ANAGOG

Privacy: The **5th P** of Marketing

…to win the customer endgame you must first figure out **the privacy endgame**

As retailers gear up for the end of what has been a challenging year, it is a good time for them to take a long hard look at their personal data practices.

Consumers are not the only ones who become active during the holiday season; it is also the season for scammers, identity thieves and cyber-criminals. The continued growth of digital commerce will only increase the cyber-risks to retailers, so companies must take special care not to unintentionally gift the personal data of holiday shoppers to these digital pirates. While making preparations for the fiercest competitive season in retail, it is important to realize that in order to win the customer endgame, you must first figure out the privacy endgame.

"App" has u location 14 ti background ov days. Do yo continue to allow location

As our Privacy Polic use and share your with trusted partn forecasts, weather ale to provide and impro

Local news, weather & recommendations

We'll use your location to recommend local news, shops and restaurants that are relevant to you.

Personalization is Necessary to Win the Customer Endgame

It has long been clear that consumers have so many demands on their attention that their patience for irrelevant communications from brands is at an all-time low. This has increased to the point that the dread of receiving **any communication at all** from brands/services is so mainstream that many only give out fake email addresses. With so many potential options for mobile engagement, companies now realize that they must prioritize quality over quantity. In order to have a chance at engaging their customers, they must be extremely selective with regards to the engagements they send.

This is the reason that personalization, the targeting of users based on their needs, preferences and behaviors, is so crucial. Without efficient, effective audience segmentation and contextually-aware messaging, companies will never meet their marketing KPIs.

Personalization with Privacy is not easy

Allow “App” to access your location while you are using the app?

You location is used to show personalized insights

Allow While Using App

Allow Once

Don't Allow

“App” Would Like to Acc

the Microphone

Let App use the microphone t

translate speech.

OK

“App” Would Like to Access the Camera

Camera usage and photo for scanning various Travel documents and Payment options

Don't Allow

OK

The problem, of course, comes down to personal data. Personalization requires knowing things about the customer, whereas consumers are less comfortable with the idea that companies control large amounts of their personal data. Companies are happy to promise that they will not abuse any personal data that comes into their possession, but it is well-known that, even with the best of intentions. they cannot guarantee they'll be able to deliver on that promise.

The problem has become so well publicized that regulators, consumer groups and other interested parties (such as Apple and Google) are blocking access of mobile apps to personal data. At a macro-level, this is good for consumers and the industry. **The result for mobile marketers, however, is a complicated reality. Establishing and maintaining a personal relationship with their customers can now feel like a high-flying circus act where they are expected to be juggling while riding a unicycle on a tightrope over a pride of lions.**

Privacy is Good for Business

Companies' personal data practices are now being scrutinized by everyone: customers, regulators, consumer watchdogs and shareholders. Insofar as a company's approach to personalization relies on personal data collection, it is clear to everyone that the exposure is great. Even consumers who fully trust your company may have valid concerns that their personal data will end up in someone else's hands.

To be clear: One third of your customers are willing to walk away over privacy concerns. In of itself, this is a sign that investing in privacy is not just for moral reasons. Studies have shown that for every dollar spent on privacy, the average company gets back $2.70 in associated benefits. The numbers don't lie.

For those who are not swayed by carrots and who prefer sticks, the risks arising from privacy breaches are somewhere on the scale between significant and catastrophic. Even before factoring in IT costs and legal damages, the average churn from a data breach results in a $3 million loss.

$2.70 the average return for every dollar spent on privacy

$3M the average cost of churn as a result of a data breach

Repeated advances in technology have introduced the digital marketing industry to remarkable capabilities and companies have eagerly spent large sums of money to upgrade their MarTech stacks. After all, the aforementioned circus act is indeed exciting and profitable. Unfortunately, these technological developments have not gone unnoticed by digital pirates on one hand and regulators on the other. Managements are therefore required to re-allocate budgets every 18 months for new security measures or new software architectures that are necessary to keep the circus act running. Understandably companies have less of an appetite to bear these incremental costs as a result of the frequent changes to privacy practices.

What is the Privacy Endgame?

The solution is to leapfrog over incremental improvements in privacy policy and jump directly to the endgame; an architecture in which private data stays private, protected from prying eyes by existing only on the user's phone. This approach makes it possible for hyper-personalized engagement to continue to fuel a compelling User Experience with no risk. **When personal data is no longer collected by the app, the company no longer has to review compliance requirements, change storage policies or sweat over the associated data hacks. That is the endgame.**

Why is Edge AI so important for the Privacy Endgame?

Edge AI is the perfect solution for digital marketers who want to provide a personalized customer experience without infringing on users' privacy and without getting into trouble with the regulators and the App stores (Apple / Google) over unsafe data practices. With Edge AI, marketers can run sophisticated, personalized mobile engagement campaigns while all personal data can stay on the device:

Companies can finally apply fine-tuned segmentation, using various data sources, without the headache and exposure of private data collection.

Regulators can be reassured that their common-sense regulations are not handcuffing digital innovation, since companies can provide excellent experiences without handling sensitive data that might be hacked.

Customers gain peace of mind, since their personal data is no longer currency that is exchanged between companies they may have never heard of.

Steps you should take: Some endgame cheat codes

01 Make the app smarter

The Anagog SDK employs Edge AI technology that allows us to run artificial intelligence on the user's phone. By integrating the SDK into your app, you will benefit from a range of insights into the actions, locations and activities of the user that are generated by on-phone analysis. These insights can then be used for precise Audience segmentation and contextual engagement.

02 Transform the Campaign Flow

Using the Anagog Console, you can create campaigns and remotely configure the SDK, including which transactional and app data you want to use in those campaigns. Without possessing any data about your customers, you can target highly granular Audience segments at very specific, individual Contexts for optimal engagement. This precision helps you devise a compelling Call-to-Action to increase the likelihood of conversion. **Only campaigns that are relevant will become active for any given user and they will patiently wait until the timing is right to trigger the engagement.**

03 Use all available 1st party data

First-party data is generated from direct interactions with the user, so it is fresh, accurate and much more reliable than other types. Depending on the user's consent, this can actually be a wide array of data. When all that data resides in the cloud, many customers may find it to be uncomfortably revealing. In the event that the data goes through a 3rd party (e.g. a cloud-based Mobile engagement platform), this can create unnecessary exposure for your company. By keeping the data on the phone, Anagog helps you avoid these thorny issues while still maintaining the ability to use a rich data set for targeting and engaging your users. Moreover, this makes it much easier to be fully transparent with the users and ensure that they maintain control over their data and how it is used.

Winning any game involves making the right moves at the right time. **Make your move to Anagog's Mobile Engagement Platform** and you (and your customers) will come out of the personalization and privacy game as winners.

Let's Talk!

www.anagog.com