Publication date:
21 Aug 2019

Author:
Eden Zoller
Omdia Distinguished Analyst & Principal Analyst, Smart Living

Making Privacy an Asset in the AI Era: Best Practice

Brought to you by Informa Tech

Table of Contents:

Table of Figures:

Summary

In brief

Ovum's data privacy best practice recommendations go beyond the basics stipulated by the General Data Protection Regulation (GDPR) and similar regulations, which should be viewed as the starting point and not the end game. Ovum's objective in this report is to raise the bar further by giving service providers a practical, actionable guide on how to adopt a consumer-first, data friending approach to privacy. Ovum's recommendations consider the impacts of artificial intelligence (AI) on data privacy, examined in the complementary report in this series *Making Data Privacy an Asset in the AI Era: Mastering Market Dynamics.* By following our best practice guide, service providers will be able to change the data privacy dialog from a negative to a positive conversation, increasing trust in data privacy to the benefit of both consumers and service providers.

Ovum view

- **Consumers have a complex relationship with privacy that needs careful segmentation.** Consumers have differing privacy profiles depending on a range of factors, and identifying the nature, motivations, and different data privacy needs of consumers is an important step in better supporting customer needs. Ovum has created a data privacy segmentation framework based on four key profiles: privacy activists, privacy rationalists, the privacy perplexed, and the privacy indifferent.

- **Empowering consumers encourages data sharing.** This is underscored by Ovum's *Digital Consumer Insights 2019* survey, which reveals that the most effective way to make consumers more comfortable sharing their data is to give them agency over that data, for example, by telling them exactly how their data is used and who it is being shared with (65%). Moreover, a comparison across Ovum's 2018 and 2019 surveys reveals that consumers' desire for control has significantly increased.

- **Privacy processes, particularly consent, are still a burden for consumers.** Legislation has tightened laws around consent in an attempt to make organizations more accountable, but the way that this has been implemented means even more hassle for consumers. This is pronounced with cookie consent, with consumers being bombarded by cookie consent boxes, directing them to a mass of small print which is hard to navigate and confusing.

- **AI predictive consent is attracting attention but is currently "too much too soon."** Machine learning (ML) models have the potential to leverage a user's data privacy profile in ways that can support predictive consent, granting or denying it on behalf of the user. This can be appealing in the context where users interact with multiple services at any one time, but the reality is that AI-powered consent faces several steep hurdles, notably lack of consumer trust in such models and the potential risk of inaccuracy and of getting consent wrong.

- **Personal data exchanges (PDEs) have potential but face significant barriers.** PDEs are mediated platforms that allow consumers to monetize their data by exchanging it with third parties in return for value of some kind. PDEs are potentially disruptive to traditional internet monetization models, but so far PDEs have not taken off in a significant way. Key reasons for the low take-up include lack of consumer trust, the consumer's lack of understanding of the value of their data, and consumers being too deeply locked into data super platforms such as Google and Facebook.

Recommendations for consumer service providers

- **Have strategies and tools tailored to each consumer segment, and tackle the problematic groups head on.** For example, data privacy activists are motivated and unforgiving, and although they are in the minority they need close attention, because they will be vocal critics of service providers that they believe have poor privacy credentials. They will also be the most likely to churn as a result. Meanwhile, the data privacy indifferent are a vulnerable group: they will not read the small print, will not proactively protect their data, and in some cases can be reckless.
- **Approach data privacy and data security in tandem.** Ovum's *Digital Consumer Insights 2019* survey shows that consumers are concerned equally about issues relating to data privacy and data security. Although the two are different, they are connected and should ideally be treated in parallel, particularly as there are elements of data security that can safeguard data privacy, for example, identity management tools that can help maintain the integrity of personal data.
- **Communicate your privacy credentials in a relatable way that resonates with consumers.** Service providers must not only have comprehensive data privacy solutions and practices in place but must be seen by consumers to have them. The company's data privacy policies and procedures must be relayed to consumers in a positive, easy-to-understand way; you do not want to scare consumers with a negative dialog that is the typical messaging around data privacy and security.
- **Make consent friction free for consumers, and show them the benefits.** Consent is presented as a complex and confusing compliance process, and this clearly needs to change with greater transparency and better, more intuitive design (e.g., using visual elements). Consumers should also be told how they can benefit from sharing data, but this must be expressed in concrete experiential terms instead of in the abstract way that is common practice and leaves consumers cold.
- **Service providers must build consumer-first personal privacy management frameworks.** Key components of such a framework include an intuitive user interface; a data vault containing privacy settings, data storage, and data categories; and a data time line. The framework should also offer a selection of data privacy tools and value-added services. A holistic framework of this kind creates a positive, valuable data privacy experience for consumers.

