Thriving in the age of privacy regulation: A first-party data strategy

Lawrence Latvala

Americas Financial Services Industry Practice Leader, Teradata, USA

Lawrence Latvala is the Americas Financial Services Industry Practice Leader at Teradata. His remit encompasses such domains as customer experience, financial crime, chief financial officer analytics, open banking, pricing agility in insurance, risk analytics and payments. Prior to Teradata, Lawrence was Chief Revenue Officer for a FinTech firm. His experience also includes working in market development at Capgemini, as well as for Deloitte, E&Y and the US Defense Department. He holds degrees from the University of Chicago and the University of Rochester.

Teradata, 1 Penn Plaza, Suite 1610, New York City, NY 10119, USA
Tel: +1 917 579 4269; E-mail: lawrence.latvala@teradata.com

Jeff Horn

Americas Financial Services Industry Consultant, Teradata, USA

Jeff Horn is an industry consultant at Teradata, with a focus on the domain of customer experience within the financial services industry. His expertise in the field of customer experience solutions includes loyalty, campaign management, mobile applications and customer experience analytics. Prior to his current position, Jeff oversaw the implementation and customer success teams at Loyalty Lab, and led customer data strategy and implementation teams for Accenture.

Teradata, 1 Penn Plaza, Suite 1610, New York City, NY 10119, USA
Tel: + 1 901 219 3241

Bill Bruno

Chief Executive Officer, D4t4 Solutions Plc, USA

Bill Bruno is the Chief Executive Officer of D4t4 Solutions. He has over 18 years of experience in the media, data and analytics sectors, and is passionate about helping clients traverse the complex customer journey to generate return on investment and create a high level of transparency across all business initiatives. Prior to D4t4, Bill spent many years as CEO (North America) at Ebiquity — the company to which he sold his analytics business, Stratigent, in 2013.

D4t4 Solutions Plc, 215 E Chatham Street, Suite 215, Cary, North Carolina 27511, USA
Tel: +1 773 203 6596

Abstract   This paper reviews the recent legislative and policy changes in the area of consumer data privacy and their impact on the effectiveness of the most popular tool for tracking customers — the third-party cookie. With third-party tracking rendered mostly ineffective, the authors present the case for marketers to implement a stronger first-party data strategy to fill the gaps left by these changes. First-party data strategies provide significant advantages over third-party techniques, including broader controls for customer data capture and the ability to generate a deeper understanding of customer behaviour and intent; they are also easier to integrate into the marketing analytic and operational process. Additionally, the authors outline the advantages of a first-party data strategy for implementing real-time identification and tracking of customers — something

that third-party strategies cannot deliver. All of this can be achieved while staying in compliance with changing regulations that control the timing and use of customer data. Increasingly, the future of customer digital marketing is private, respectful, in real time and first-party.

KEYWORDS: data, regulation, privacy, digital, marketing, strategy, customer management

INTRODUCTION

Today's marketers face the onerous challenge of raising the bar to meet customer experience expectations while satisfying the laws and policies that increasingly restrict the use of customer data. The hard reality is that governments, political unions and individual companies are increasingly adding limits on how customer data collected by third-party applications can be stored, used and shared. Achieving this balance requires marketers to consider these fundamental questions:

- How are regulatory and policy changes impacting how a company identifies and interacts with its customers in a respectful but knowledgeable way?
- What strategies must be put in place to close the gap left by the deprecation of third-party cookies?
- What are the critical delineations in the marketplace between first and third-party solutions?
- What capabilities and benefits does a stronger first-party strategy enable in addition to regulatory compliance and respectful engagement?

The answer to these pivotal questions lies in embracing the power of first-party data and evolving one's marketing strategy to focus upon building stronger first-party data sets. First-party is now the definitive benchmark for capturing deeper levels of customer behaviour and intent in real time and using this information to analyse and orchestrate every interaction with customers. Increasingly, the future of customer digital marketing is private, respectful, real-time and first-party.

POLICY CHANGES AND THE SCRAMBLE TO SAVE THE THIRD-PARTY SHIP

Governments, political unions and companies are empowering consumers to control their own data. What has been seen to date is just the beginning of a living, breathing process. The General Data Protection Regulation (GDPR) in Europe, the Lei Geral de Proteção de Dados Pessoais (LGDP) in Brazil and the Personal Information Protection Act 2011 (PIPA) in South Korea are just a few of the recently passed international laws governing the collection and use of customer data. In the USA, the complexity is increased because laws are also passed at the state level and many states are in varying degrees of legislative consideration. In addition to the California Privacy Rights Act 2020, amending the California Consumer Privacy Act 2018, at least 42 state legislatures have proposed their own privacy legislation.[1] Figure 1 illustrates the notable jurisdictions around the world with consumer data privacy regulations.

