



Modern Product Management

Part 3: Data Privacy + Looking Forward

A TAPLYTICS GUIDEBOOK





Modern Product Management

Part 3 - Data Privacy & Looking Forward


In the final section of this guide, we'll highlight the importance of data privacy. We'll look into what data privacy is and how it impacts product owners, the history of privacy regulations, and product strategies for the post-privacy era. Finally, we'll explore how the future of product is privacy first.

What Data Privacy Is & How It Impacts Product Owners

Microsoft. Zoom. FaceApp. Cambridge Analytica. All four companies have been at the center of serious data privacy and security concerns over the past two years. Some survived, while others did not. And they're not alone—every year, there are more and more reports of companies mismanaging valuable customer data. Whether they're not following regulatory guidelines to secure data or are running into rapid scaling issues amidst a global pandemic, one thing is clear—data privacy is a big issue.

So big in fact that, according to [Cisco's 2019 Consumer Privacy Report](#), 84% of consumers care about data privacy and seek more control over their data. But only 57% think they can adequately protect that data on their own. That's why it's so important for modern companies to have a handle on data privacy and security.

Modern consumers expect a certain level of personalization whenever they interact with your brand and products. And that experience requires access to a lot of customer



data. But with all this data comes great responsibility—consumers are savvier than ever regarding the value of their personal information. Ensuring data privacy is no longer a differentiable feature. It is table stakes for every company.

Failing to secure sensitive data will have a significant impact on the customer relationship. So, communicating your company's commitment to data privacy is at the core of:

- Your relationship with customers
- The perception of your brand
- Your liability to consumer litigation or regulatory oversight

This is a fundamental shift in the structure of relationships between companies and customers. Pervasive access to customer data changes the way companies compete. You can't rely on a strong product offering any more. Your ability to capture revenue is built on relationships. And those relationships are built on data.

We'll take a look at what data privacy and security mean for modern companies, how the privacy landscape has changed over time, and what happens if you don't keep your customers safe. From there, we'll make recommendations based on [Taplytics](#)' own experience building a privacy-first platform and provide proactive solutions you can implement for your customers and your team.



What Is Data Privacy & How Does It Impact Product Owners?

Having a strong data privacy and security policy is one of the most important things you can do as a company to build trust with customers. A [2019 Pew Research report](#) found that 81% of Americans think the potential risks of companies' data collections outweigh the benefits. Part of a product manager's job is to ensure the data we collect is only used to make a users product experience better.

To do this, it's crucial to showcase the immediate value of collecting customers' personal identifying information (PII) and contextual behavioral data. When you have access to so much data, you can use it to build better products, target people who will benefit the most from your product, and create an experience that builds trust and loyalty over time.

And you can't do that when consumers are worried about whether or not their personal data is safe.

Understanding how to manage customer data privacy and communicate your policy with customers helps build stronger relationships without sacrificing trust. Your customers want to see that you're using their data to make their lives easier through your product, whether that happens during their experience with your product or with the content surrounding it.

What Is Data Privacy?

Data privacy is an aspect of [data security management](#) that establishes best practices for the proper handling of valuable customer data. Think about it as the umbrella for everything related to the collection, storage, and usage of customer data and personal identifying information (PII).


The term covers many different aspects of how consumers and companies manage data, including:


- The way companies collect data from customers.
- What first- and third-party sources interact with customer data.
- The way data is stored and which employees have access to it.
- When and how customer data is shared with other tools.
- The level of control consumers have over their personal data.
- How companies communicate the way they collect customer data.
- Compliance with privacy regulations like [GDPR](#), [HIPAA](#), [GLBA](#), and [CCPA](#).


Each piece of data you collect from customers contributes to the overall understanding of how those individuals interact with your product and your brand.


Understanding Customer Data & PII

We talk a lot about using customer data, behavioral data, and personal identifying information to create relevant and personalized experiences for customers. It's important to understand what we're referring to when we talk about this kind of contextual data.

 **Customer Data:** This is the overarching term for everything related to how customers interact with your product and your company. It includes their personal information, demographics, and behavior. This data is how you contextualize the user experience.

 **Behavioral Data:** A subset of customer data, behavioral data focuses on the interactions between customer and company. Whenever someone clicks on a link, makes an order, or sets up a process in their account, that's another piece of behavioral information you can use to learn more about the customer.

 **Personal Identifying Information (PII):** Also a subset of customer data, PII is the data you collect from customers that is specific to an individual, like their



name and contact details. Basically, it is anything companies use to identify specific customers and differentiate them from others.

As you learn more about data privacy and security, it's important to understand how integral the process is for many of the underlying drivers of your company's growth. Being able to secure your customer data is one of the keys to scaling your company and building a better user experience without impacting your relationship with customers.