One size does not fit all: the need for data privacy segmentation

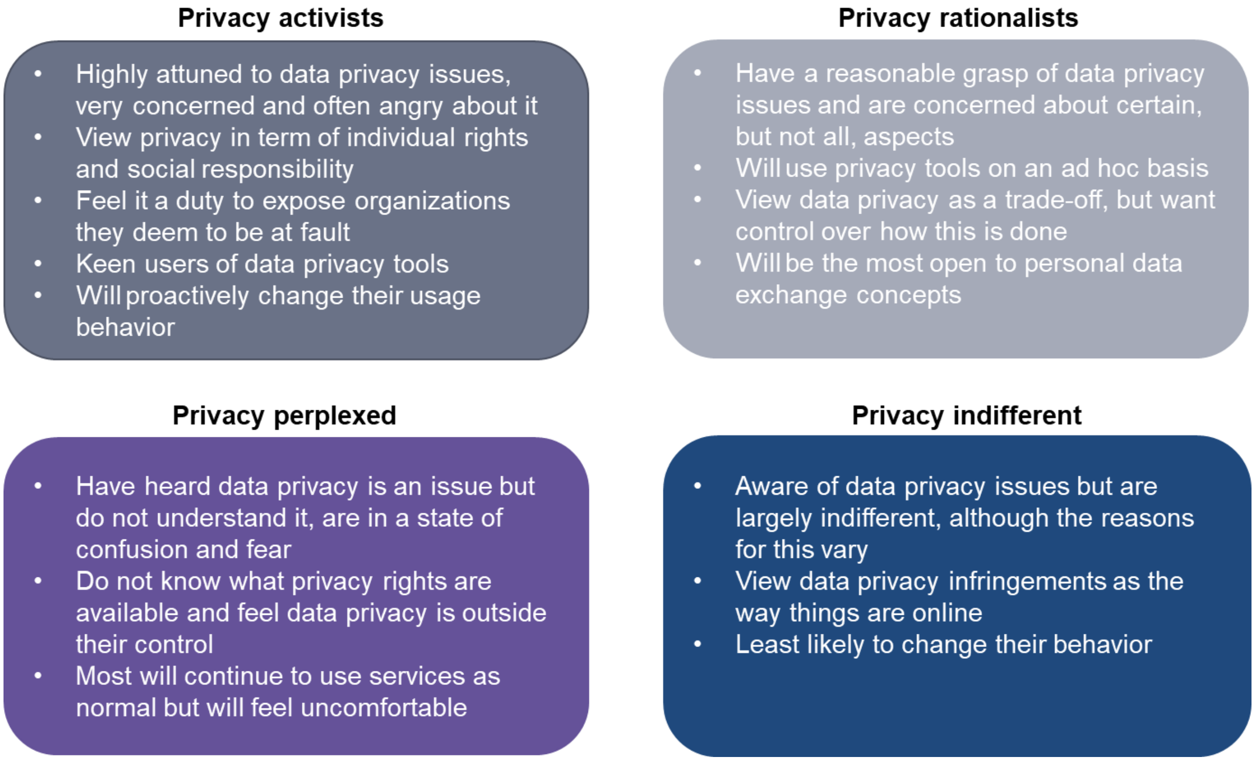
Consumers have a complex relationship with data privacy