The central tenet of current and emerging legislation is the ability to opt out, the right to delete and the need to ensure all marketing activities focused on personalisation, offers and building unique experiences are driven by compliant data.

Establishing and maintaining compliance presents a myriad of challenges from customer data capture, opt-in/out,

Figure 1: Notable jurisdictions with consumer data privacy regulations

monitoring and audit of use, and reporting. However, the core of compliance is identity management — the ability to accurately identify an individual — without which there is no way to ensure compliance across a customer's activity, preferences and time. If a company does not know who the individual is and is unable to retain preferences previously chosen, then it is at risk of capturing data when it should not be.

For years, tracking using third-party cookies has been the primary method for identifying and tracking customers. However, the new reality is that leading third-party technology solutions, including those that mask themselves as first-party, are no longer viable options for identifying and tracking customers on digital channels in a meaningful, compliant manner. Third-party tracking, with workarounds such as canonical name record (CNAME) and tag management, has introduced unnecessary complexity and risk. These legislative changes have finally caught up to marketers and advertisers, exposing their high reliance on third-party tracking to understand and sell to consumers.

Browser developers and mobile companies are also taking action to protect customer privacy. Companies like Firefox are implementing significant restrictions on tracking, rendering many cookie strategies ineffective. One of the most discussed examples of this is Apple's Intelligent Tracking Prevention (ITP), which limits customer data tracking via cookies to seven days for third-party solutions that use CNAME to mask as first-party cookies. Google will be following suit by phasing out third-party cookies from Chrome browsers in 2023,[2] meaning that over 50 per cent of US web browsers will no longer support third-party tracking, based upon market share.[3]

For mobile devices, both Apple and Google have a unique advertising identifier for each device running their operating systems. Apple recently implemented App Tracking Transparency, a policy requiring explicit opt-in permission for applications on iOS. Google is expected to follow suit with

some version of this for Android, but this has been delayed because of Google's new approaches being largely rejected as industry protocol. This will significantly decrease the amount of available third-party data available from these platforms for marketers and advertisers as many users will continue to opt out of tracking and data sharing across apps. Based on data from Flurry Analytics, since the introduction of App Tracking Transparency, US users agree to be tracked only 4 per cent of the time. The global number is significantly higher, at 12 per cent.[4]

Here, it is important to note that it does not matter whether marketers use true first-party technologies embedded in their brand's digital infrastructure or adopt third-party solutions (eg SaaS) that use DNS tricks to mask themselves as first-party applications — the same restrictions apply.

Inevitably, industry and third-party providers have scrambled to find technical workarounds to combat these policies. Although DNS and masking tricks like CNAME have been in place for many years, they have come under greater scrutiny during the past 12–18 months. However, for every offensive technology change that is created to take advantage of a loophole, a defensive counter measure is launched to close it. Thus, traditional third-party technology solution providers offer only temporary relief.

Other non-technical approaches to the problem exist but have limitations and have not demonstrated effectiveness. Data-sharing partnerships, sometimes referred to as second-party data and cohort-as-proxy approaches like Google Federated Learning of Cohorts (FloC) and Neustar, attempt to offer solutions to the third-party conundrum. In many cases, these arrangements require organisations to upload and share their first-party customer data, leaving open how said data will be used. It should be evident that moving first-party customer data outside a firewall represents

significant risk with little strategic thought behind it. Sending data outside the firewall also requires aggregation and anonymisation that inherently lowers the data's value for targeting purposes.

One other key point is that there are now several options in the marketplace that offer a new approach to using first party-data for advertising purposes, such as those from Nielsen, Acxiom and others. As these solutions entail giving up customer data, companies must approach them with a critical eye. It is essential to interrogate these options to understand fully how the data would be managed, stored and potentially shared with a larger audience in an anonymised way. In many cases, value can be achieved by controlling the data and selectively choosing what to upload when combined with a true first-party identity graph that is owned and controlled.

THE NEW REALITY

In short, the existing third-party approach no longer delivers the capabilities necessary for a targeted, digital experience.

