

Winning with GDPR: How to build customer loyalty

The evolving role of identity in privacy and consent



Brought to you by

MYcustomer

In association with


FORGEROCK

Foreword

Whether you're managing the customer experience, marketing or digital operations, the single most pressing issue for you today is understanding your customer and their journey. The problem is that the modern customer journey is a complex web of interactions – cross-channel, cross-device, at any time, in any place. And of course, customers increasingly expect their interactions to be seamless, joined-up and personalised.

The reality is that organisations rarely have the structures, processes and technologies in place to deliver this kind of experience – or the single customer view that provides the platform for omnichannel service.

The result is a frustrated customer. And the concern is that unless this relationship can be nurtured, and trust developed, the customer will never willingly share the vital personal data that can support greater personalisation and better interactions, and ultimately foster a single customer view – for the benefit of both company and consumer.

Indeed, with the next wave of Big Data being heralded by the emergence of Internet of Things (IoT), and the countdown to the General Data Protection Regulation (GDPR) compliance well underway, data privacy has never been more important – ensuring that this is truly a pivotal moment for organisations as they seek to build more trust with customers.

The following report sheds light on the connection between customer experience, trust and data sharing, and surfaces the challenges and opportunities that exist. In collaboration with Survey Sampling UK, we surveyed 1,000 UK adult consumers who have at least one online account with a retailer, financial service provider or similar, in a bid to examine their digital experiences, where the disconnections arise, and the impact this has on customer relationships.

In this paper, I explore both the dilemma this presents, for equally frustrated businesses and their customers, and examine potential solutions - from the tactics being employed by consumers in the absence of better services, to the positive steps businesses can take to improve.

I also highlight why identity relationship management represents a key part of the solution and the difference it can make.



Paul Laughlin

Customer insight expert & consultant

Today's customers are complex

Modern customers are channel agnostic, and their purchase journeys are no longer linear, often hopping from device to device, and channel to channel, sometimes even within the same conversation.

A growing body of research demonstrates just how common the omnichannel approach to shopping has become. A 2015 study¹ found that eight out of 10 consumers now use a computer, smartphone, tablet or in-store technology while shopping.

Indeed, Accenture Strategy's Global Consumer Pulse Research² indicates that over half (51%) of UK consumers are comfortable crossing back and forth between multiple channels, even within a single interaction.

However, organisations have found it hard to keep up with the modern customer. A variety of organisational silos are undermining the customer experience, but the most damaging are often the channel silos that are so prevalent.

1. [Mastercard Omnishopper Report, 2015](#)

2. [Accenture Global Consumer Pulse Survey, 2016](#)

“Know Your Customer (KYC) initiatives have been a constant in all B2C organisations for at least a decade,” notes Doug Norton-Bilsby, Global Vice President, Retail and Consumer Products at ForgeRock. “Yet the concept of KYC across all channels of engagement still seems to evade even the most sophisticated businesses.”

Companies make it extremely difficult to interact with them across multiple channels without excessive effort. Customers often have to start the conversation afresh every time they shift to another channel, as well as re-establishing identification. Customers can be left feeling like they are known by one channel, such as their digital account, but treated as a completely new customer when walking into a store or calling a service centre.

Despite all our advances in available technologies, too few businesses are managing to offer a joined-up service across all channels. To create the seamless experiences that consumers seek, organisations need to move beyond segment-level ‘personalisation’ and targeting, to interactions guided by insights into individuals, based on data they have shared. But of course, this happens to coincide with the emergence of a more privacy-conscious customer.

So, what characterises the digital behaviour of today’s customers? What do they think of the digital services they receive? Do they trust businesses enough to share their personal data, and how can businesses engender greater trust?

Digital difficulties

The digital maturity of today’s customers is demonstrated in our research by the number of online services used by consumers of all ages, and the number of devices regularly used by them.

Our research revealed that across 30-50 year-olds, the average number of different types of services (i.e. banking, shopping, utilities, etc) used is over seven. Even 70-year-olds are using six digital services, on average. The most popular service is ‘communication’ (through email or messaging apps), with 93% of respondents using those. Also scoring highly, with over 80% of consumers, are online banking and non-grocery shopping. The least used service, by some way is health tracking through wearables (with only 21% using those).