Thoughtful segmentation is needed to reflect this

Most people express some degree of concern over data privacy and find common ground on key pain points, notably security. This came through in Ovum's Digital Consumer Insight survey findings shared in the first report in this series. But a deeper investigation shows that consumers have differing, more nuanced privacy profiles depending on a range of factors including age, digital knowledge and experience, digital service consumption patterns, and wider cultural and societal outlooks. Identifying the nature, motivations, and needs of different data privacy segments will allow service providers to support customers better and to devise policies and practices that speak to the particular requirements of each segment. Ovum has created a data privacy segmentation framework (summarized in Figure 1) based on the four key profiles: privacy activists, privacy rationalists, the privacy perplexed, and the privacy indifferent. This segmentation provides a solid starting point for service providers, but they will need to further refine it to reflect the particular dynamics of their own markets and customer base.

Figure 1: Ovum consumer data privacy segmentation

Figure 1: Ovum consumer data privacy segmentation1



Privacy activists

- Highly attuned to data privacy issues, very concerned and often angry about it
- View privacy in term of individual rights and social responsibility
- Feel it a duty to expose organizations they deem to be at fault
- Keen users of data privacy tools
- Will proactively change their usage behavior

Privacy rationalists

- Have a reasonable grasp of data privacy issues and are concerned about certain, but not all, aspects
- Will use privacy tools on an ad hoc basis
- View data privacy as a trade-off, but want control over how this is done
- Will be the most open to personal data exchange concepts

Privacy perplexed

- Have heard data privacy is an issue but do not understand it, are in a state of confusion and fear
- Do not know what privacy rights are available and feel data privacy is outside their control
- Most will continue to use services as normal but will feel uncomfortable

Privacy indifferent

- Aware of data privacy issues but are largely indifferent, although the reasons for this vary
- View data privacy infringements as the way things are online
- Least likely to change their behavior

Data privacy activists

A motivated and unforgiving minority

This group is a small, proactive segment. Members are highly attuned to data privacy dynamics and have the best grasp of data privacy issues and what is at stake. Many data privacy activists will be aware of how AI is starting to impact privacy and raise the stakes. They are most likely to be digital-native millennials (people born between 1981 and 1996, but the span can vary) or digitally competent baby boomers (born between 1946 and 1964, but this can vary) with a high level of distrust in how enterprises handle data privacy (and other issues). People in this segment are concerned about most aspects of data privacy and, in many cases, are made angry by perceived failings in this area. They see data privacy not just in terms of individual rights but also in terms of broader social issues and responsibility. They want to do something about data privacy and will keep a close watching brief on service providers and feel it a duty to report and expose those organizations they consider at fault on social media and other channels. They will interrogate data privacy settings and statements very closely and want to have maximum control over data destiny. Members of this group will be the most proactive in changing their behavior if they do not trust and are not happy with a service provider's track record on data privacy and how it approaches it. Data privacy activists will churn from a service provider they are unhappy with or, at the very least, use services less.

Actions for service providers

Data privacy activists form the most challenging segment for service providers to address, but ignoring them is a mistake, because they will hit back at service providers with a poor track record in data privacy. They will also be the most likely to change their service usage behavior, which could damage service revenues. Conversely, they will show goodwill toward and esteem companies that have strong privacy credentials. Apple's stance on data privacy will make it the poster child for this group. Service providers should look to engage this group with strong evidence on regulatory compliance and how they are moving beyond this along with strong positioning on data privacy social responsibility. They should provide data privacy activists with services that put them in control; this group will be most likely to use the data privacy protections and tools made available to them. Ovum suggests providing a feedback mechanism for this group and being responsive to comments. It is better to handle this via your own channels than see it after the event on social media.

Data privacy rationalists

Pragmatists that view data privacy as a trade-off

Data privacy rationalists will be digitally savvy, high-usage consumers who place a high priority on value for money. They are aware of data privacy issues and have a reasonable grasp of what is at stake. Data privacy rationalists are concerned about certain, but not all, aspects of data privacy but nowhere near as much as the privacy activists. They are more likely to use a service less for a short time rather than churn on principal if a service provider has a less-than-stellar track record on data privacy, and they tend not to view data privacy through the prism of social responsibility. Data privacy rationalists will be aware of data privacy settings and will focus primarily on how easy and fast they are to navigate. They have a very pragmatic approach to privacy and will be interested in trade-off scenarios in which they share data in return for value.