If an organisation relies heavily on third-party data, this means there will be significant gaps in its ability to understand and communicate with customers in a timely and relevant way. With third-party data, companies can no longer persist, identify and recall who someone is across channel and device. This means they cannot generate the context needed to add value in the customer experience, thus limiting the potential effectiveness of real-time approaches. With consumers demanding a personalised experience in exchange for sharing data, this creates a potential issue for brands.

Most third-party solutions in the market rely on data-tagging. This is a complicated approach with less flexibility to respond to changes in market conditions. If the data are not tagged, or if the digital experience is updated, this will impair the integrity of the data, and critical events and behaviour

may be entirely missed. Should the strategy not align with a provider's pre-built tagging models, custom development effort will be required. Remedying these issues generally requires significant IT effort and integration, resulting in significant time and cost implications when changes are required.

When flexibility is compromised in this manner, any changes in compliance requirements will impact effectiveness and costs. Moreover, some solutions are simply unable to adapt to the constantly changing digital environment across web and mobile channels.

Compounding the situation is the fact third-party solutions cannot support the real-time use cases that effective digital customer engagement demands. Third-party tagging suffers from significant data latency issues, taking 30 minutes or more to provide customer context. This latency is far too long to manage the customer experience in the moment.

Gaps such as these impact the bottom line through loss of revenue and increased costs due to inefficient interactions with customers. These gaps include a fundamental loss in ability to understand the customer, their intermediate and long-term behaviour and, ultimately, their real needs. The result is inefficient targeting that is both more costly and less relevant.

Additionally, latency and tracking gaps prevent marketers from having deeply personal interactions with their customers. Real-time personalisation and interaction requires customer recognition and activity tracking with sub-second latency. This is critical to providing messaging that supports the customer's immediate intent in the moment.

THE FIRST-PARTY SOLUTION

So, the question is how do companies see and understand customers, respect their customers' wishes for privacy and utilise ethical analytics to interact with them in timely and relevant ways? The answer to addressing these gaps lies in embracing first-party data captured by true first-party solutions.

Simply stated, 'first-party data' refers to the data collected directly from customers and prospects using technology that is embedded in a company's digital infrastructure. As first-party data are completely within the company's control, using such data offers significant advantages:

- *Comprehensiveness:* First-party data are the most comprehensive and may be used to create a highly relevant data set of customers and prospects across digital touch points. Companies can capture behaviour and interactions across all channels. Capturing all customer digital interactions — scrolls, hovers, orientation, etc — enables insights that web analytics just cannot provide in a practical manner. Most importantly, using first-party data allows companies to create a complete customer view with all identifiers linked to both the individual and their behavioural and historical contextual data.
- *Accuracy:* Having a direct relationship with customers means the data collected will almost certainly be more accurate than third-party data. This is because first-party data are obtained directly from customers and prospects, while third-party data will tend to be aggregated from various data sets. Third-party data reflect a single point in time and will degrade in quality over time.
- *Relevance:* By using first-party data, the company gains specific valuable insights into exactly how its customers and prospects behave, putting it in a better position to determine audience preferences.
- *Cost-effectiveness:* Using first-party data is, quite simply, more economical than buying data from a third party. As a matter of course, most businesses already have the infrastructure to capture first-party

data. Where that infrastructure needs to be expanded as digital channels evolve, data may require more time and effort to collect, but even the cost of this will be outweighed by the benefits of having reusable data. This is a significant difference compared with third-party data where budget is spent on imprecise data aggregated into broad segments rather than detailed insights into individual customers. Ten segments of 10,000 customers will never be better than 100,000 segments of one.

- *Control and compliance:* Companies that own and control their data can build a dataset that is fully compliant with the privacy legislation in the marketplaces that are applicable to their business. It is important to remember that many of the recent browser changes are designed to protect the consumer from third parties taking advantage of them. Companies are capturing consumer data across a variety of touch points, and a best practice and future-proof approach would be to work with solutions that respect this approach and provide the full capability to manage what and who is tracked based upon their cross-channel and cross-device preferences.

- *Structure:* Whether the data are an input for attribution (any flavour), scoring models, machine learning or otherwise, the challenges for tag-based solutions tend to remain the same:
  ◦ lack of a data model and schema;
  ◦ accuracy issues or missing key elements of data;
  ◦ inability to structure the digital data output in a usable format;
  ◦ inability to deliver timely data for models that require more immediate inputs;
  ◦ lack of individual-level data; and
  ◦ inability to build cross-session attribute tables at an individual level.

