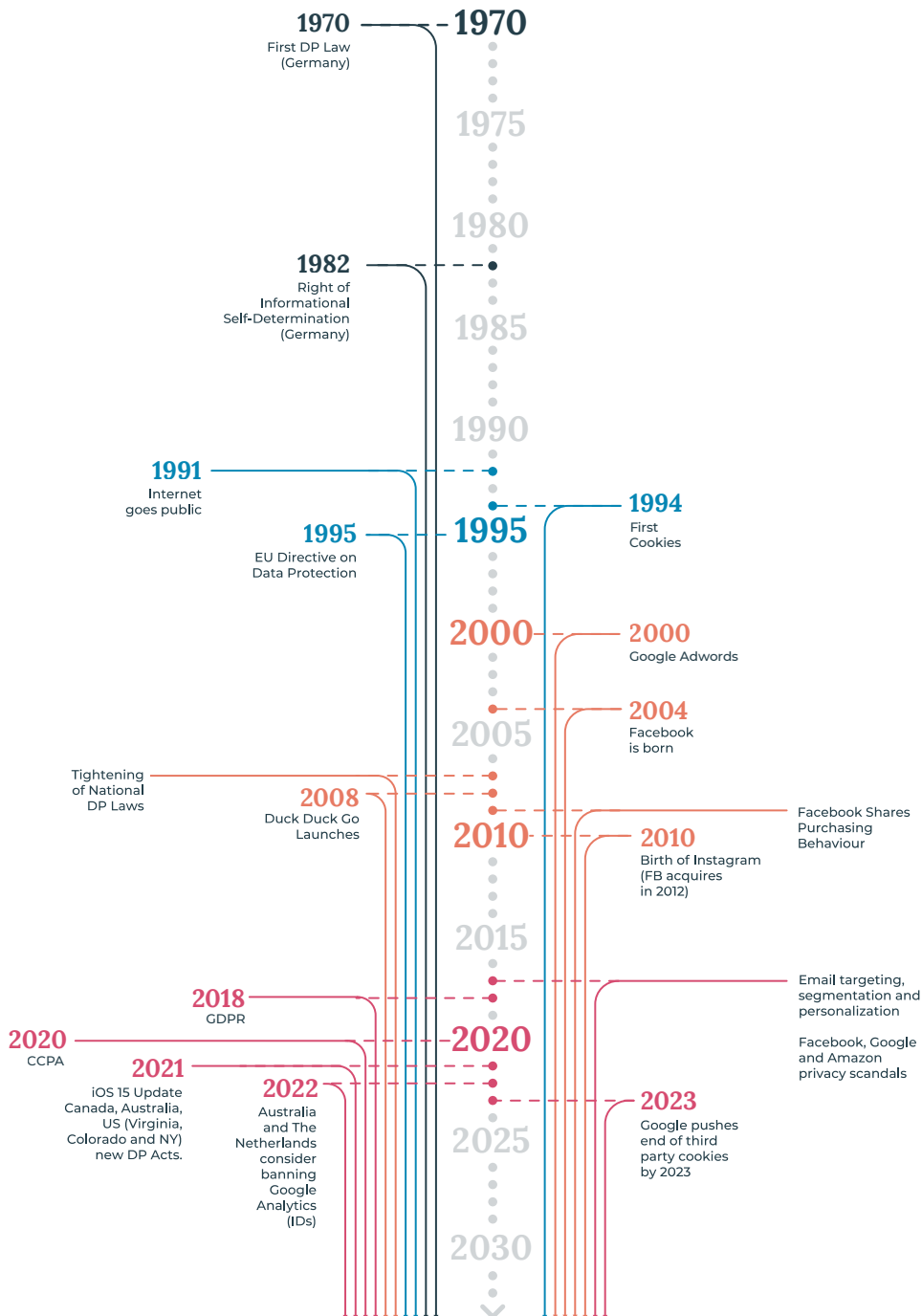


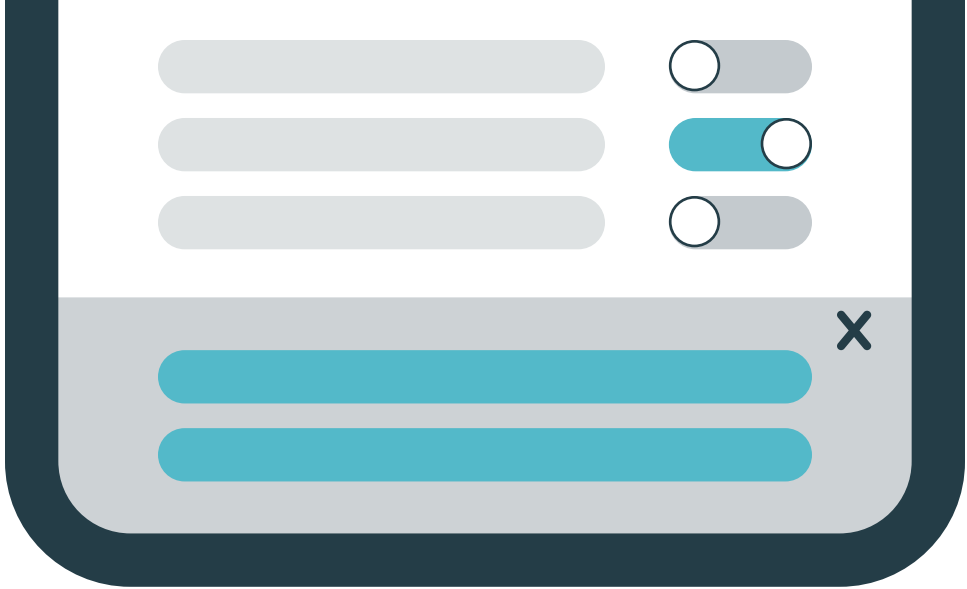


# WILL PRIVACY SHAPE COMMERCE?

Trust by Design Commerce Search  
Powered by Empathy Platform

EMPATHY.CO



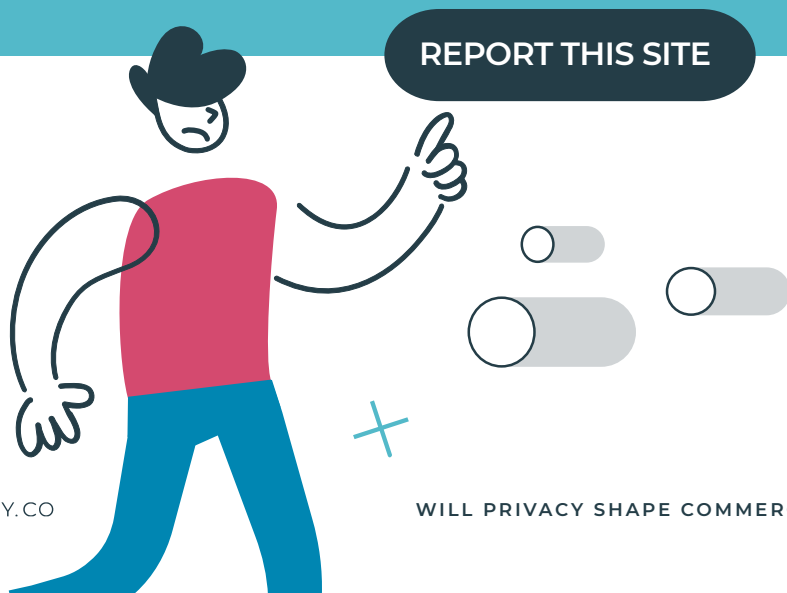


Amazon, Google and Meta have set the innovation pathway for everyone to follow. These giants have defined the rules of engagement for **Commerce SaaS vendors** and the digital industry as a whole.

With the exception of Apple, until now, these giants and their followers could not have cared less about **users' privacy**. Tagging, tracking and targeting are essential to their models and value. For these companies, the user's attention is an asset to be leveraged, against which features can be attributed with objective value.

Today customer surveillance is common practice among commerce solutions and platforms. User segmentation, personalisation, recommendation or hyper-localisation depend on user tracking. The trouble is that this dependency results in murky customer data practices that are now in question.

“An initiative directed at 10,000 sites through a single wave of complaints.”