Actions for service providers

Privacy rationalists will respond best when data privacy is expressed and positioned in terms of the value it presents. They will be interested in the concept of PDEs, but they will have high demands in terms of how PDEs are supported. This group will want to have control over how a data exchange is handled rather than have a service provider dictate terms. Moreover, they will not approach data exchange as a blanket exercise but rather on a case-by-case basis depending on what they get for the data they give. Privacy rationalists will appreciate access to data privacy and security tools, but they are likely to use them more on an ad hoc basis than as a matter of course. But this does not mean service providers can cut corners; this group will apply a value lens to any additional services provided.

The privacy perplexed

Confusion and unease rule

The data privacy perplexed typically comprise an older demographic, and while some may be confident users of digital services, others will be less savvy. Consumers in this segment are aware, largely because of media reports, that data privacy can be an issue but do not really understand it and are in a state of confusion, doubt, and even fear. They care about privacy but feel it is beyond their control and that there is not a lot they can do about it, even though they may want to. The endless privacy statements and requests to accept/decline terms leave them dazed. They do not know what data privacy rights and protections are available to them and, as a result, feel helpless. When breaches and scares do occur, most will continue to use services as normal but will feel uneasy. However, a few will use services less, seeing this as the only way they can reduce being exposed to any negative impacts posed by data privacy vulnerabilities.

Actions for service providers

This group is characterized by fear and doubt, and if this is allowed to escalate, more consumers in this segment will use services less with a negative impact on revenue. Service providers should also pay close attention to those consumers in this group that are carrying on as normal; this is not because they are happy and relaxed, but because they feel helpless. The damage here is more insidious. Confused consumers who feel at the mercy of uncaring service providers will become resentful, which will erode overall trust. When standard contracts end, their poor experience of data privacy will be a renewal consideration factor, even if it is not consciously front of mind.

Providing these consumers with transparent, intuitive tools to navigate and manage data privacy will engender trust and goodwill. There is also great value in educating these consumers about data privacy, although this must be framed in a positive conversation: you do not want to make them more uneasy and fearful. Handled correctly, data privacy education will remove confusion and make this group feel empowered in a way that will foster goodwill toward the service provider.

The privacy indifferent

A broad, mixed group that is more complex than meets the eye

This is a varied group that includes digital savvy users from a young demographic – earlier millennials and Generation Z in particular. They are totally habituated and at ease with sharing data on social network and messaging platforms, with little thought of the consequences. But the data privacy indifferent groupalso includes an older demographic of less digitally literate users, who have probably picked up on data privacy stories in passing but for whom it has not registered as a pressing concern; they feel there are more important things to worry about.

The predominant feeling about data privacy is indifference and lack of deep concern. The privacy indifferent are aware of data privacy issues in broad terms, but they do not reflect much on the implications and risks involved in sharing data. They tend to view data privacy breaches as just the way things are online, and there is a feeling that infringements do not happen often, and when they do, they happen to other people and not to them. Although the younger people in this segment will use multiple service providers, try new things, and switch at the drop of a hat, data privacy will not be a prime motivation for doing so. The older demographic are more static in their digital behavior generally, and for them the prospect of switching a provider because of data privacy issues is more trouble than it is worth: there is a prevailing feeling of "better the devil you know."

Actions for service providers

The fact that these consumers are indifferent to data privacy makes them hard to address, doubly so as the indifference is coming from very different places depending on age and digital habits. Being indifferent to data privacy may sound like a relaxed place to be, but it is far from ideal and could make consumers vulnerable. Younger people in this group are prone to being reckless with their data, while the privacy indifferent as a whole will tend to take few if any measures to protect their data and will certainly not look at any small print. Service providers need to educate and encourage this group to be more mindful. Data privacy measures and tools will need to be very assessable and easy to use, otherwise this group will not bother. They need to feel that the ability to control their data is a good thing and worth the effort. A more data privacy-aware and responsible customer base will ultimately benefit service providers.