How Data Privacy Affects Product Teams

Data privacy isn't just keeping customers safe and ensuring compliance with laws and regulations—it's how product teams safeguard one of their most valuable assets. Product teams use customer data to make smarter decisions about what they build, personalizing user experiences, and the results they expect. When so much of the relationship with a customer is built on personalized experiences, failing to keep customer data secure can have a direct impact on your bottom line.

The more relevant data you have, the easier it is to build products that are relevant to your audience. Instead of guessing at what would bring value to your customers, you'll know exactly how to position your product in the market.

Modern consumers expect a certain level of personalization as a part of their experience with your brand. Customer data is how you create these experiences. And each additional data point is a building block in your understanding of actual customers.

As you learn more about customers, you'll be able to create more robust and personalized user experiences for each different kind of customer you have.

Most customers have an implicit understanding that companies collect this kind of personal data about their experiences with brands, products, and content. But they

don't often understand the extent to which that data is used. Your job as a product manager is to manage their data in a safe way that manages, stores, and uses customer data in a secure way.



Example customer persona with various data points.

When you do this, it builds trust in your company and customers. This leads to savvy consumers who understand that allowing access to their PII and behavioral data can lead to a more relevant and, ultimately, more useful relationship with your product and your company. Just keep in mind that as strong as this relationship may be, any perceived breach of trust or lack of communication will have a lasting negative impact on this relationship.

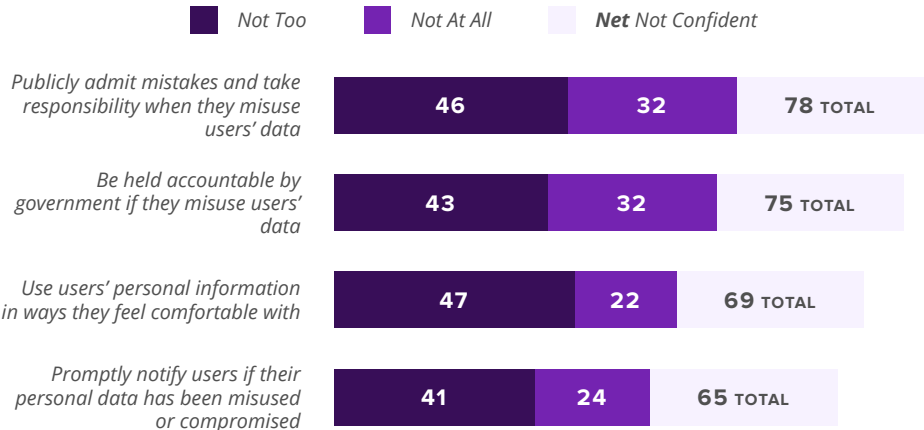
When consumers are more concerned than ever with how you use their data, data privacy needs to be your primary concern.

What Product Management Looked Like In A Pre-Privacy World


Before consumers were as privacy-conscious as they are today, companies, more or less, had free rein to do what they wanted with customer data. This led to a number of practices that negatively impacted data privacy standards. While many companies are still using similar methods today, product management was a very different experience for your company and your team.

In the pre-privacy market, companies relied on third-party tools to gain cheap or free access to consumer data. They leveraged these tools to create the kind of contextual and personalized experiences customers have now learned to expect. But using free tools like [Google Analytics](#) impacted their ability to maintain data security at scale because these companies didn't have complete control of the data they accessed through third-party tools.

Most Americans are not confident that companies would publicly admit to misusing consumers' data. Here are the %'s of U.S. adults who say they are ___ confident that companis will...



Note: Those who did not give an answer or who gave other responses are not shown.
Source: Survey conducted June 3-17, 2019. [Pew Research Center](#)



As these tools became more ubiquitous and more companies started using them, the potential for data breaches and loss of valuable information became more prevalent. This led to more concerned consumers and an overall lack of trust that companies had their best interests at heart.

In fact, according to the Pew Research Center, only 35% of consumers believe companies would notify them if issues occurred. That's a staggering lack of confidence you have to overcome to even start building trust in your brand.

Relying on these tools and practices also led to a lack of oversight and understanding of data privacy for many companies. This lack of control put the customer relationship at risk, and that risk increased when bad practices led to issues with how data was monetized.

Basically, companies could use, sell, and share PII and customer data freely as long as it served their goals. There was no need to vet tools for security—only for usability and price. The analytics and data management tools could also set their own terms when it came to how they used data.

As a result, customer experiences were built on poor data management and signaled to customers that, while they benefited from personalized experiences, they couldn't really trust the companies that created them.

Data Privacy Helps Build Strong Customer Relationships

When you have a solid understanding of how data privacy impacts your relationship with customers, it makes providing those customers with a great experience easier. And communicating your commitment to privacy also increases the level of trust between company and consumer.



Next, we'll talk through the history of privacy regulations, highlight how data was monetized, and address the impact of that process on consumers. We'll also touch on why there is a need for more security, especially for enterprise businesses, and how changes to privacy best practices impacted businesses and consumers in every market.



