celebrus

A shifting landscape:

Revolutionizing the privacy-first customer experience

The idea of treating everyone like a free-spirited consumer who shares data carelessly and loves personalization is very outdated.

Key takeaways

- Increasing consumer privacy expectations are a massive opportunity
- What consumers REALLY want
- The five privacy personas, and how to market to each of them
- Redefining your understanding of privacy and consent
- How to effectively market to opted-out and privacy protected-visitors

Introduction

Marketing is ever-changing, and the current evolution may be the biggest yet. It's also presenting a massive opportunity for marketers to step up and stand out, adapting their focus to be more customer-focused than ever before.

We're experiencing unprecedented changes to privacy and personalization - and increasing consumer awareness about privacy and their digital footprint is driving them. As consumers become more privacy-savvy, and regulators find more holes to fill, organizations must rise to the challenge of adapting to a privacy-focused customer experience.

Contrary to popular opinion, it's not the end of days for marketers. It's an opportunity to do it the right way. And the brands that do are going to be the ones that end up winning against their competitors. This is a huge competitive advantage opportunity for organizations to rethink their entire technology stack and ensure they've got vendors that align with this go-forward strategy.

What consumers really want

It's pretty much a given that consumers want relevant content and experiences. According to Forrester's 2022 Media and Marketing Benchmark Recontact Survey, 34% of U.S. online adults say they're more likely to purchase from brands that share content that interests them - and they're willing to join loyalty programs to get it. In fact, Forrester's Consumer Benchmark Survey 2022 reports that 50% of consumers say they join loyalty programs just to get relevant messages, offers, or promotions. Unfortunately, those same consumers aren't impressed with brands' personalization efforts, nor how organizations are handling their data. Only 22% say the information companies collect on their behaviors makes their online experiences better and 62% of consumers reported being concerned about their online behavior being tracked in 2022.

The problem is that organizations tend to think of privacy in a binary way – you either care about it, or you don't. It's much more complicated than that.

Consider the concept of buyer personas - marketers have been using (and honing) them for years to understand consumer attributes and behaviors so they can create target segments to deliver customized flows and personalized experiences. Yet the attitude towards privacy has been a one-size-fits-all approach. It doesn't make sense. Privacy and consent management is another component of marketing (and a huge part of customer experience) and should be approached just as strategically and critically as every other factor.

In the same spirit, Forrester identified five distinct privacy personas, based on how willing they are to share their personal information.

We dug into these at length in our webinar, Privacy in the customer journey. According to Forrester, the five personas are defined by four different factors:

1. Willingness to share information: Does a loyalty program entice them? Are they willing to sign up for that loyalty program and share some information to get the points and the perks, etc.?
2. Privacy awareness: Do they read privacy policies? Are they aware their information and activities are collected by the sites and apps they use?
3. Comfort with the data economy: Are they comfortable with companies sharing and selling their information? Are they comfortable sharing their location data knowing that it's probably going to be it resold to other parties
4. Protective behaviors: Are they taking measures to limit data collection by apps and sites? Are they trying to limit how much personal information they share?

Understanding privacy personas

The idea of privacy personas have been around for decades, since Alan Westin first began researching it in the 1970s to develop his Privacy Segmentation Index. Although attitudes and concerns about privacy have understandable evolved with the rise of digital, the primary concept still holds true. Consumers tend to fall on a range from low to high privacy concerns based on their level of comfort and concerns. When it comes to digital marketing and personalization, this has a direct correlation with data sharing. Here are the five personas:

1

Low Privacy | High Sharing

The group Westin calls "Privacy Unconcerned", these individuals readily share data, and don't have too many concerns about their privacy. They're also more likely to be comfortable sharing details like location data if they get something in return.

2

Low Privacy | Med Sharing

This persona loves to shop and tends to love loyalty programs. They're into tech, but they're also very privacy conscious. However, they know the value of their data and they're not afraid to use it. While they'll often be the group using ad blockers, they'll also happily share data if you provide value – especially bonuses like incentives and loyalty program perks.