Security and privacy are best treated in tandem

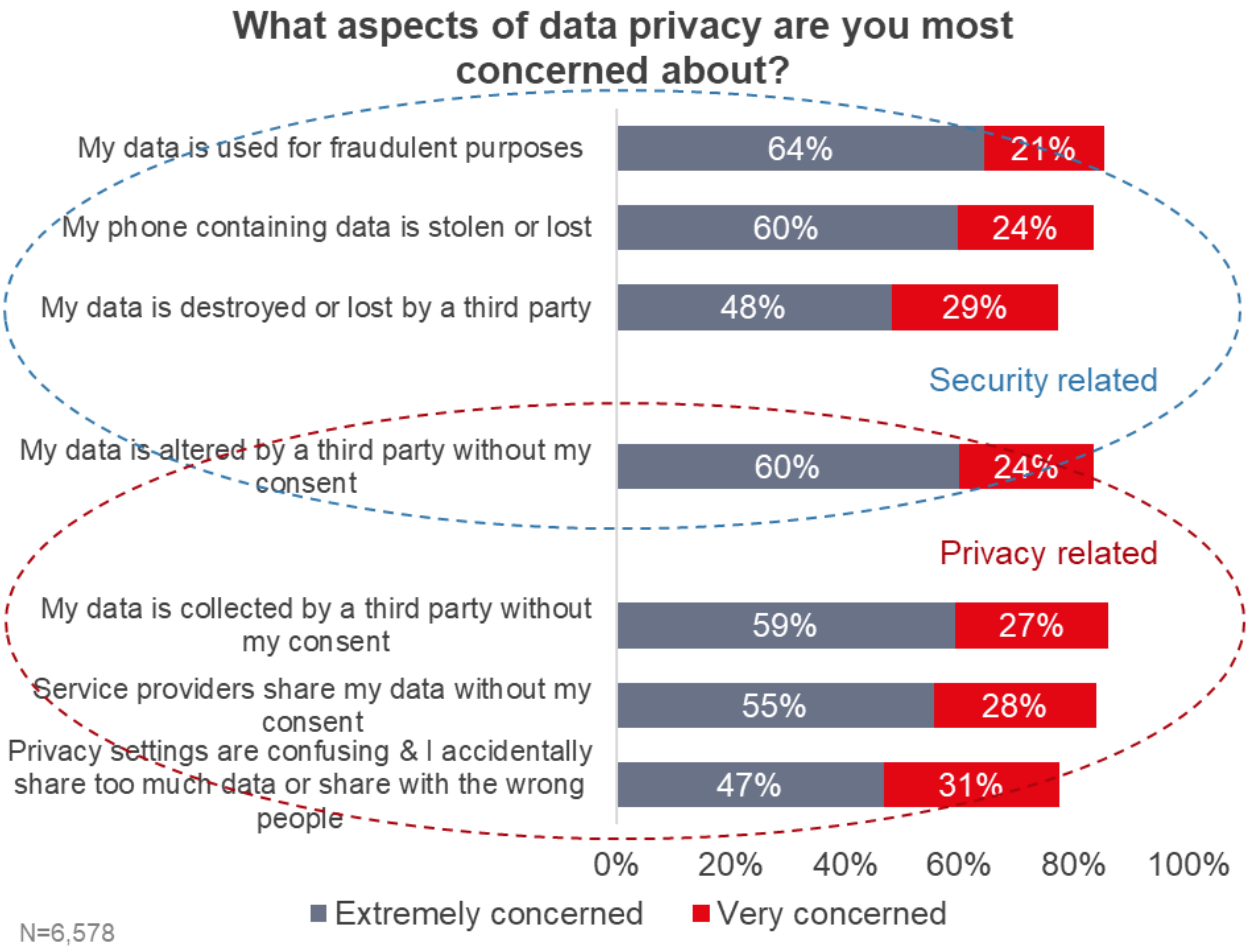
Data security and privacy are different but closely connected

Data security and data privacy are different but closely related, and although this report is principally about the latter, it is important that service providers understand the connection. Data security is focused on maintaining the integrity of personal data and protecting it against unauthorized access and fraudulent misuse of various kinds. Data privacy is focused on governance: Who has legitimate, authorized access to personal data, and how may or may not that data be used with respect to individual privacy? Data privacy is grounded in regulations and legal process and has strong ethical connotations. Data security is focused on the technical solutions and processes for protecting personal data. Data security tools include data-loss prevention software, antivirus protection, fraud protection software, and identity management tools.