The History Of Privacy Regulations

We talked through what data privacy is and how it impacts your company. Now we're going to look at the underlying drivers that make data privacy such an important issue for your brand—specifically, privacy regulations.

Let's start with a little context. According to a [2019 CISCO study](#), 45% of consumers think the federal government should be responsible for protecting data privacy. And 21% think that responsibility should fall with the companies managing the data. This puts the burden of keeping customers safe squarely on our collective shoulders.

Being able to keep your customers safe takes a considerable amount of insight into how data-privacy regulations affect your business. While there isn't any federal-level legislation in the United States, there are statewide and industry-specific laws that everyone needs to pay attention to, not to mention international regulations. This makes positioning your company as a privacy-first organization very important.

Let's take a look at how these various data privacy regulations evolved over the past 50 years and talk through how they came to be such an important part of doing business online.

Why We Needed Data Privacy Regulations

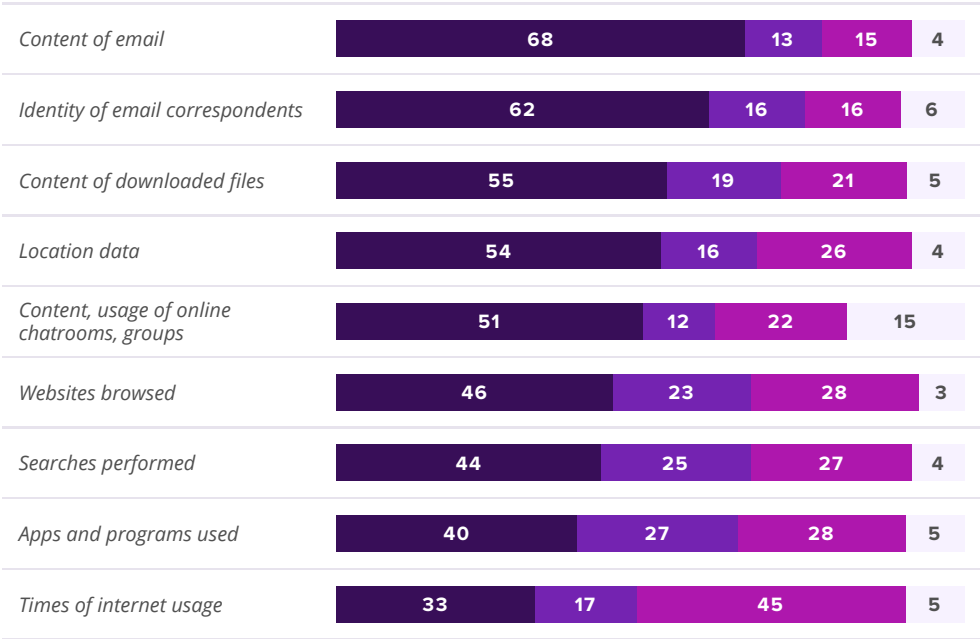
As consumers moved more and more online for their work, commerce, and entertainment, their digital footprints expanded, and they left more data behind. With so much access to different types of data, companies in the early aughts learned to rely on contextual information about their target customers to build their products. When this reliance is paired with an overall lack of oversight, everyone's privacy and security was at risk.

Increased access to consumer and market data shifted focus from product marketing to experience marketing. Instead of consumers seeking out local businesses to make their purchases, they relied on ecommerce platforms like Amazon to provide them with a seamless and convenient purchase experience.

And these experiences were built on data. So, access to that data became a competitive advantage. As soon as access to customer data became a primary driver for overall business success, monetizing this data soon followed. It was easy to see that companies with more access to contextual and behavioral data had a better chance to succeed than those that didn't. This increased consumer concern for the types of data collected, specifically from a digital perspective.

Consumer Privacy & Protection Concerns Vary By Type Of Digital Data:

Very Important Somewhat Important Not Too Important N/A



Relative importance by data type, % of respondents (n = 792)

Source: Internet & American Life Project, Pew Research Center / [McKinsey Research](#)

This increased competition for access to data led businesses to develop bad practices when collecting sensitive information about their customers. These bad practices are exactly what spurred the need for privacy regulations. When you combine this with the fact the consumers were spending more of their time online, it was clear that the privacy landscape needed to change.

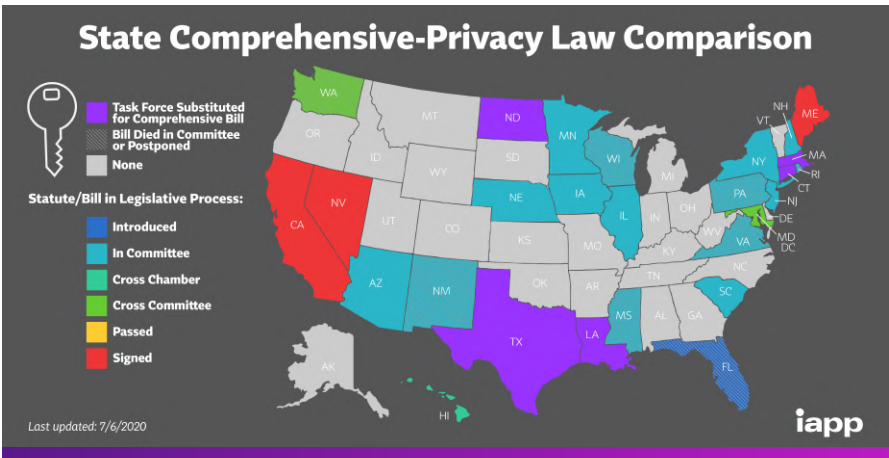
How Privacy Regulations Impact Your Business