Perhaps more telling is the average number of different digital devices used to access digital services. Using multiple devices is now the social norm.

Our findings also reveal that most consumers (54%) rate their digital services as merely ‘satisfactory’ to use. Only a third report that they find achieving their online goals to be ‘easy’, while 14% report the experience as ‘difficult’ or were forced to abandon their efforts altogether.

Our survey results demonstrate that difficulties are most pronounced when digital services are being used across multiple devices – a serious problem given the tendency of today’s customers to use several digital devices during interactions.

The top four issues, experienced by respondents, when using multiple devices, were:

- **48 % = Multiple logins**
Having to login again when switching device.
- **30% = Lost details**
Other devices lacking customer details already provided.
- **27% = Reset password**
Having to reset passwords on other devices.
- **22% = Lost preferences**
Other devices lacking user preferences already set.

Customer response

While the most likely reaction to problems (42%) is to take no action (British stoicism creeping in there, perhaps), 34% of consumers said they ended up ‘giving up’ what they were trying to do, and almost

a quarter (24%) said they decided to switch to another provider instead.

And there’s a further warning for organisations.

The ‘device rich’ digitally-savvy and more affluent consumers are the least tolerant - they are the most likely to switch provider (reported by 40%) and also the least likely to come back to a provider who is difficult to use. This compares to 40% of single device users, who take no action.

As far back as 2010³, the connection between Customer Effort Score (CES) and customer retention/loyalty has been highlighted, so these findings are not a great surprise.

But given that studies continue to demonstrate that customer retention remains one of the top priorities for most marketers, who simultaneously wrestle

3. [Harvard Business Review, Stop trying to delight your customers, 2010](#)

with average churn rates of 20%⁴, any cause of increased attrition should be addressed urgently.

Also of importance is that customers are not being passive in the face of their sometimes-frustrating digital life. In particular, with login difficulties proving to be such a major aggravation, users are exploring their own ways of circumnavigating the issue of multiple user IDs and passwords.

Our survey asked UK consumers which potential solutions they used to help them. By far the most popular solution (55%) was to simply save their passwords on each device (either manually or through option prompted by browser app).

However, social logins, involving sharing more data with Facebook or other social networks was still a popular option, with 29% choosing social logins.

Roughly 20% each made use of a password app, remaining anonymous or no solution (presumably relying on their memory).

This underlines how important it is for businesses to make multi-device switching as seamless as possible. Adoption of password apps and social logins, for example, is far greater amongst those regularly switching multiple devices. Consumers are not yet finding these services as easy as they should be, but they do offer some improvement. So, there is a prize to be gained by businesses that crack this.

“As we move towards a password-free society, organisations need to consider how, when and by which channel they start the movement to authenticate an individual consumer’s identity to enable frictionless engagement,” says Norton-Bilsby.

The erosion of trust

Perhaps unsurprisingly given these experiences, the level of trust that respondents have for their digital providers is somewhat limited. The majority (54%) who report their online ease as only ‘satisfactory’ rated their trust level as only ‘some trust’ (3.1 out of 5) – that is their level of trust in digital providers to use their personal data appropriately. This trust level falls below 3 (to ‘little trust’), for those who found it ‘difficult’ or abandoned use.

It is striking to notice, however, how this rating of trust improves for those consumers who found their digital services ‘easy’ to use. This group (33% of consumers), increased average trust rating to 3.4 (with more identifying as ‘mainly trust’ their provider to use their personal data appropriately).

4. [DataIQ Life events - the hidden marketing key to solving customer churn, 2016](#)

Clearly, those digital services that are difficult to use or require more effort will suffer from lower consumer trust. And with respondents telling us they have lower trust in providers to appropriately use their personal data, this means those organisations will struggle to encourage customers to share additional data with them.

On the flip side, this does suggest there is a great opportunity for businesses who can deliver better experiences. Making digital services frictionless, easier to use and seamless across different devices, could both please customers and foster greater trust, which in turn increases the likelihood of them sharing personal data.