In Ovum's *Digital Consumer Insights 2019* survey on data privacy, consumer concerns are fairly evenly split between data privacy-related issues and those linked to data security, as shown in Figure 2. Although data security and data privacy are different, the two are, as noted, connected, and there are elements of data security that can safeguard data privacy, for example, identity management tools that can, among other things, help maintain the confidentiality of personal data. Service providers must try and treat the two in an integrated fashion, being mindful of where data security can work to the benefit of data security.

Figure 2: Consumers have multiple concerns when it comes to data security and privacy

Figure 2: Consumers have multiple concerns when it comes to data security and privacy2



Communicate your data privacy and security credentials

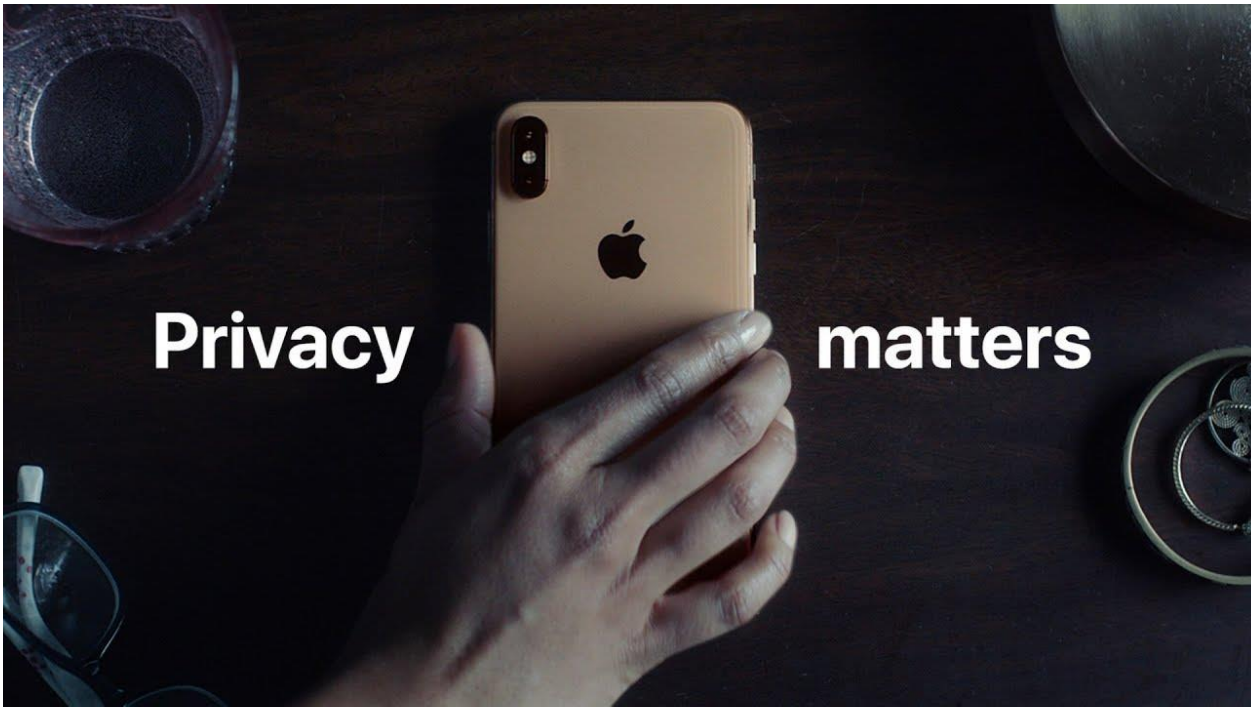
But do so in a way that is positive and relatable

Service providers must not only have comprehensive data security solutions and data privacy governance in place but must be seen by consumers to have them. It is no good having strong systems and policies if consumers do not know about them or understand their benefits.