Even though the United States doesn't have any federal-level data privacy regulations, businesses need to be aware of how statewide and global laws affect their markets. Whether it's the [GDPR](#) or the [CCPA](#) or an industry-specific regulation like [HIPAA](#), businesses are at an increased risk of issues related to data privacy and security.


Most privacy regulations dictate the way businesses

- Create guidelines for how they safeguard customer data,
- Share sensitive information with first- and third-party sources, and
- Communicate their commitment to data privacy to consumers.

Failing to follow these regulations increases your liability for consumer litigation while putting your customers' valuable information at risk.



Privacy laws by state via [iApp](#)



When you understand which regulations affect your business, you can create guidelines for your team that decrease the potential for privacy issues, like a data breach. We'll talk more about the overall impact of data breaches in the next chapter, but it's important to understand how damaging these issues are to consumer trust and perception of your company.

The rise in regulatory oversight also increases the amount of focus companies need to put on data privacy and security. Ensuring compliance with all relevant regulations requires a sincere time investment, which is only possible when teams have a defined role to tackle difficult security issues. This increases hiring needs for jobs centered on data security as well.

Most of these regulations require companies to share their commitment to privacy as well. While this increased visibility does build trust with consumers in your market, it also opens you up for potential issues if you were to fall short on your promises. This is especially serious for enterprise businesses, whose larger team size and increased access to customer data lead to more potential points of failure.

Sharing your privacy policy publicly also forces you to define how your team interacts with personal identifying information (PII), which gives customers insight into their potential risk. Our's is a static element in the footer of every page.



© 2020 Taplytics Inc. All right reserved | [Privacy](#) | [Taplytics End User Terms Of Service](#)

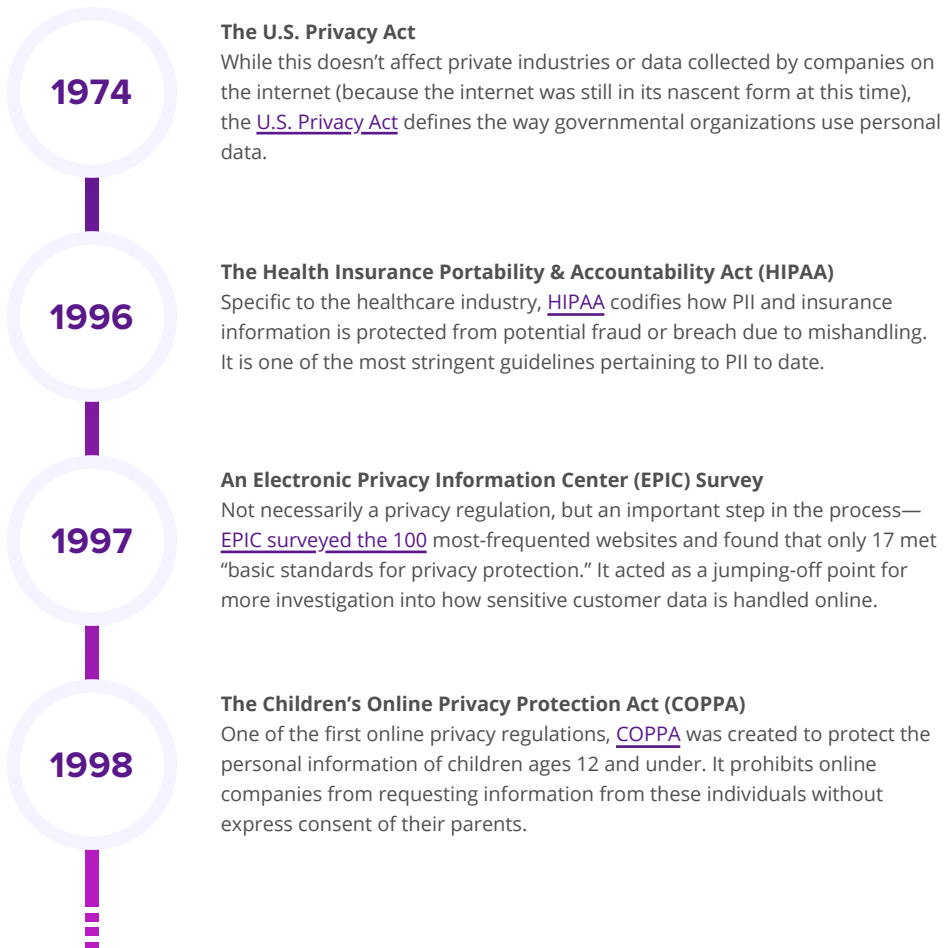
As consumers have become more concerned with their data privacy, you need to ensure that you're communicating your commitment to their security every chance you get.