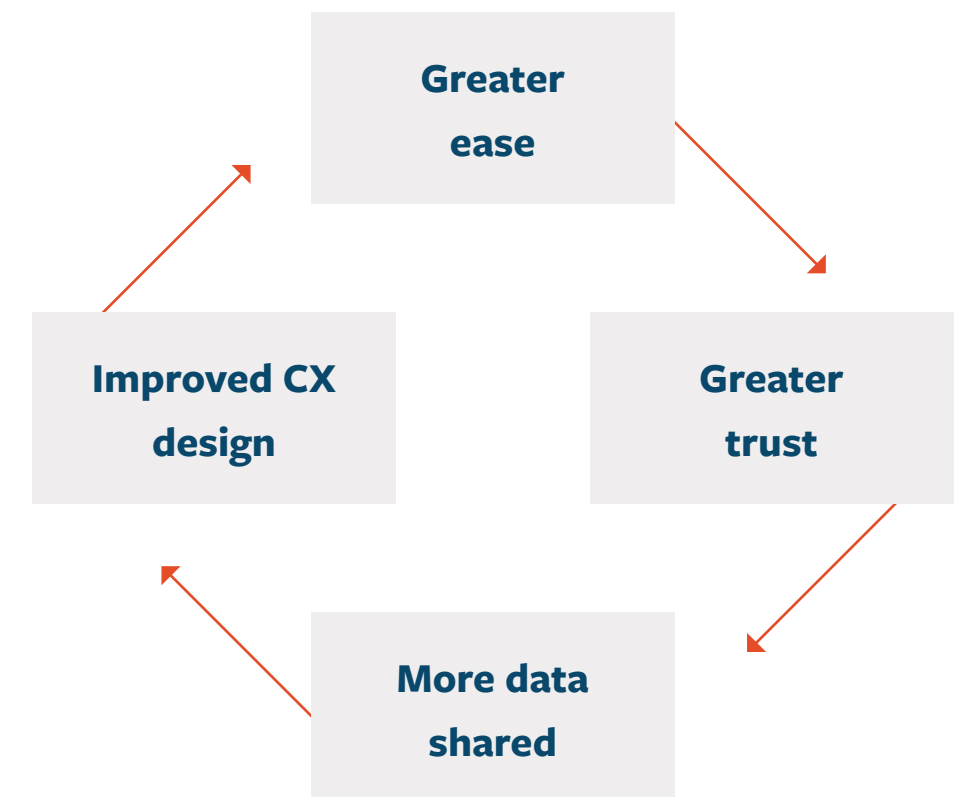
This presents the potential for a ‘virtuous cycle’:
when customers have a low-effort experience,

“Clearly, those digital services that are difficult to use or have a customer experience requiring more effort will suffer from less consumer trust.”

they trust the provider and share more personal data, the collection and use of which enables the provider to improve personalisation and automation of tasks, which in turn creates an even easier experience and fosters greater trust.

Norton-Bilsby notes: “As the social marketing strategist Ted Rubin said, ‘Indifference is expensive. Hostility is unaffordable. Trust is priceless. It’s all about relationships.’ Trust is the outcome of transparency and the more transparent organisations are with their use of consumer data, the more trust they will generate.”

