syrenis

GUIDE

The ROI of Consent Management

syrenis.com

Introduction

In today's environment of budget tightening, functions that businesses traditionally consider to be cost centers find they are struggling to justify their expenses more than ever.

Fortunately for consent management done well, the Return on Investment (ROI) is clear and compelling, flipping the idea of privacy and consent management as a 'cost center' on its head. When the explanation includes consent automation, through a consent management platform, the calculation additionally eases budget concerns and provides an easy case for the resource allocation.

The following are factors to consider when considering a bottom-line justification for consent management and related automation:

- Efficiency of marketing spend
- Value of trust
- Reduction of individual rights requests
- Benefits of personalization
- Lower compliance risk

Efficiency of Marketing Spend

In some ways, direct marketing is a numbers game. A company that manages to obtain contact information about or access to individuals about whom they know very little directly, must guess what products, services, and advertisements might interest those people.

Segmentation based on demographics and cross-context advertising can help educate that guess, but at the end of the advertising day, it is still a guess. This means that the company must pay for a shotgun approach to marketing, spraying tiny pellets across a wide audience in the hopes that the message will resonate with some small percentage of recipients.

However, especially if a company applies an opt-in, explicit consent model for marketing, it can use a more cost-efficient rifle approach to marketing. Rather than guessing what types of messages, media channels, products/services, and experiences will resonate with targets and result in conversion, the company knows because it asks.

In fact, there is evidence to suggest that consent-based marketing results in 2-5x the conversion rate. This means that a company can be much more efficient in targeting the right people, with the right message, through the right media – spending less money to receive a higher conversion into revenue.

The exact efficiency coefficient will be different for each company. However, even a 10% reduction in marketing costs, enhanced by twice the conversion rate, will represent persuasive numbers backing a decision to move towards consent and consent management done well.

Impacts on Advertising Spend

Web browsers are an essential part of our daily lives, but not all browsers are created equal. As consumers have become more privacy-conscious, web browsers have evolved to meet this shift in behavior.

Many browsers have joined the privacy movement, enhancing user privacy and data protection with features like cookie management, tracking prevention, fingerprinting prevention, ad blocking, enhanced encryption, and preferences management.

With Google planning to implement privacy settings similar to Safari and Firefox where cookies are deleted automatically after a short time period, it's crucial to consider how these changes impact your user base. Safari, Chrome, and Firefox together hold 83.7% of the global browser market share, with Safari managing 47% of all mobile traffic in North America.

Up to 35% of your traffic might be misidentified as new visitors instead of returning ones. Privacy browsers enhance user privacy but can hinder legitimate tracking.

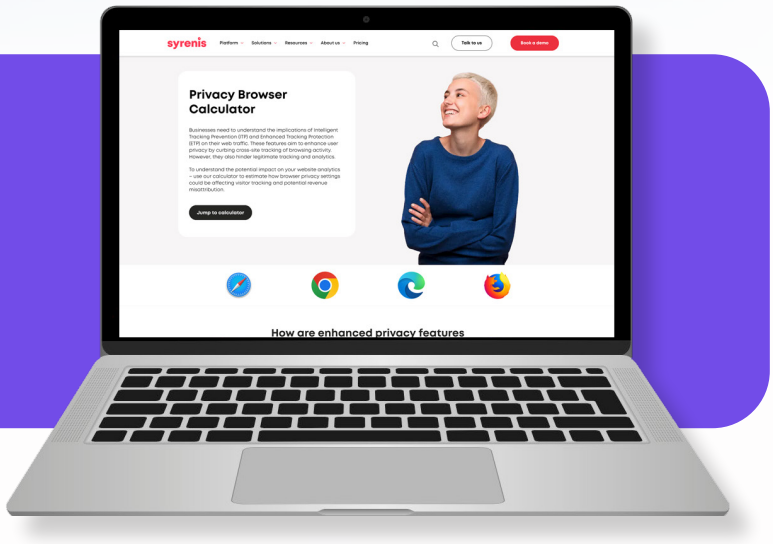
Correctly identifying returning visitors means being able to serve them more relevant incentives, adverts and content. Save money and improve ROI (i.e. retailers won't erroneously give away incentives/discount codes to returning customers).