3

Med Privacy | Med Sharing

The middle group is just that, in the middle of the spectrum. They're not incredibly concerned about their privacy or sharing data, but they're not careless with it either. Westin refers to them as "Privacy Pragmatists". They're privacy-aware and typically won't share data if they don't have to – no matter what you offer them. But if they see value, they'll provide the minimum amount of information needed to get it.

4

Med Privacy | Low Sharing

The least tech savvy, this persona is the least aware of the data economy. They want to protect themselves, but don't know how to. Their lack of knowledge often translates to fear, so they'll routinely deny data sharing out of lack of understanding. This group would be likely to abandon an online application that asked for too much information online and might feel more comfortable interacting in person.

5

High Privacy | Low Sharing

The final persona is at the far end of the spectrum – they're highly concerned about their privacy and distrusting of most companies. Westin refers to this group as "Privacy Fundamentalists". They're often the oldest segments and actively limit their data sharing. This group is also the most likely to report privacy intrusions.

Organizations need to expand their understanding of privacy and consent

It's no secret that marketers are facing data deprecation, which according to Forrester is a combination of four forces: Consumer action, Browser and operating restrictions, Privacy regulations, and Walled gardens. As consumers become more privacy aware, and more privacy savvy, they're taking action to protect themselves. At the same time, browser/ operating system providers and regulators are taking note, implementing stronger guardrails to protect consumers. You also have the companies who see the value in the vast amounts of customer data they have and capitalize by putting more restrictions on how marketers use and access that data.

So, what are marketers doing in response to this widespread data deprecation? According to Forrester, 76% said they're collecting more first-party data. Which makes sense, right? When your relationship with consumers is being disrupted by the decisions external forces are making, the natural response is to simply collect the data directly. And that works great with 40% of the privacy personas. But what about the others? Only two of the five are okay with freely sharing their data – more specifically, one freely sharing and one potentially sharing - with exceptions.

And getting legitimate consent is key. Remember, consumers are very privacy conscious, and they're frustrated. Think about how you're going to ask for consent in a way that encourages consumers to give you their data, and in a way that generates trust and convinces them you're doing the right thing and they should continue to share their data with you.

Many organizations oversimplify privacy into just a matter of whether they get consent or not. It's much broader than that. You must consider how you're asking for permission, if you're doing what you say you're doing, if you're acting in the best interests of consumers, and if you're acting ethically.

The rapid adoption of regulations and restrictions has resulted in a lot of brands simply slapping a consent banner on their website and calling it a day, but the approach to consent needs to be thought of more holistically. Enough is enough of operating in silos. The organizations that are going to do this right and avoid negative news coverage are the ones that bring business and technology together - and have compliance at the table when they do it. There's a widespread concern that this will make the organization move slower, but it's not a bad thing to put a little more thought into things like privacy and compliance that come with serious consequences for customer loyalty, not to mention some pretty hefty fines.

While a lot of vendors, especially software-as-a-service solutions like tag management, claim to offer privacy and consent management, the truth is they don't. These third-party solutions are rooted in JavaScript, and they're just hoping their technology isn't blocked by a browser that's already trying to restrict what they can do.

If a vendor can't persist what they're doing because of all the challenges in the marketplace, they definitely shouldn't be managing something as critical as consent.

And consent is about more than a checkbox. Many brands rush to put a cookie banner up and hope that somebody clicks accept, or just reduces it so there's no consent or no confirmation of consent. That's missing the point (not to mention using questionable ethics) - if there's no confirmation of consent, then what are you going to do? Is no confirmation of consent implied consent? What if a person just didn't understand the consent options?

To truly respect privacy and consent, organizations need to approach it with a consumer focus and be transparent in their collection and use of customer data.

What privacy personas mean for personalization strategies

The idea of treating everyone like a consumer who shares data carelessly and likes personalization is very outdated. The privacy personas represent a wide variety of attitudes. And these attitudes are constantly evolving as consumers gain more and more control over their experiences – when they share data, and when they don't share data. Not everyone wants to engage in a world of consented and transparent data collection. And that's ok – but marketers need to understand, accept, and adapt to that reality.

There are two key segments marketers need to be highly aware of, those in the middle ranges of the matrix. These are people with major purchasing power. More than half of each segment are the primary contributors or payer of their household expenses, and 61% of each persona say they're the primary decision maker for household purchases.