The virtuous cycle of data value exchange





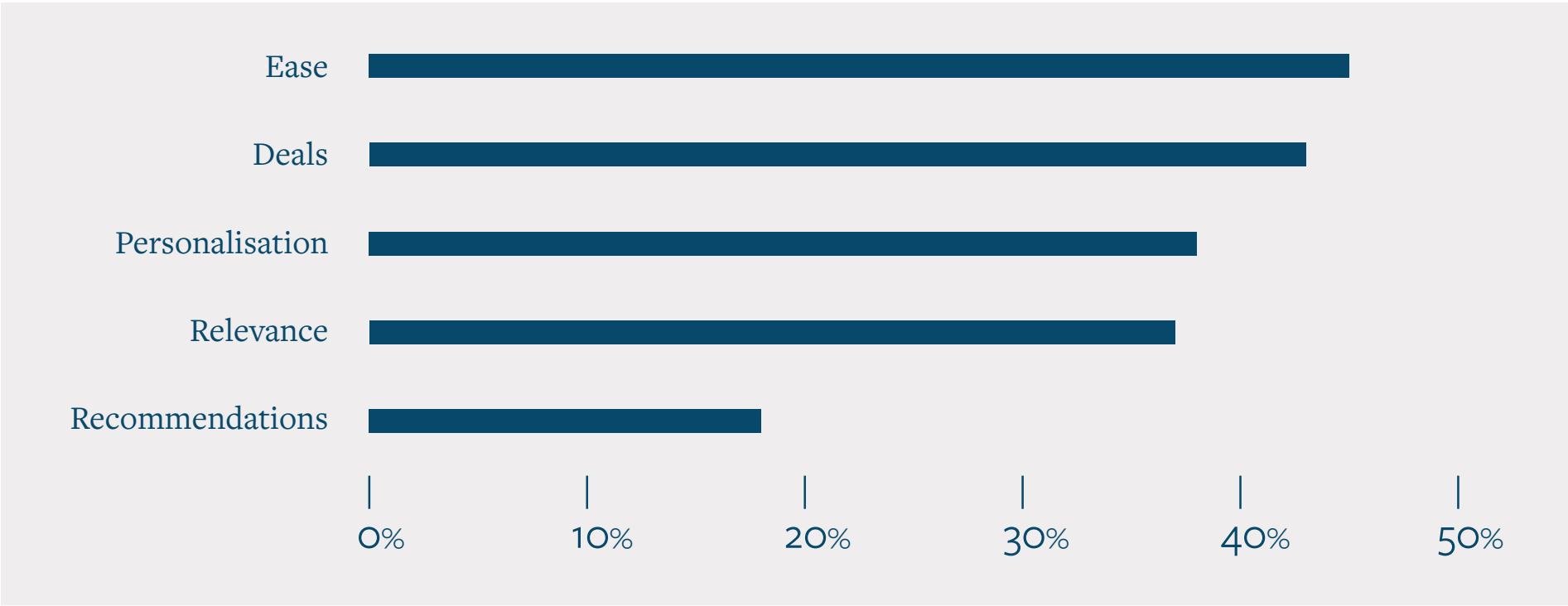
Incentivising data sharing

While trust is a major factor in whether customers are prepared to share personal data, businesses are also exploring a variety of other ways to incentivise data sharing.

A few examples include:

- **Improved customer experiences:** the promise of a simpler/faster experience if data is shared.
- **Exclusive deals:** offer extra discounts in exchange for more data.
- **Personalisation:** offer more personalised interaction, like the ‘corner store’ analogy.
- **Tailored communications:** offer better targeted comms that appear suitable.
- **Recommendations:** of products and services.

When our survey asked UK consumers about their willingness to share data, it was interesting to see which benefits were valued most highly. Across all consumers, the most appealing benefits were an easier customer experience (46%) and exclusive deals (44%):



Willingness to share data

Looking to act on those selections presents two challenges for businesses.

Firstly, focusing too heavily on exclusive deals can erode margin, especially if you don't yet have a good understanding as to the value of different data items.

Secondly, delivering an easier customer experience can be dependent on securing data first, so how can you bring it to life, to convince the customer to share?

Building on that last point, we examined whether trust influences the types of benefits that customers would prefer in exchange for data sharing. When we combine these two dimensions, we can see that greater trust does indeed increase openness to other 'data benefits'.

*“Only **68%** of marketers believe their businesses will be compliant by May 2018.”*

Those customers who distrust their digital service provider are not willing to consider the benefit of ‘recommendations’ and only 30% would choose either personalisation or more relevant communications. But openness to product recommendations grows as trust improves. Of those customers who state they ‘mainly trust’ their provider, 50% could be persuaded to share data in exchange for personalisation, relevance or recommendations.

GDPR and privacy

As if there wasn’t already enough incentive for organisations to foster trust with their customers, next year sees the implementation of the General Data Protection Regulation (GDPR). GDPR coming

into effect on 25th May 2018, at the heart of the regulation is the issue of consent, requiring that businesses make it as easy to withdraw consent to use their data as it is to give it. In other words, trust and permission not only needs to be earned in the first place, but also maintained.