Tag-based solutions, or those that rely on a data layer as a primary input, require

advanced configuration to ensure that the micro-interactions within a particular page or experience are not only captured, but also tied to the session and to the individual. Even the most complex implementations struggle to piece together customer journeys that span multiple sessions and devices. This is a core challenge for data science as many of these micro-interactions are signal inputs for the models being developed.

Furthermore, without the costly process of associating micro-interactions with downstream data, the lack of relational structure makes the data relatively useless for data science. The importance of having a data model and schema readily available from whatever vendor is being used to capture digital data cannot be overstated. This is a gap in the industry and something that companies might not realise is an issue until they try to connect the data from a marketing cloud or tech stack to an external system or vendor.

REAL-TIME CUSTOMER INTERACTIONS — THE KEY DIFFERENTIATOR

Latency of data capture can range from milliseconds to minutes or hours depending on the solution. Those of a third-party nature will inherently be slower and less comprehensive for many of the reasons discussed previously. True first-party data, however, can inform real-time targeting and action models that are exponentially more effective.

There is a good reason why most moments-based use cases do not actually happen in the moment: because to do so requires millisecond latency between the technological requirements. To be clear, in significantly less than one second, data must be captured and connected to a system of insight, and that insight must then be conveyed to a system of engagement (see Figure 2) — and this is something the vast

Know
the person

Recall
history & profile

Append
current session

Enhance
Identity Graph

Send
relevant data

Decisioning must happen in 200ms

celebrus•

Figure 2:   What must happen in real time to truly know and activate based upon the customer
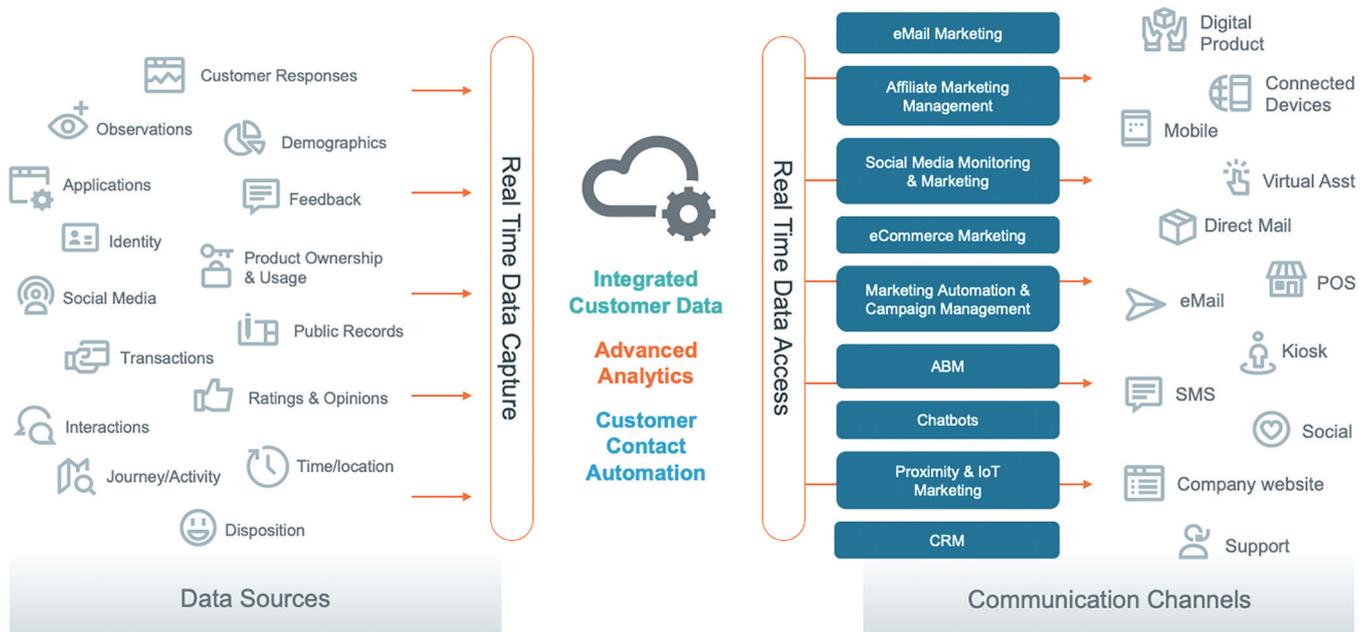
Figure 3:   Reference architecture for real time customer analytics and engagement

majority of martech stacks and clouds are simply unable to achieve.