It is also important that you communicate your data privacy and security credentials in a positive way, rather than scaring consumers with a negative dialog that is typical of the messaging around data privacy and security. A good example of how to get it right is Apple, which is building a reputation as a data privacy champion. In March 2019 Apple kicked off a TV campaign in the US to promote its data privacy credentials, the first time it had done so in a high-profile national ad campaign. The short, funny, and relatable 45-second slot shows how people try to guard their privacy in everyday life: no-trespassing signs and people closing window blinds and doors, shredding documents, locking drawers, and so on. The advert closes with the tagline: "If privacy matters in your life, it should matter to the phone your life is on. Privacy. That's iPhone." This is simple but effective messaging, as captured in Figure 3.

Figure 3: Still from a closing shot of Apple's US privacy TV campaign

Figure 3: Still from a closing shot of Apple's US privacy TV campaign3



Empowering consumers encourages data sharing

Give consumers more control over their data

People like to feel in control of their lives, and this applies as much to their digital identities as it does to their finances or health. The desire to be in control resonates with data privacy, as shown by Ovum's Digital Consumer Insights survey on data privacy (see Figure 4). The results reveal that the most effective way to make consumers more comfortable sharing data is to give them greater control over that data, so that they

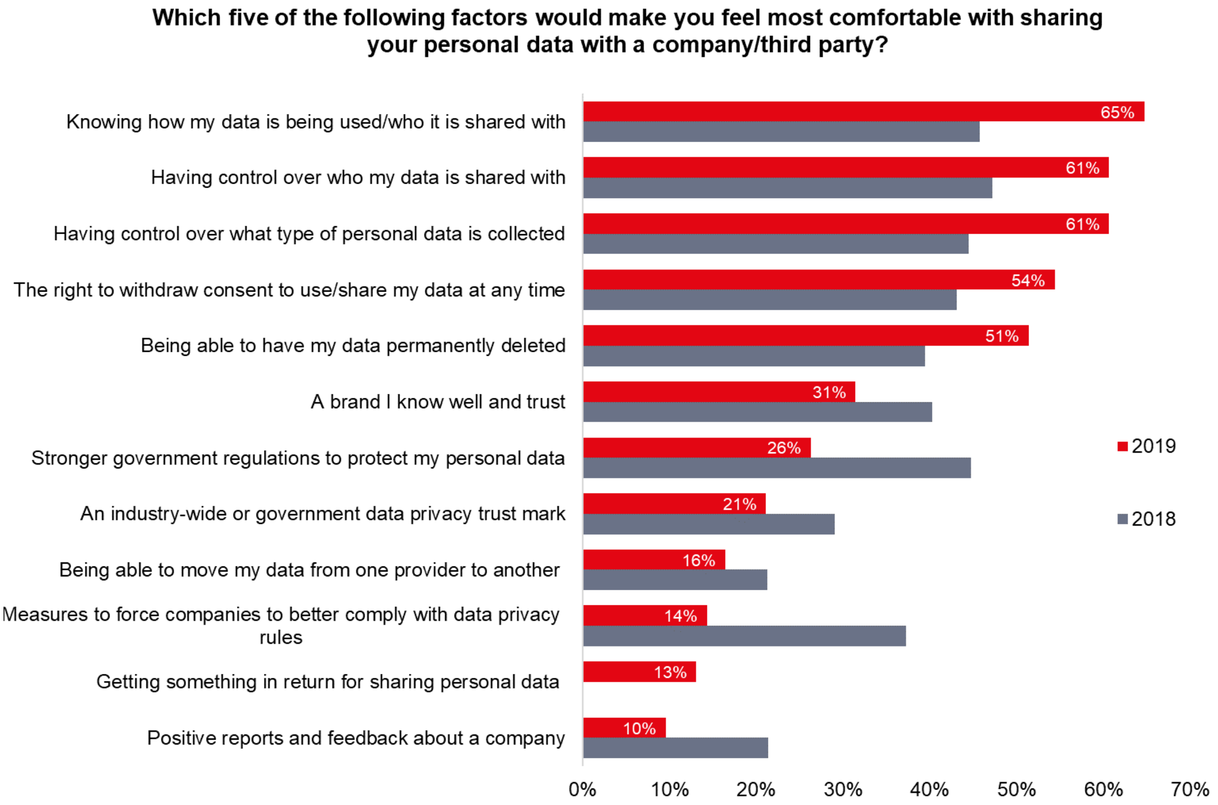
- know exactly how their data is used and who it is being shared with (65%)
- have control over the types of data collected (61%)
- have control over who their data is shared with (61%)
- can withdraw consent to use and share their data at any time (54%)