They control a lot of the buying decisions, but they're also really hard to reach. They're very privacy savvy and they're the least likely to engage with email ads. Only about a quarter will actually open those ads. Treating these major buyer segments like careless data sharers won't work.

Your interpretation of privacy personas should dictate what you do with your various marketing initiatives. In fact, conducting your own research on your own customers and target markets can provide invaluable insight for you to build your own privacy personas, unique to your business and industry. If you think about campaigns you want to run as an advertiser or as a marketer, they're only going to work for certain individuals because some of them rely on different levels of data being shared to execute effectively. There's also a direct correlation between the perceived value of a perk, and the perceived cost of the data requested. When you find that balance, everyone wins.

When it comes to personalization in your owned properties, like your websites and mobile apps, it's also dependent on what that person is willing to share. That will ultimately dictate whether the things you're trying to do to provide a positive experience for consumers will be effective.

Even more complex, what an individual is willing to share can vary on a daily basis depending on whether they decide to accept cookies or not within a given browsing session. And it most definitely can vary from organization to organization, so while an individual may be willing to carelessly share data on a trusted brand site they've done business with for years, they may be completely reluctant to share anything with a different brand.

People may also behave differently with different brands or find themselves in different personas, depending on how they perceive a brand to be using their data. Especially the savvier personas. If an organization tries to personalize but does a terrible job, or offers a subpar product when they've already purchased the higher- end version, then the perception is that the company is foolish and/or not taking care of their data – so why would they share more?

When dealing with consumers, you're only as good as your last effort as a brand. If you're not a good steward of consumer data, and you end up in the news for the wrong reasons or make a negative personalization decision that upsets an individual, that can very quickly push a consumer from the far left of the scale to the other end of the spectrum with your brand. Worse, it could trigger them to view your competitors more favorably if they've done a better job with their data.

The double-edged sword - consumers want their privacy, but they also want a positive experience

The ultimate goal of marketing with a privacy-first mindset is to walk the line between being helpful and being creepy – without tripping over it. And consumers are the only ones who can tell you where that line is.

Think of it (data sharing) as shining a light in a room. If a consumer is accepting and willing to share data, the room is going to be extremely well lit. As a result, you're going to know a lot as a brand and it's going to present a lot of opportunities for you to interact with that consumer in a highly personalized way.

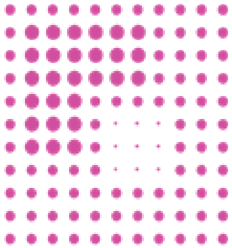
As you start to move down the spectrum from left to right and you get to the more data and privacy savvy consumers, maybe it's more of a warm light - it's not as bright, but it's there. And the expectation from these consumers is that the little bit they're going to share with you will be used in a very positive way. If it's not, they'll turn off the light.

When you get to the other side, the lights go out because these personas aren't sharing anything. Due to fear or cynicism, nothing you do will convince them to give up their data. But that doesn't mean they don't want, and deserve, a relevant experience.

As a marketer, you must think about how to best use the data you have and create a balanced approach. It's not one size fits all, and it's not one size fits most.

If you're not thinking about data from the perspective of Forrester's five privacy personas, you're risking the trust of those personas who might be providing you data without any concern because they love your brand, they feel comfortable sharing their data and there's a perceived value in exchange for it.

You must think through all the levels of consumer privacy comfort and define strategies for what you're going to do in each of those situations - and what you're even able to do from a legal perspective. At the end of the day, marketing is trying to increase relevance, but to increase that relevance, you can't always be on a one-to-one basis, depending on how an individual is behaving or the consent they're providing in that moment. Having a dynamic personalization strategy in place for every privacy persona will ensure you're maximizing every opportunity to deliver a relevant individual experience.



Focusing on data ownership is the key to building trust.

The first step to moving forward with privacy-focused marketing is accepting that third-party data can't be trusted and it isn't reliable. It's the reason we're at this challenging point in time with regulations and restrictions - because third-party data was being shared all over the place without consumers even being aware of it.

Starting from what you own (i.e. true first-party data) gives you better control as a brand, which means your consumers can trust that you know, and you're making decisions on, how that data is going to be used. And they trust they can hold you to that via the various privacy policies and legalese that you might have in front of them.