To understand more about what kinds of regulations you have to pay attention to, let's take a look at the history of privacy regulation over the past 50 years.

A Complete History Of Privacy Regulations

To illustrate how the landscape of privacy laws and regulations have changed over the past 50 years, we've put together a timeline.

Let's start with one of the first privacy regulations in the United States.





1999

The Gramm-Leach-Bliley Act (GLBA)

While the [GLBA](#) is much more than a privacy or data security law, this financial regulation does include specific requirements for how banking institutions collect nonpublic personal information, which the regulation defines as “information collected about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available.”

2001

Guidelines Establishing Standards For Safeguarding Customer Information

These [now rescinded guidelines](#) from the Office of the Comptroller of the Currency (OCC) were an attempt to build on GLBA with more specific information related to how financial institutions manage their information security programs to keep consumers safe.

2003

The Controlling The Assault Of Non-Solicited Pornography & Marketing Act (CAN-SPAM Act)

The [CAN-SPAM Act](#) “establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.” Basically, it creates guidelines for how businesses interact with other businesses and consumers via email.

2003

The Fair & Accurate Credit Transactions Act (FACTA)

This piece of legislation builds on the Fair Credit Reporting Act ([FCRA](#)) of 1970 and provides guidelines for how consumer information is shared online. The goal of [FACTA](#) is to protect consumers from identity theft that results from negligence on the part of institutions that handle PII.

2004

The California Online Privacy Protection Act (CalOPPA)

As the first state-specific privacy regulation, [CalOPPA](#) stipulates that any business that collects information on California residents needs to [conspicuously post a privacy policy on the company website](#). The goal of this policy is to define exactly how that business manages consumers PII.



2013

The CalOPPA Amended

The 2013 amendment updates the language of [CalOPPA](#) to “require two new privacy policy disclosures for websites and online services regarding behavioral tracking.”

2016

The California Electronic Communications Privacy Act (CalECPA) & The Delaware Online Privacy & Protection Act (DOPPA)

Two more state-specific regulations went into effect in January of 2016—[CalECPA](#) and [DOPPA](#):

- The California Electronic Communications Privacy Act states that “no California government entity can search our phones and no police officer can search our online accounts without going to a judge, getting our consent, or showing it is an emergency.”
- The Delaware Online Privacy and Protection Act [expands on CalOPPA](#), citing users instead of consumers, bringing in mobile apps, and widening protections to any or all entities dealing with the PII of Delawareans.

2018

The General Data Protection Regulation (GDPR) & The California Consumer Privacy Act (CCPA)

In May of 2018, the European Union (EU) enacted the [GDPR](#)—one of the largest data privacy and security regulations to date. This [comprehensive piece of privacy legislation](#) codifies how businesses collect, store, manage, share, and access users’ PII. Billed as a common-sense data security law, the GDPR provides guidelines for how data is secured at every touchpoint in the customer life cycle. In the same year, California passed the [CCPA](#). Mirroring the GDPR in many ways, the CCPA is arguably the most comprehensive data privacy regulations in the United States.

The CCPA [defines these privacy rights on their site](#) as follows:

- The [right to know](#) about the personal information a business collects about them and how it is used and shared;
- The [right to delete](#) personal information collected from them (with some exceptions);
- The [right to opt-out](#) of the sale of their personal information; and
- The [right to non-discrimination](#) for exercising their CCPA rights.



2020

The CCPA Goes Into Effect

After passing in 2018, the CCPA finally goes into effect in January of 2020. According to [Wired](#):

“The CCPA [applies](#) to any company that operates in California and either makes at least \$25 million in annual revenue, gathers data on more than 50,000 users, or makes more than half its money off of user data. For California residents, it creates a handful of new rights over their data. The most significant categories are what Alastair Mactaggart, the California real estate magnate behind the ballot initiative that led to the law being passed, calls ‘the right to know’ and ‘the right to say no.’ That means users will, as of today, be able to see what data companies have gathered about them, have that data deleted, and opt out of those companies selling it to third parties from now on.”

As the landscape of data privacy and security continues to evolve, we’ll likely see more regulations enacted across state and federal levels. It’s important to understand how each of the regulations affects your business as well as consumers in your market.

Product Management In A Post-Privacy World Isn’t Easy

The increased visibility into company data privacy practices means your business is more at risk of damaging customer relationships. As regulations change and consumers become more invested in their own security, you need to remain diligent in your practices.

