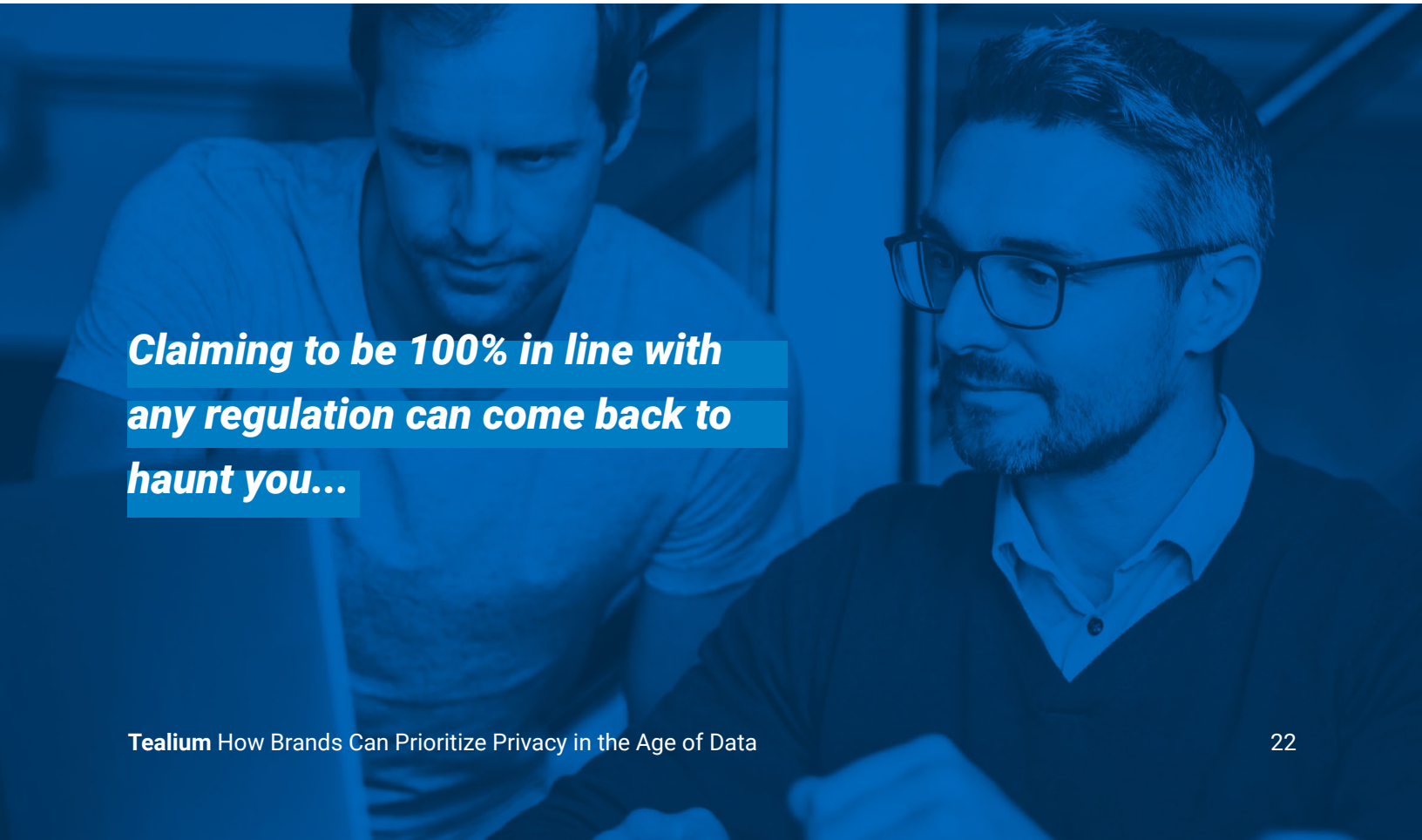


Solution 1

Prioritize compliance — for both the present and future.

Given the number of American brands with EU customers, if you haven't complied with GDPR you need to start now. Not only is your company required to communicate with and handle your European customers' data in line with GDPR's policies, making moves to comply now will set you up for success with other inevitable privacy regulations. Carefully review these GDPR guidelines, especially those related to email communication, and take action soon.

At the same time, your company would be wise not to announce any sort of compliance on your website. Claiming to be 100% in line with any regulation can come back to haunt you, as it's impossible to attain full compliance in the short term.



Solution 2

Use common sense to prepare for regulations.

This solution rolls back to our first Golden Rule: When readying your company for upcoming data regulations, think about the protections you would want for your own data.

Key steps include:

- Create a data map that clearly spells out the data your company has, what you're doing with it and where it's going
- Clearly define your positions around data sales and third-party sharing
- Insert mechanisms to deal with data access and deletion based on individual rights

Solution 3

Be good to your customers.

Yes, it's that simple. Consider the extent of Americans' trust in Amazon — the company delivers their perishable groceries, automatically re-stocks their toilet paper, suggests a new pair of sneakers and listens to and answers their questions about the weather. That reach comes down to trust and delivering on brand promises.

Under CCPA and other compliance initiatives, consumers will have recourse when that trust is broken: data deletion and correction, as well as litigation. Follow our golden rules now, and you won't deal with recourse later.

Conclusion

Today's consumers have succumbed to the fact that data privacy is out of their control, and accept that businesses have and will use their data. But this doesn't mean we live in the Wild West of data. In fact, companies should only expect their access to private information to decrease.

CCPA is far from perfect, and it came to fruition because California consumers were fed up with political inertia. But it's also a manifestation of a growing trend, and the added destruction of accessibility to third-party data enforces why companies need a partner like Tealium.

It's impossible to predict how the data world will evolve. Every time a company turns around, the space has changed, whether due to technology, regulations, or consumers. Tealium's tools empower you to seamlessly manage this change, earn and solidify consumers' trust through transparency and take action to protect their privacy and get ahead of regulations now.

If your company retains anything from this report, let it be this fundamental branding question: If consumers don't trust your brand from a website data perspective, why would they trust you with their money?

Tealium helps companies meet the requirements of data privacy regulations by supplying data governance solutions that give visibility into the collection and usage of customer data, while also supplying tools for consumers to manage their data preferences. Combined with resolving customer identity across channels and devices giving a single view of the customer with Tealium AudienceStream CDP, these data governance tools allow organizations to better see and manage their usage of data to improve performance and mitigate risk. This helps enterprises build consumer trust, enhance customer data and continue to bring innovative customer experiences to market.

To learn more about how Tealium AudienceStream CDP can help organizations comply with the evolving data privacy landscape,

visit tealium.com