Many brands are convinced they have first party data, but when they start talking about the process it takes for them to get access to that data it's clear they don't own it and they don't control it - so how could it possibly be first-party? This confusion needs to be addressed in organizations.

Ultimately, true first-party systems are embedded within your environment, are part of your ecosystem, and part of how you bring your channels to life.

Understanding whether your data is true first-party is key when it comes to the regulations and challenges around data deprecation. Look at your technologies and the data sets you have available, think about what level of control you have, how you get access to it, where it comes from, and the limitations of that data set, then put them into buckets of first- party, second-party, or third- party. This creates your starting point and clarifies what you can control.

You can't build a strategy around the restrictions of your technology

The second step is understanding digital identity. When most vendors talk about digital identity they're talking about when someone logs in. That's a lazy approach - of course when someone signs in you know who they are. It's an easy solution for vendors who think it's worth ignoring a huge portion of consumers just to have a subset of "known" individuals so they can say they provide identity resolution.

That's not good enough if you want to truly understand consumers and deliver a positive experience. Digital identity needs to be thought of starting from a position of being anonymous. An anonymous individual who's in the far left, who's willing to share data - that's an identity. They're providing valuable information. You don't need to know who they are as a person to know what they're interested in if they're providing that information.

If the approach you're taking today is based on the limitations of your MarTech, most of your consumers are going to turn off data sharing with you because they don't think you care, and they don't think you're being a good steward of their data. When they provide their information to you, they don't want to be asked for it again when they return to your site in eight days. That sends a message that you don't know (or care) what you're doing. And it doesn't matter to the consumer that your system forces you to purge data after 7 days. They only care about their experience.

If you don't have technologies that can maintain an anonymous individual beyond seven days, stitch that automatically across channel and device, and recall those profiles (including the anonymous individuals) in-the-moment, you're going to fail your consumers. You're not going to meet their expectations and you're almost forcing them to go to the right on the privacy persona scale and stop sharing data with you.

To keep people engaged, to build and keep their trust and build that relationship, you must rethink your marketing strategy. You must leverage strategies and technologies that will work in every single one of those categories. So, what does that look like?

For those willing to share their data, it's pretty unlimited. You can capture data across all channels, domains, and devices to build comprehensive identity profiles that fuel your personalization efforts. Just remember to maintain focus on delivering value and using data ethically and logically to create a relevant customer experience.

For more hesitant consumers, the middle of the spectrum, it's important to think about the right moments to customize - i.e., personalize the personalization. Ask the consumer for input instead of assuming that everyone wants full-scale personalization. Look for opportunities to ask what products they're interested in and how you can best serve them. This is especially helpful when you remember consumers have different levels of comfort with different brands.

Even with those concerned about data sharing, you can still deliver a relevant experience. If somebody opts out and shuts everything off, turning the room dark, there's still an opportunity to present that individual with reasons they might want to share something with you later in the journey. Presenting them opportunities to inch back in as you build their trust doesn't have to be all or nothing. It just has to be really well thought out and educated from a brand to consumer perspective.

If you want to maintain your relationship with consumers, it comes down to respect and compliance. This includes respecting that behaviors and preferences may change across different channels and devices. The same individual who opts in on their laptop may block everything on their mobile.

The technologies you're using to capture data or to contextualize those experiences must be able to manage that. They must be able to change how they're behaving in-the-moment, remember that, persist it, and really embrace privacy restrictions.

What do you do as a marketer or advertiser when the lights go out?

When you have visitors who've turned off all data capture, the ones that don't want to share data, what do you do? In one environment in Europe, a client indicated that their consumers opt out of tracking one way or another over 60% of the time.

For a marketer, that's a massive challenge.

What are you going to do when you don't know anything about those individuals, and you can't capture information? A lot of people have written about a cookieless future, and cookieless technology, but when you drill into it and you start reading it, it still sounds a lot like a cookie – because it is. No one has been able to deliver a solution. Until now.

Celebrus CX Vault is a true cookieless solution – no BS.