In particular, content owners and placing ads with publishers are seeing significant impacts on ROI on ad spend. For publishers and content owners we typically see a CPM on Safari being 10%-15% lower than Chrome. Some cookie solutions, like Syrenis, are able to stop the effects of privacy browsers by recognizing when a first party cookie is being stripped and replacing the original cookie selections / value. This leads to more data being held on anonymous user journeys in your CDP / ID Graph.

By making Safari act like Chrome, for an organization bringing in $1B ad revenue, you can typically see the revenue impact being circa $60M – a huge impact on ROI.

Estimate how privacy settings could be affecting visitor tracking and potential revenue misattribution

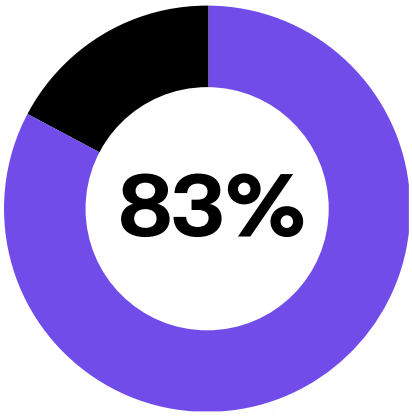
PRIVACY BROWSER CALCULATOR



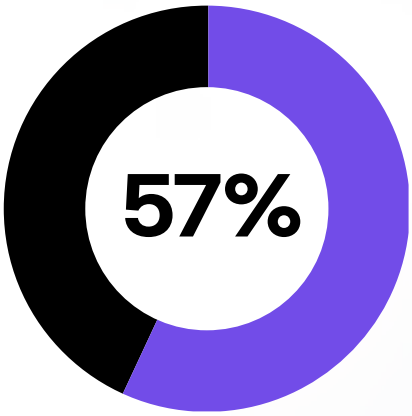
Value of Trust

Over and over, market research underscores that people care about privacy, are more willing to buy from companies they trust to handle their personal data ethically and are equally willing to walk away from companies they do not trust with their data.

For example, a **Forrester study** showed that consumers are willing to walk away from a company they do not trust.



of consumers protect their privacy by engaging only withtrusted companies



of app users have uninstalled an app for privacy concerns

READ MORE

In fact, privacy protection is the top non-product-related influencer for shopping, with fraud prevention and social/corporate responsibility in distant second and third place. As a **Forbes article headline** declares, “The Imperative of Customer Trust in 2024” is a trend that businesses cannot ignore.

Moreover, the key factors that positively influence trust seem to be consumer control over personal data and transparency of privacy practices. One study shows that “perceived privacy control significantly influences trust and perceived privacy.” Additionally, the **International Association of Privacy Professionals (IAPP)** reports that 64% of consumers trust companies that provide clear notice of data handling practices more than those that do not.

> “Are customers told when they are speaking to a chatbot rather than a human? Do they know they can opt out of their data being used and stored? Businesses will have no alternative but to be clear and transparent with customers to gain and keep their trust.”
>
> **Mattias Goeler, Zendesk CTO**

The exact calculation of the value of consumer trust, and the benefits of supporting factors that lead to that trust, such as transparency and control, will vary from business to business. However, even if a conservative estimate of a few percentage points increase of customer retention/loyalty and sales comes to pass, the return on these investments will be significant.

Reduction of Individual Rights Requests

Though each jurisdiction that outlines data subject requests as a requirement differs in its process, timing, and rights provided, most regulators agree that the main intent of individual rights is to give to consumers more control over their personal data.