The penalties for those that are in breach of GDPR are significant - fines of up to €20m or 4% of global turnover (whichever is the greater) are eye watering even for the most battle-hardened CEO.

But the risks of non-compliance are not confined to financial penalties, and the implications that it could have for the company’s reputation and customer trust cannot be underestimated.

Privacy matters greatly to consumers. Symantec research⁵ has revealed that 59% of UK consumers

are worried that brands wouldn’t keep their data safe and the study indicated that this causes Brits to self-censor the data they share with businesses.

According to research from DataIQ⁶, only 68% of marketers believe their businesses will be compliant by May 2018.

This is a shame because, rather than being seen as ‘the enemy’, most of the changes required by GDPR make good sense from a customer relationship perspective. Marketing thought-leaders including Seth Godin and Don Peppers have for years suggested businesses need to make the transition to truly permission-based marketing - an environment where customers are treated as owners of their own data and any usage of their data is transparent and for mutual benefit. “The concept of GDPR pushing organisations to help consumers manage and

5. [Symantec, State of privacy report 2015](#)

6. [DataIQ Life events - the hidden marketing key to solving customer churn, 2016](#)

“GDPR compliance should therefore represent an opportunity for organisations to rebuild trust and develop consumer confidence in the collection, storage and use of their data.”

control their ‘digital self’ will set a precedent for all future data transactions between customer and provider,” predicts Norton-Bilsby.

GDPR compliance should therefore represent an opportunity for organisations to rebuild trust and develop consumer confidence in the collection, storage and use of their data.

Now is the time to invest in a data strategy and infrastructure that enable firms to put customers back in control of their data. Demonstrating trustworthiness

in permission capture, honouring privacy and showing benefits for both parties from data sharing, has never been as important as it’s set to be within the next 12 months.

GDPR isn’t the only complexity on the horizon - the age of the ‘Internet of Things’ (IoT) is also shaking things up.

Take-up has not yet reached mass adoption, as shown by lack of reference to wearables, smart car or smart home technology in our survey. However, sales of

fitness trackers and smart watches continue to increase and internet connectivity is fast being added to most new household appliances.

This of course heralds the latest wave of Big Data for organisations to collect, manage and ultimately leverage to deliver more personalised and convenient experiences.

However, in light of GDPR and an increasing public awareness of data privacy, success in a multi-device world that includes smart watches, self-driving cars and data-driven fridges means an ever-greater need for transparency in relation to permission capture and data use.



“Now is the time to invest in a data strategy and infrastructure that enable firms to put customers back in control of their data.”



A recipe for managing customer identities better

For organisations to be able to deliver on the promise of a seamless, joined-up, omnichannel customer experience, that fosters trust in the context of the changing regulatory environment, a number of ingredients are required:

- **Compliant customer data capture:** *with recording of source and recency.*
- **Access for customers:** *to see/correct the data they have shared.*
- **Access for customers to change their permissions:** *by media/channel.*
- **A single customer view:** *Eliminate customer identity silos to enable informed and better engagement with customers in real-time, from anywhere, on any device.*
- **Personalisation capability:** *consolidating identity attributes and real-time context to offer better, personalized services based on real buying habits.*
- **An identity management solution:** *working across multiple systems, controlling access and managing relationships.*

Despite the business and technology press being dominated with stories about data, GDPR and privacy, relatively little is shared on the key topic of identity management. Yet ease of customer identification and a more seamless transfer of customer data are pivotal to improving the customer experience, something that is a primary goal for today's businesses.

Businesses are well-acquainted with using access management systems within their organisations, but in a world where customers own and share valuable data, there is a need for an equally secure but easy-to-use identity management solution.

ForgeRock was the first in the market to have coined the concept of Identity Relationship Management (IRM), as a step beyond customer identity and access management. In recognising the importance of consumers having

control of their personal data, ForgeRock was among the first to implement the User-Managed Access (UMA) standard. UMA is built upon the open standard, OAuth⁷, and gives individuals unified control over who can access their data, no matter where data or services reside.

This is not just a secure means of consumers identifying themselves (like a customer version of internal controls), but also an enabler of a more transparent relationship. Customers are able to share details with businesses and in exchange this enables them to see which data is shared with which service providers, maintain it and grant/revoke access as they wish. Thus this simultaneously resolves issues around trust and convenience.