If you go to a website where Celebrus is deployed and the customer has this functionality running, when you opt out of tracking the opted-out session begins on that website or mobile app, and Celebrus does two things:. We completely sever the connection, and we put a vault in your device for that session, for that domain. That vault contains two things:

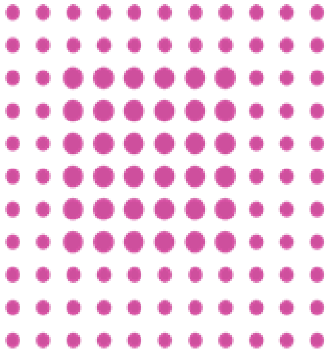
1. A list of machine learning algorithms that run based on contextual relevance. Insight is gathered from the session as you journey the website or the mobile app, as you look at products or add things to your cart, or perhaps interact with forms or watch videos and other content. The machine learning models that CX Vault provides out-of-the-box create signals.

These aren't individual signals. They're just signals of interest and intent based on the content you're consuming which is then paired with a ruleset.

2. A ruleset that states that if certain signals happen, an action should be taken. Maybe it's showing a certain page or directing you to a certain channel. Maybe it's showing you a personalized experience where content is pre-sorted in a different way to show you something you care about. But everything, including the algorithms, ruleset, and activation, happens within the device.

The critical piece is that as all of this is happening, the data is never captured, never shared, never stored, and cookies are never set. It's entirely managed by the consumer on their device for that channel on that domain. It doesn't remember who you are. It doesn't build an identity. It doesn't even put a cookie or a device ID on the device.

It runs completely severed and provides an opportunity for any brand to be able to take that segment of people where the room is dark, and at least try to guide them to whatever it is they're interested in. This is patented. It's the only true cookieless solution in the space today that actually puts privacy first.



The brands that embrace privacy-first will be the winners

At the end of the day, you've got five privacy personas and you must create solutions for each one because all of them, regardless of how they feel about data sharing and privacy, still expect to have a good digital experience with you.

Brands and marketers have been treating everyone as if they're willing to openly share data and love personalization. In reality, this approach is fine for about a third of US online adults but leaves the two thirds who don't love hyper-personalization out in the cold.

Remember, it doesn't have to be all or nothing. Done right, brands can help graduate people into different categories for different types of things they're interested in.

Marketing has never approached strategy as if all consumers are in the same bucket when they build personas or segments for targeting, so trying to do that with consent doesn't make any sense. It's much more effective to overlay these privacy personas against a marketing strategy that ensures you're doing whatever you can for each of them. And over time, you can also figure out what persona your ideal consumer base generally tends to fall within.

It's pretty easy to get to this level of privacy-focused personalization if you think about it as a journey of getting to know consumers with a compliance-first mindset, then use that to dictate how you interact with those individuals and how you can add value regardless of where they fall on the privacy spectrum. It doesn't always have to rely on data collection and sharing that information – you can provide a relevant experience while still completely respecting privacy.

Supercharge your CX with Celebrus

Many enterprise organizations around the world use Celebrus from D4t4 Solutions as an integral part of their data driven CX infrastructure because of how easy the solution is to deploy – a single line of code to be exact. Celebrus is 100% laser-focused on data capture and is constantly innovating and staying ahead of the curve.

Data captured by Celebrus satisfies privacy regulations including GDPR, CCPA, and more, providing peace of mind across global businesses. And with native consent management and compliance, clients can breathe easy while delivering highly personalized customer experiences at scale.

As the first data capture solution to combine advanced machine learning (ML) with natural language processing (NLP) and real-time data capture, Celebrus enables enterprise clients to have total visibility of customer behavior, arming them with powerful insight into customer intent, to deliver genuine, individual-level experiences - for ALL visitors. With out-of-the-box machine learning and patented first-party data capture, Celebrus removes the configuration headaches and costs typically associated with capturing behavioral signals.

Offering patented capabilities, like cross-domain continuance and CX Vault for opted out visitors, Celebrus powers the ultimate flexibility in delivering relevant, real-time personalization by shifting marketing activities from reactive to 'in-the-moment'.

Ready to see how a genuine first-party data capture solution can solve YOUR identity challenges?

CONNECT NOW

Connect now and book a demo

celebrus

www.celebrus.com | | in