Even data subjects without those rights make data subject requests, showing more cross-jurisdictional consumer interest than ever before. For example, **Data Grail reports** that 52% of all individual rights requests made in the United States come from individuals who reside in a state without explicit individual rights.

Intuitively, it makes sense that companies with effective communication about data practices and that offer granular choices about data collection, sharing, and uses will see fewer individual rights requests. After all, an individual rights request is a demand for control. Consumers who already feel that they are in control over their own personal data will not need to exert additional control in the form of a deletion, correction, access, do not sell, use limitation, or other request.

Handling individual rights requests is complicated, time consuming, and involves the risk of noncompliance. Individual rights requests are expensive to handle as well.

Gartner, in its **Market Guide for Subject Rights Request Automation** document, reveals that the average cost to fulfil an individual rights request manually is US $1,524. Automation can reduce this cost, but even a 50% or more reduction leaves both human and budgetary resources committed to addressing requests.

$1,524

Average cost to fulfil an individual rights request

A majority of countries have implemented laws that provide for individual rights, and given consumer interest in and concern about privacy, individual rights is a compliance obligation that will not go away entirely. However, if clear notice and a sense of real control over personal information heads off some percentage of requests, the customer experience overall improves dramatically and the company's case for these improvements increases through lower costs and distractions from core business activities.

Benefits of Personalization

Personalization is simply the act of customizing experiences. Historically, companies had to make educated guesses about which experience would resonate with customers by segmenting, or categorizing people in large groups based on demographic or other information.

For example, if the company in question knew that a website visitor was a single female with a higher income in Texas, it might present one set of experiences or send a specific direct marketing campaign to that individual, which might be different from the experience or campaign the company directs at someone who falls into a different segment.

The challenges with this type of personalization based on segmentation are twofold. First, the company often must infer which group an individual belongs based on data obtained from aggregators and small details it may know from first party data collection. Second, not all single, high-income females from Texas are alike in their preferences. This means that any set of experiences a company believes will appeal to people in this segment may resonate for some, and even most of the individuals, but it will not resonate with all. In other words, personalization based on segmentation is a numbers game that bets on an assumption that an experience or campaign will resonate and result in conversation with some recipients but will lose others.

On the other hand, Artificial Intelligence (AI) and the enormous amounts of online data available today have allowed companies to instead base personalization on individual factors. Called hyper-personalization, a company now has an opportunity to tailor content, campaigns, and other experiences according to everyone's unique set of interests, preferences, demographics, behaviors, and needs. That is, rather than guess based on gross factors, a company can just ask and act accordingly.

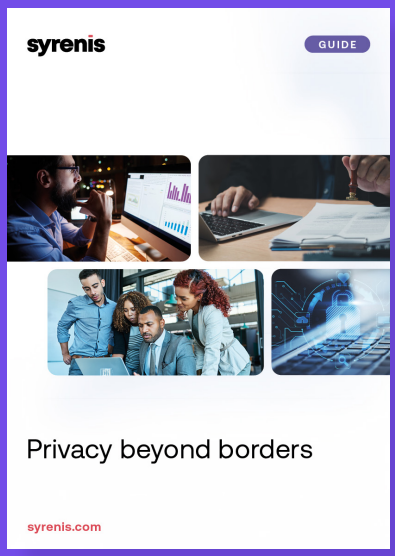
Consent and preference management is a critical component of hyper-personalization. Without AI and a robust consent/preference management platform, a company would find it difficult, if not impossible, to collect and understand the amount of data it must have to tailor experiences for each individual person. To work, a company wishing to adopt a hyper-personalization strategy for experiences and campaigns must be able to interface with individuals to ask about their preferences and get consents, and then analyze and manage those preferences/consents.

The benefits of this newer technique are substantial, however. Deloitte reports that 90% of customers like personalized advertising. They also point to increases in clickthrough rates of 65% and conversation rates of over 33%. Similarly, 80% of customers are more likely to purchase from a company that offers experiences personalized to an individual level. There is also evidence that younger generations, such as Generation Z, expect this type of individual preference-based interactions from those companies with which they do business.