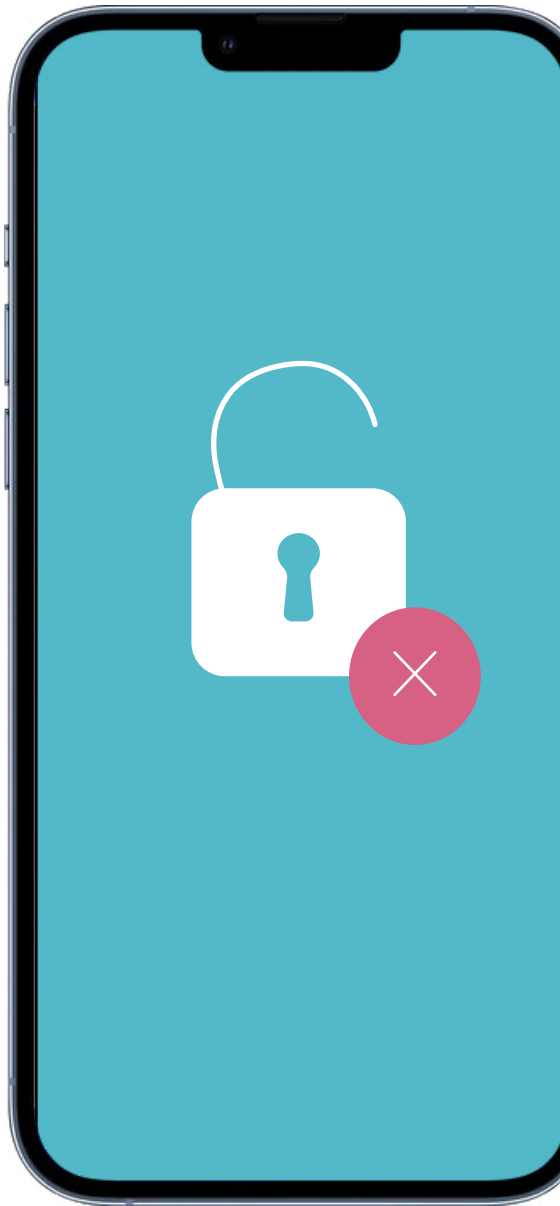
It seems, however, that the law is beginning to catch up with the help of privacy activists, such as NOYB.EU - European Center for Digital Rights and ICCL - Irish Council for Liberties.

NOYB.EU recently announced a new initiative that focuses on compliance of cookie banners in Europe. An initiative directed at 10,000 sites through a single wave of complaints.

And one that follows 500 draft complaints already submitted for unlawful cookie banners (according to NOYB).

This initiative, together with the recent Google Analytics ban in Austria (also an NOYB victory), have surfaced privacy concerns across the industry.

As per ICCL, their recent victory on IAB's consent framework (The Transparency and Consent Framework used within OneTrust and other consent management solutions that has been considered neither transparent nor consented), also signifies an acceleration in legal response to known, yet so far ignored, **privacy violations.**

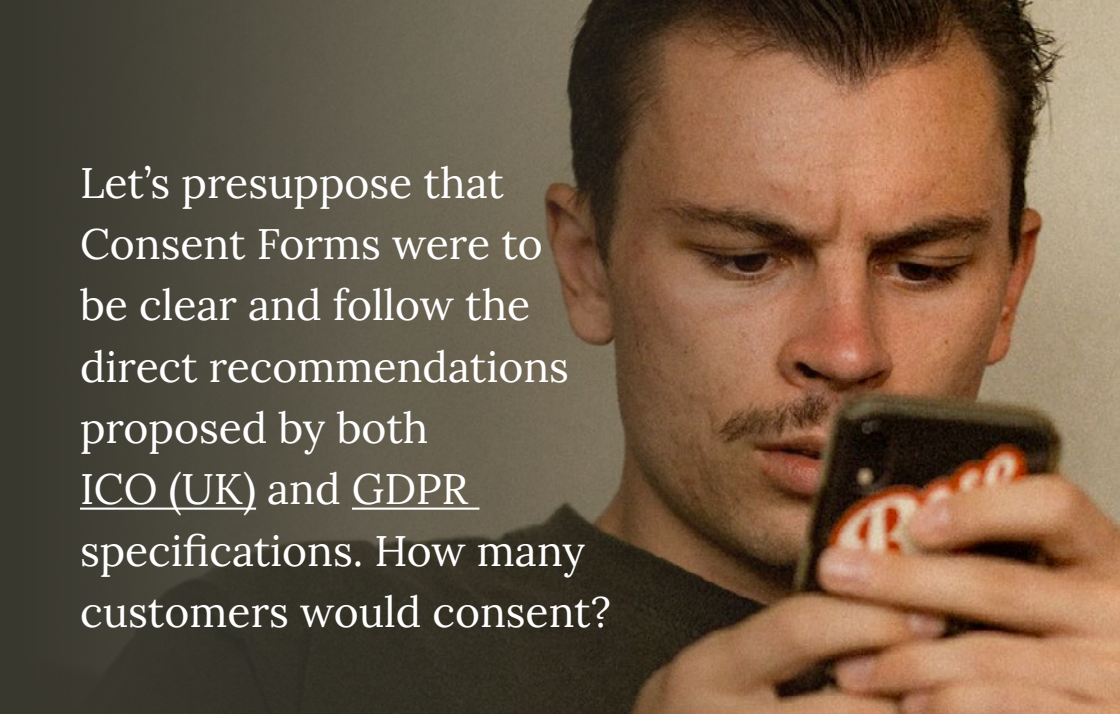




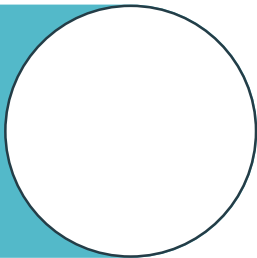
# DO THESE PRIVACY VIOLATIONS AFFECT RETAIL?