Customer identity and access management solutions that are relationship-focused also support cross-device portability. Businesses can consolidate identity data of



7. [OAuth 2.0 authorisation framework](#)



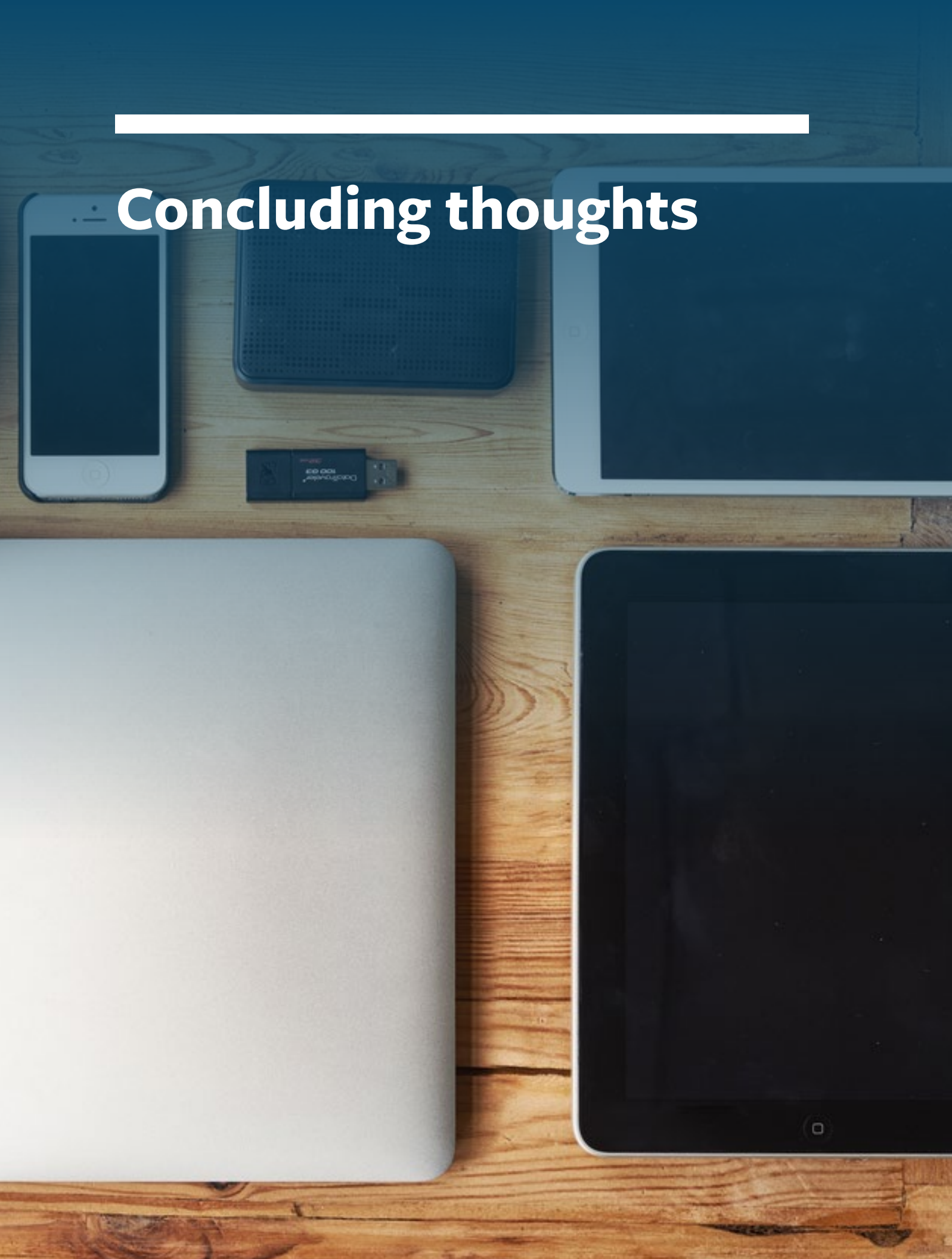
users, their devices, connected things, and preferences to create a unified customer profile across all digital channels, giving customers a seamless experience as they move across multiple devices.