The true goal should be to separate the data capture from the data activation and think of data as a foundational component that companies use in a 'collect once, use many times' approach. From there, the captured data can flow instantly into enterprise systems of insight and engagement, such as decisioning platforms, analytics environments and data modelling (see Figure 3).

WHAT CAN BE DONE WITH FIRST-PARTY DATA IN REAL TIME?
Determine identity
When someone arrives on company's website, mobile app or another digital channel, marketers can immediately

determine if the visitor is known based upon a persistent identifier on the device and whether this person has been there before. The history and profile attributes about that individual can then be recalled and be prepared to tailor each engagement using everything the organisation knows about that customer. This is one element of connected identity and has incremental benefit for financial crime interdiction as well, using the greater predictive power of integrated data.

Detect and capture digital behaviour

Having resolved the customer's identity when they first engage on a channel, companies can then detect and capture customer-specific digital behaviour at a granular level in the moment. Such data are immediately available to inform actions as the customer progresses through their session. Relevant data, from the current session or history or both, can be sent to the right systems in the right format to allow for decisions, A/B tests, triggered campaigns, audience updates and more. Companies are also able to append relevant digital interaction and identify graph data to the current customer data model to leverage across all marketing analytics, such as attribution and advertisement targeting.

Analyse and orchestrate the customer's experience

Artificial intelligence and machine-learning targeting and predictive models can leverage both immediately observed behaviour and historical context to drive extremely relevant interactions. 'Micro models' run in real time for individual customers and specify the next digital interaction — messaging, education, offers, etc — based upon the behaviour that immediately preceded it. Defined customer journeys, whether that involves account opening, path to purchase, or service recovery, can be managed more effectively using a more granular level of customer digital behaviour.

Build flexibility

First-party data capture is generally far more flexible and future-proof. Tagging implemented for current strategies often fails to capture all interactions that have relevance when market conditions and strategies change. The result is a need to change the technical implementation, which has lag time and increased costs. A strong first-party data partner will have solutions that are self-adjusting and capture all interactions that are potentially relevant. A strong partner will also have a low or no-code solution to extend the solution's capture of new behaviours.

DELIVERING INCREMENTAL VALUE THROUGH FIRST-PARTY ENABLED BUSINESS CAPABILITIES

A strong first-party data strategy provides value across the entire marketing process, yielding a breadth of revenue-generating and cost-saving capabilities. At the core of these use cases is 'identity', and solving for identity in a meaningful way is critically important on the path to value. While there are many identity graphs out there, the majority are third-party in nature and require companies to upload customer data. As a best practice, it is worth selecting a solution that offers a true, first-party identity graph that can be owned and controlled, and ultimately, streamline the consumer profiles across digital touch points. As discussed below, there are several critical elements to consider.

Identity graphs and profiles

Comprehensive identity graphs provide a complete view of a consumer across channels and devices from anonymous to known party solutions. Businesses often create multiple customer identities as individuals log onto different systems using

different devices and through different channels. A powerful data model can stitch these together into a seamless integrated view of a single customer. It sounds simple but it is vital for hyper-personalisation. Unfortunately, most data models serve individual silos and so do not cater to interactions with different customer IDs in different channels. They seldom provide a unified view of the customer across products, devices and channels.

Marketing decisioning

The ability to determine the significance of customer interactions with digital channels can optimise the effectiveness of downstream real-time interaction management and decisioning systems. Connecting customer data to real-time modelling environments can identify anomalous behaviour, which may signify risk. This data enrichment capability can also be used to identify opportunities. Behaviour occurring across all digital channels can be captured and connected to models operating in scoring environments that identify behaviours such as sustained, systematic searching for specific products or prolonged dwelling on product pages. Profiles augmented with this scoring data deliver more accurate 'next best' actions when customer profile data are connected to decisioning solutions, resulting in more relevant personalisation and higher conversion rates.

Attribution

Attribution reporting and models based upon tag-based solutions (ie cookies set by JavaScript) provide an inaccurate representation of the individual with potential gaps in visitor history in the event that a cookie has expired. Where a user has deleted a cookie before returning to complete a conversion or business-value event, companies might not be able to stitch those sessions together if the time between is more than seven days.