Most retailers struggle to keep pace and ‘innovate’ through ‘ready-made’ SaaS solutions that for the most part also depend on users’ consent and EU-US data transfers.

Take **hyper-personalisation** and **localisation**. These are common offerings among SaaS vendors of today. Have these conflicting privacy features been updated to meet the new law requirements? Not much beyond consent management solutions, which just, as the IAB’s consent framework, nudge the customer into accepting tracking because otherwise these features don’t work.



Let's presuppose that Consent Forms were to be clear and follow the direct recommendations proposed by both ICO (UK) and GDPR specifications. How many customers would consent?

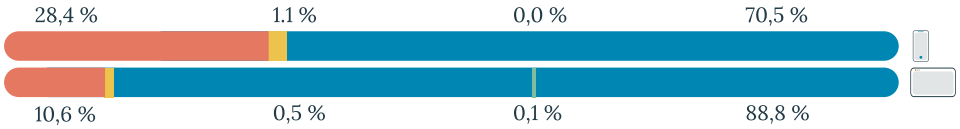


ONLY  
**30%**  
OF VISITORS WOULD CONSENT  
TO THE COOKIES THAT THESE  
FEATURES NECESSITATE.

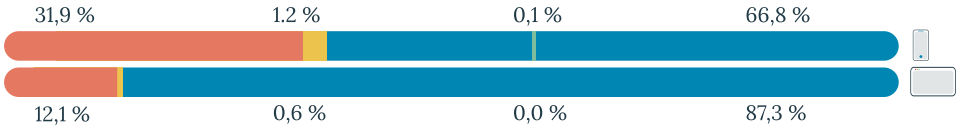
According to (Un)informed Consent: Studying GDPR (Ruhr-University Bochum, Germany, and the University of Michigan in the US), only 30% of visitors would consent to the cookies that these features necessitate.



### W/O PP-LINK & "DATA"



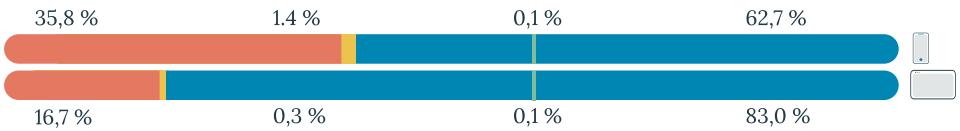
### W/ PP-LINK & "DATA"



### W/ PP-LINK & "COOKIES"



### W/O PP-LINK & "COOKIES"



0 % 25 % 50 % 75 % 100 %

% VISITORS



The **implications of EU-US data transfer** ban and IAB unlawfulness signify major inadequacies that cascade all the way down into the commerce landscape. The knock on effects will continue to flow through the chain and create opportunities for retailers to return back to their most unique differentiation: Trust.

Therein lies the big flip, a whole new alignment where traditional businesses will be able to invite **trust back into the brand-customer relationship**. Retailers who share history with households, on some occasions through generations, will recall the sustainable and ethical significance that the markets demand.

Who could have foreseen only five years ago that **the very companies that set the horizon of digital value**, such as Google or Meta, would now **receive such disapproval**?

Consequently, the customer surveillance practices that these players have anchored and their propagated presence across commerce technologies are now equally challenged.

To make matters more interesting, the new ePrivacy Regulation (which will extend and complement GDPR), is expected to see the light towards the end of 2022. A regulation that enforces customer's privacy by expanding cookie concerns to any form of customer tag, substitutes or alternatives.

The law on cookie consent is clear. Web users must be presented with simple choices. However, most sites still choose to make a mockery of the law and their customers through **skewed consent UIs**. These approaches will make those retailers a target for complaints.

There is a war between data business models and privacy advocates (ICCL, NOYB, etc). Privacy will always win because common sense wins.

The common sense behind any common person who innately knows that one's choices belong to oneself (as long as there is no harm).

When organisations see people's choices as part of their model, they disassociate themselves from people and naturally lose purpose, value and trust.



How can we improve your brand's Search & Discovery?

Get in touch and let's see!



emPATHY.CO

LONDON | NEW YORK | ASTURIAS | GALICIA