Product Strategies For The Post Privacy Era

Throughout this guide, we've highlighted the underlying forces that fundamentally changed the privacy landscape for online businesses. We defined what data privacy is, talked through why it is important, and how an increase in privacy regulations and consumer concerns changed the way we make decisions about customer data.

When [79% of consumers](#) are concerned about how companies collect and use their data, providing a consistent customer experience requires tact from companies and trust from customers.


To put it simply, doing business in a post-privacy world isn't easy.



Aaron Glazer — Co-Founder & CEO of Taplytics

"It's a matter of adopting as a mindset and making decisions, while working with like best-of-breed third-parties, to take their products and technologies and implement them in a privacy-first way. This allows companies to work really quickly and protect the trust the customer puts in them."

In this section, we'll bring together the ideas presented so far and provide strategies you can use to create the kind of personalized experiences customers expect, narrowing our focus to talk through how to accomplish these goals without opening the customer's valuable data up to potential privacy and security issues. With so much access to customer data and personal identifying information (PII), modern companies need to put a sincere focus on keeping customers safe.



We'll start with a discussion on how to determine what kinds of data you truly need, then move on to highlight other strategies for building out your strategic approach to data privacy.

Know What Kind Of Data Is Truly Valuable (And When To Use It!)

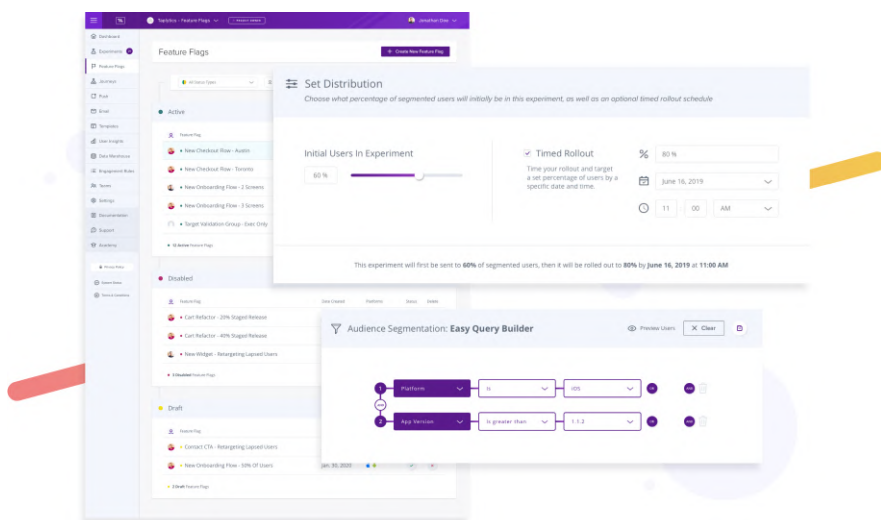
Even with the increase in regulations surrounding data privacy and security, modern companies still have access to substantial amounts of customer data. Understanding the value of different data types and which of them are actually useful to your business is the key to keeping customers and your company safe.

To determine what customer data and PII are most valuable for your business, start with your [user personas](#). These personas give you a comprehensive overview of the various types of customers who use your service, as well as the overall value they provide to your business. Digging into these personas helps you understand the different types of data you can collect and makes it easy to prioritize which ones you need first.

We build these personas from useful customer data, like:

- Demographic information
- Most-used features
- Account engagement history
- Preferred communication channel

Talk to your product, marketing, sales, and development teams to see what they find valuable and use audience segmentation and prior launch data to refine the types of data you want to use as well. This will help you build better products and release features that are relevant to different audiences.



Example audience segmentation via Taplytics.

Understanding data that provides insights into your core users' behavior helps you prioritize the way you collect it from customers. And that data will highlight when people are most likely to provide it willingly based on their experience with your product as well. If you ask for too much too early, it can hurt the customer experience.

While some customers are more than willing to provide a wealth of information during the signup process, others might first need to see the value of your product before jumping in. Personas help you identify the points in the relationship where you can ask for this information, like during account signup or just after new user onboarding is complete.

Just make sure you clean your data regularly. Keeping too much data on previous customers can expose a larger group of people to potential security issues. While we're not saying you should purge all customer data once someone cancels their account, you should remove any PII and contact details quickly. Many of the privacy regulations we talked through in the last chapter list specific timelines and data types you can keep for "historical data" integrity.

Once you've determined the various types of customer data you need to build a successful marketing strategy, the next step is thinking about how you'll communicate those needs to customers.

Communicate Your Commitment To Data Privacy To Customers

Building a successful product marketing strategy in the post-privacy era is all about communication. Many of the regulations we discussed earlier in the guide have clear guidelines on how companies should communicate their privacy and security processes—both internally and externally. But being forthright with your commitment to data privacy isn't just about following the rules; it's also a great way to increase engagement from customers.