48%

of consumers say that lack of personalized content sways them to opt out of marketing emails from brands.

DOWNLOAD NOW



Though consent/preference management is not the only activity that allows for hyper-personalization, it is a critical effort that helps a company understand what an individual expects and prefers. The benefits in conversion rates, revenue, and even future-proofing sales numbers with younger generations that expect hyper-personalized experiences all add to the ROI for consent and preference management.

Lower Compliance Risk

Most ROI calculations will include both the honey and the vinegar – the upside for the business case, and the cost or risk avoidance expected from the activity.

While the benefits of marketing efficiencies, and increased revenue from hyper-personalization and earning customer trust have the potential to add to the bottom line, there are also cost and risk avoidance benefits that add to the ROI of consent management done well. As we have seen, there is the cost reduction potential related to a reduction of individual rights requests. Additionally, in any compliance area and especially in the privacy space, sound consent management reduces risk and associated costs of non-compliance.

The marketplace has seen increased 'teeth' in privacy laws around the world in the form of significant fines and penalties. The European Union's (EU's) GDPR provides for up to 4% of global annual revenue, for example. The United States (US) State of California's privacy law provides for up to US $ 7,500 per violation, which frequently adds up to millions of dollars.

Enforcement is also incredibly active in the privacy space. Not only privacy-specific regulators are active in privacy enforcement. General regulators have also expressed a priority for enforcing privacy. For example, the US Federal Communications Commission and Federal Trade Commission have both underscored privacy and security as priority concerns. Additionally, lawmakers across the globe continuously are adding new privacy laws and updating existing privacy laws with stronger requirements.

The complexity of getting privacy right and potential downside for a privacy miss combine to form a world in which there is a real possibility of even good, well-intentioned companies facing significant fines and penalties. Adding to the cost of fines and penalties are the legal fees to address regulatory investigations and lawsuits and stock and revenue drops resulting from brand damage can have significant negative impact that a company must add to the ROI calculation.

Consent is not the only component to privacy success. However, given that all global privacy laws strongly focus on consent and transparency, it is almost guaranteed that a company that does not address consent management well faces all these risks of privacy noncompliance – fines/penalties, brand damage, lost revenue, legal fees, and decreased stock price. Any calculation of the benefits of consent management must also address the cost and risk reduction aspect.

Cost/Benefit Analysis of Consent

Any ROI discussion must consider the costs, and making the case for consent management must also consider the full cost of that activity for comparison with the benefits in revenue and reduction of risk/costs. Depending on how the company is considering managing consent, the true costs may be a combination of:

- Annual consent management platform license fees
- One-time integration and set-up costs
- On-going maintenance costs
- One-time and ongoing training costs
- Ongoing support costs

The ROI calculation itself is fairly straightforward: ROI (%) = ((Total Benefit – Total Cost) / Total Cost) × 100. However, the way to get to a firm number for all benefits, including indirect, predictive, or risk/cost avoidance benefits, can be difficult.

That said, the way to succeed in capturing the total picture is to get input from cross functional stakeholders. Marketing teams are experts in predicting and measuring positive impacts from increases in conversion rates and efficiencies in marketing spending. Technology teams deeply understand the costs and savings related to technologies. Operational privacy teams know the costs and complexities in managing individual rights requests. Legal teams know the costs of addressing regulatory inquiries and lawsuits.

Together, these and other teams can pull together the numbers needed to fill in the simple – but complicated – ROI equation.

syrenis

Contact us
hello@syrenis.com

US Office
Suite 700 3379 Peachtree Road NE
Atlanta, Georgia 30326, United States
+1 844 585 6264

UK Office
V2, Sci-Tech Daresbury, Warrington,
WA4 4AB United Kingdom.
+44 (0) 20 4551 9501