This is especially important in the growing phenomena of information ‘ecosystems’. Consumers with multiple Apple, Google or Microsoft devices both have commitment to those ecosystems, due to existing breadth of content and have been educated to expect easy portability across devices with consistent access to the same data.

This brings us onto another benefit from consistent approaches to customer identity relationship management, in the commercial ecosystems emerging between different providers. Think Uber and credit card providers, Apple and app developers or public spaces and wifi providers.

Complementary services that should work well together, to better meet consumer needs, also rely on frictionless identification and sharing of data. A well-designed customer identity approach, supported by consistent technology offers the potential to maintain the same data transparency and consumer empowerment across these ecosystems. This would create a more trusted environment for consumers, to engage with multiple providers, and share more relationship-building data.





Concluding thoughts

In conclusion, we have seen the difficulties experienced by today's multichannel multi-device consumers.

And the complexities of the customer journey will only become more pronounced as new smart devices emerge and the need to control access to data in various media (including location and voice recordings), becomes more prevalent.

We have also seen the challenges that businesses face, such as legacy systems, dwindling levels of consumer trust, increasingly complex customer journeys, a growing number of channels and devices, and a lack of key infrastructure building blocks. Elsewhere, new regulation presents challenges, in the form of GDPR.

But in amongst these challenges there are also opportunities - to engage with customers more transparently, with open permission for data sharing for a purpose the customer can understand and value.

On the topic of new regulation, Norton-Bilsby highlights: “There are many benefits for organisations who lead the way on adopting all of the GDPR principles but top of the list should be the additional benefit of gathering more specific customer information - ‘Knowing Your Customer’ in depth, across all channels and serving them personalised experiences is the essence of competitive advantage.”

Indeed, as well as revealing the imperfect state of current digital experience, our survey highlighted the potential to develop a virtuous cycle - that by improving customer experience and improving ease of use, greater trust is engendered, which in turn encourages greater data sharing from the user,

which ultimately enables the provider to deliver an even better customer experience and more effortless interactions.

This is particularly timely - trust has never been more important, as we enter a permission-based age. Permission-based marketing, once a recommended strategy, is now becoming regulation.

Amidst the building blocks needed to get there, we saw that managing customer identities and their relationships was key, both facilitating improved experiences but also increasing trust. A solution conforming to the new UMA standard could distinguish providers.

“Permission-based marketing, once a recommended strategy, is now becoming regulation.”

There are already organisations embracing many of these change. Looking at the way the BBC has [launched its BBCID and MyBBC service](#), for example, highlights a brand grasping the opportunity of capturing and using data transparently.

However, I encourage all digital service providers to follow. Despite the risks and changes required, the opportunity to reconnect with customers and earn their trust is one not to be missed. If they can help make digital experiences easier and trustworthily transparent, then all our digital lives might just start living up to our earlier aspirations.



About ForgeRock

ForgeRock® is the digital identity management company transforming the way organisations interact securely with customers, employees, devices, and things. Organisations adopt the ForgeRock Identity Platform™ as their digital identity system of record to monetise customer relationships, address stringent regulations for privacy and consent (GDPR, PSD2, Open Banking, etc.), and leverage the Internet of Things. ForgeRock serves hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, TomTom, and Pearson, as well as governments like Norway, Canada, and Belgium, securing billions of identities worldwide.

ForgeRock has offices across Europe, the USA, and Asia.

Get free downloads at:

www.forgerock.com

and follow us [@ForgeRock](https://twitter.com/ForgeRock)



About MyCustomer

MyCustomer.com is Europe's leading online resource for customer-focused professionals, with over 100,000 members. Sharing news and advice on fields including customer service, marketing, sales and CRM. MyCustomer.com is a vital hub for business leaders looking to enhance every part of the customer experience they deliver. With a network of expert contributors from around the globe and a focus on strategy, technology and in-depth research, members of the MyCustomer community are able to tap into a wealth of knowledge and receive the most comprehensive view of the trends affecting and influencing the world of customer management.

Join the community:
www.mycustomer.com