First things first: Make your privacy policy clear and easy to understand. Regulations like [GDPR](#) and [CCPA](#) state that you need to present your privacy policy in an easy-to-see area of your site, but making it easy to find is just the beginning. Most privacy policies understandably include some legalese to highlight specific aspects of compliance, but when you include this difficult-to-understand language, it's important to clarify it for your customers as well.

Our [privacy policy](#) is always accessible in the footer of our website.



© 2020 Taplytics Inc. All right reserved | [Privacy](#) | [Taplytics End User Terms Of Service](#)

Taplytics privacy policy.

And here's an example from the **Your Inputs** section to show how we talk about privacy with customers:

We collect personal information you provide to us on our website, such as your name, email address, telephone number, and username and password, when you:

- *Contact us through the website and fill out an online form;*
- *Create an account on our website;*
- *Sign-up for our newsletter; or*
- *Sign-up for our services provided via the Taplytics Dashboard.*

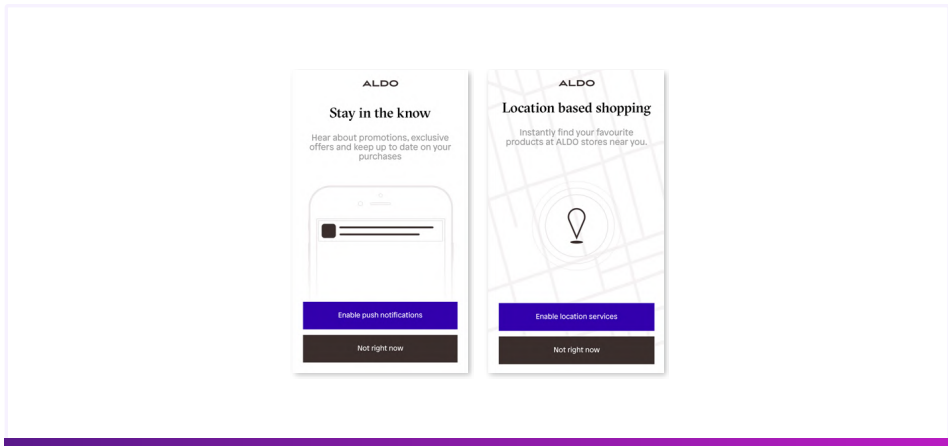
This information collected is only used to fulfill the service you have requested, such as authentication for access to the Dashboard or delivering the newsletter, or to contact you in regards to your inquiries. Information collected through the Dashboard is also used to track usage and activity for diagnosis purposes. We use your browsing activity to discern your interests and provide you with advertisements and updates tailored to your interests.

Section on how Taplytics collects customer data in our Privacy Policy.

Customers need to understand your commitment to privacy just as much as the regulatory entities. The GDPR website includes content on how to [write an effective privacy notice](#) to help get you started.

Try using [push notifications](#) to let customers know when you're asking for additional information. When you include language like "you told us you liked X" or "we noticed that you did Y," it helps engage the customer directly and makes their experience better.

These notifications are also a great way to highlight how your company uses customer data and PII to craft a better experience for the customer.



Example push notifications via [Taplytics](#).

Take a look at how [ALDO](#) lets the customer know specifically how each type of notification will benefit their experience. When people expect a certain level of personalization in their user experience, this kind of direct explanation is really helpful.

The more context you provide to current and potential customers, the better prepared they'll be when you ask them for more information.

Define Processes That Increase Security

The methods you use to transfer data between tools and internal documentation are rife with potential security issues. That's why it's important to ensure that the processes your team follows and the tools they use are secure. Human error can cause as much damage to your data privacy and security as technological issues.

Here's an example from our CEO:



Aaron Glazer — Co-Founder & CEO of Taplytics

"So, now you've got PII data and the business intelligence team will send you a CSV. That's going to sit on someone's laptop. And now there's the risk of 'should the person who even receives that data have access to this information.' It sits on a laptop, that laptop could get stolen. That CSV file could go anywhere or that CSV file might get forwarded. It might get thrown on a cloud server somewhere, and years down the line, somebody's going to find that F3 bucket and download this data. And all of a sudden you've got a data hack, because somebody downloaded CSV."

This is a surprisingly common situation your team might encounter in their day-to-day responsibilities. As a lot of customer data and PII are often shared between teams, the potential for lax security measures increases when processes aren't defined. That's why it's vital to outline your data privacy and security measures internally. Every member of the team needs a clear and comprehensive understanding of their part in the operation.

Train incoming team members in these proper data handling methods as well. When your team grows, the potential for oversights increases as well. The best way to mitigate the risk of any issues is by creating an internal privacy policy that's shared in a single, easy-to-find location. This document should outline:

- Who is responsible for owning data security at a high level
- What processes are in place to mitigate the risk of human error
- Where team members can learn more about these processes
- What happens if something goes wrong

As long as you revisit these processes regularly, it's easy to keep your team compliant with the most up-to-date regulatory mandates.

Another part of the equation is an understanding of the tools and platforms that are involved in these processes.