Furthermore, many attribution models include third-party advertising as an input, which is typically captured by third-party cookies. With third-party cookies and data under attack from the various browsers, this will require a new strategy and approach.

Personalisation

In a 2019 survey by Harris, 63 per cent of respondents commented that they 'expect personalisation as a standard of service'.[5] Indeed, according to Forrester,[6] 77 per cent of consumers have chosen, recommended, or even paid more for a brand that provides a personalised service or experience. First-party data provide the most complete context for personalising the customer experience as the data are sourced direct from the customer. This in turn provides the ability to deliver relevant experiences to customers at every moment across the purchase journey. Companies that can deliver personalised and relevant experiences can expect achieve cost savings of up to 30 per cent and revenue increases of as much as 20 per cent.[7]

Building deeper relationships

Companies have an opportunity to build trust and transparency around how they use consumer data. Consumers know when a company uses data that they have not provided directly and this has a negative effect on the customer experience. Thoughtful actions based upon first-party data are more likely to be relevant and perceived as valuable by the customer. This translates directly to revenue as 91 per cent of consumers are more likely to shop from brands that provide relevant product recommendations.[8]

Omni-channel management and measurement

Using first-party data on individual customers collected from all touch points, companies can see customers as they move

across channels on their path to purchase or on their path to attrition. These insights will allow organisations to pinpoint problematic parts of the customer journey more accurately and single out these areas to test and implement improvements in the customer experience. With such a complete and detailed view of the customer journey, companies can more easily segment and optimise for different audiences and guide behaviours that lead to conversion and retention.

Managing the customer journey

First-party data can be seen as the essential ingredient to attribution and to understanding the customer journey. Data from third parties may improve the short-term performance of marketing, but cannot explain the relationship with customers and their paths to purchase. First-party data, captured across channels, enables marketers to map the buyer journey, discovering the different steps that consumers take on their path to conversion as well as the order in which they take them. Marketers can then deploy the right message at the right time to move customers through the purchase cycle or intervene when the potential to churn has been identified.

CONCLUSION

The waning effectiveness of third-party customer data, driven by regulation and policy changes, creates an imperative for an alternative approach. Companies that do not adjust their data strategy in the face of these changes will see significant impacts to their ability to understand and engage customers in an effective and compliant manner.

Embracing a first-party customer data paradigm will not only minimise the impacts of these changes to their business but also realise the benefits of driving deeply relevant customer engagement. A first-party strategy is also critical for enabling real-time engagement for personalisation, targeted messaging and lead conversion on digital channels. Additionally, foundational marketing decisioning and attribution will benefit from a stronger first-party strategy.

Marketers should move quickly to engage their internal and external partners and begin executing a stronger first-party customer data strategy.

References

1. National Conference of State Legislatures, 2021 Consumer Data Privacy Legislation, available at: https://www.ncsl.org/research/telecommunications-and-information-technology/2021-consumer-data-privacy-legislation.aspx (accessed 8th October, 2021).
2. Goel, V. (2021) 'An updated timeline for privacy sandbox milestones', available at: https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/ (accessed 8th October, 2021).
3. StatCounter (2021) Desktop browser market share United States of America, June 2021, available at: https://gs.statcounter.com/browser-market-share/desktop/united-states-of-america (accessed 8th October, 2021).
4. Laziuk, E. (2021) 'IOS 14.5 opt-in rate — daily updates since launch', available at: https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/ (accessed 8th October, 2021).
5. Businesswire (2019) 'Redpoint Global and Harris Poll survey exposes gap between consumer and marketer expectations for customer experience', available at: https://www.businesswire.com/news/home/20190327005062/en/RedPoint-Global-and-Harris-Poll-Survey-Exposes-Gap-Between-Consumer-and-Marketer-Expectations-for-Customer-Experience (accessed 8th October, 2021).
6. Witcher, B. and Berg, D. (2016) 'Forrester Webinar — individualization vs. personalization', available at: https://www.slideshare.net/TrackIF/forrester-webinar-individualization-versus-personalization (accessed 27th October, 2021).
7. Patel, S., Field, D. and Leon, H. (2020) 'Responsible marketing with first-party data', available at: https://www.bcg.com/publications/2020/responsible-marketing-with-first-party-data (accessed 8th October, 2021).
8. Accenture Interactive (n.d.) 'Personalization Pulse Check', available at: https://www.accenture.com/_acnmedia/PDF-77/Accenture-Pulse-Survey.pdf (accessed 8th October, 2021).