Own As Much Of Your Data As Possible

Earlier, we talked through some of the underlying drivers in the shift toward privacy-first companies. While increasingly savvy customers definitely contributed to this change, another significant part of this evolution was a reliance on third-party tools that were inherently less secure. In a post-privacy world, companies need to own as much of their data as possible to maintain control.

[Taplytics](#) offers single-tenant and private cloud hosting functionality to ensure that all your valuable customer data is safe and secure at all times. We're committed to maintaining both our data privacy and the security of our customers.




Commitment To Data Privacy

Taplytics is the only solution that offers single-tenant and private cloud hosting options, allowing you to own and protect your customer data, avoid privacy risks, all while providing personalized customer journeys.

PRIVACY-FIRST

When you're looking for different kinds of tools, it's important to understand how those tools handle data privacy and security, then vet each one accordingly. Companies need to have as much control as possible over the types of data they collect, and the tools you use to gather this data are a big part of that.

You also need to understand who owns the data, the methods used to collect it, and what recourse you have if any potential issues arise with any tool in your technology stack. Most privacy regulations require a concrete process overview to ensure that privacy and security are maintained at all times.



Look for platforms that integrate seamlessly into your current tool stack. The better these connections, the easier it is to share data safely, and the less likelihood there is for human error to cause problems. As you figure out which tools help you understand customers without increasing the chance for privacy-related issues, you make it easier to maintain proper security across the board.

Don't Make Pre-Privacy Decisions In A Post-Privacy World

Maintaining data privacy and security is an arduous process—but a necessary one. In today's post-privacy era, your team needs to remain diligent in their practice to ensure ongoing security for customers. When you understand the nuances of privacy regulations and make decisions based on these ideas, maintaining security for these kinds of things is much easier to scale.

The Future Of Product Is Privacy First

Concerns about consumer data privacy and security aren't going away. According to a Pew Research Report from 2019, [75% of consumers](#) think that there should be new regulations for what companies can do with personal data. Understanding how to market your business in light of these considerations is vital to your survival.

And those concerns are only trending up. As consumers become savvier, companies become larger, and third-party integrations become the norm, maintaining data privacy and security will become a primary concern for every business.

What does it mean to be a successful online business in the post-privacy era?



Aaron Glazer — Co-Founder & CEO of Taplytics

"We think of a post-privacy world as eliminating the parts of the chain where your data can get exposed, without giving up any of the functionality."

In many ways, it comes down to control. Throughout this resource, we talked through how important it is to understand privacy for modern product managers. Let's revisit those takeaways one last time before closing out the guide.

4 Guidelines For The Post-Privacy Era

Maintaining customer security has to be your primary concern in a post-privacy world. Whenever someone interacts with your company, they need to trust that you're able to keep them safe. Without that trust, you'll never be able to build the types of relationships required to support your business goals.

1

Data Privacy Starts With Data Ownership

The tools you use and the processes you create have a direct impact on how easy it is to keep your customers safe. Ceding control to third-party providers can put your customers at risk—which is why it's so important to own as much of your data as possible. So make sure you properly vet every tool, process, and workflow that interacts with customer data. Failing to do so will make it difficult to have the type of control you need to maintain proper data privacy and security for your customers.

2

Privacy Regulations Will Evolve

There are no country-wide privacy regulations in the United States, but that's bound to change. Post-privacy companies need to stay up to date on all relevant laws and mandates in their industry to ensure compliance. Whether it's industry-specific regulations, like [HIPAA](#), or more far-reaching privacy laws, like the [CAN-SPAM Act](#), understanding which laws impact your business helps keep your customers and your team safe.

3

Customer Communication Is Key

As the privacy landscape continues to evolve, it will become even more important to highlight your privacy and security measures. Communicating your commitment to data privacy shows current and potential customers that you have a shared interest in keeping their personal information safe. Not only does this position your company as a trusted partner in the market, but it also fosters the types of relationships your company needs to grow.

4

Post-Privacy Decisions Aren't Easy

Every decision you make for your company in the post-privacy world needs to be rooted in keeping customers safe. When their valuable data is exposed, it can cause irreparable damage to your relationships and, ultimately, your business. Using pre-privacy thinking will put your company at risk, so make sure you have a team who can support your data privacy and security processes.

Taplytics Helps Keep Your Customers Safe

With private cloud and on-premise deployments, [Taplytics](#) is committed to helping you maintain your data privacy as your company grows. Whether you're rolling out a new feature to customers, setting up A/B tests for an upcoming release, or triggering push notifications to specific users about their accounts, keeping customers safe needs to be your primary concern.

Conclusion

In this guide we've covered planning and prioritization, execution, and the significance of data privacy. We hope that with this guide you'll now have the tools to make your role as a product owner easier.



For more information about Taplytics and how we help companies optimize their apps and websites, feel free to [reach out](#) - we'd love to chat!



LinkedIn



Twitter



Instagram



Facebook