- can have their data permanently deleted (51%).

What is particularly interesting when the results are viewed across the 2018 and 2019 surveys is that consumers' desire for control has increased substantially. This is a powerful message for service providers.

Figure 4: Factors that make consumers more comfortable sharing their data

Figure 4: Factors that make consumers more comfortable sharing their data4



2018, N=5,122; 2019, N=6,578

Most of the control-related elements tested in the survey are captured under GDPR, although most consumers will not be aware of this. GDPR's remit is focused on the EU, but given how much consumers value the control and accountability principles enshrined by this regulation, Ovum recommends that all companies align with GDPR, whether they have to or not.

Consent must be made friction free for consumers

Regulations have tried to make consent more effective

Consumer data insights are the foundation of an increasing range of business models and monetization opportunities, as examined in the complementary report in this series, *Making Data Privacy an Asset in the AI Era: Mastering Market Dynamics.* Consumer service providers and other organizations need data insights to enable digital commerce and financial transactions, to enhance personalization, and to feed the predictive analytics that fuel recommendations, cross-selling, and upselling. This creates an unstoppable need to keep the data flowing. Obtaining consumer consent to use their data has long been recognized as an industry best practice, but in reality this has not always been followed, and in some cases it has been handled in ways that are dubious at best. This has prompted regulatory intervention and increasingly strict rules on consent, most conspicuously with GDPR, although other regulatory regimes are looking to follow the EU's lead in tightening how consent is handled.

GDPR has tightened laws around consent to access and process consumer data, making it a requirement that consent is explicitly requested by an organization (data processor) and given by the consumer (data subject). GDPR consent also applies to cookies, which as we will see below are proving particularly problematic.

GDPR states that consent must be freely given, informed, for specific purposes and unambiguous, and obtained prior to processing consumer data. Freely given consent means that it cannot be bundled into service terms and conditions unless consent is needed to provide the service (e.g., passing address details to a courier for product deliveries) and that people should be able to refuse or withdraw consent without being penalized. Taken together, this is meant to give consumers more control and choice over how their data is being used. Conversely, if a person is given no real choice, then consent is invalid and in breach of GDPR.

But despite new rules, consent is still a burden for consumers

Cookie walls are a flash point and are best removed

But the reality for consumers post GDPR is proving very different, with the burden of consent being placed on consumers and in a highly negative way. Cookie consent is a particular problem. Consumers are being bombarded by cookie consent boxes that pop up on websites and in apps, directing them to a mass of small print on data privacy rules and uses that are hard to navigate, confusing, and time consuming. In some cases, there can be a threat that services cannot be used unless cookie consent is given, a setup often referred to as "cookie walls." The situation is made worse – and even more confusing – by the multiplicity of ways that cookie consent is handled across different websites and apps. Faced with these scenarios, most people simply comply and give consent. Handling consent in this way leaves consumers feeling frustrated and coerced, which is hardly conducive to fostering trust.

Regulators are stepping in

Regulators are continuing to scrutinize consent closely, particularly when it comes to cookie walls where consent is not freely given as per GDPR stipulations. For example, in March 2019, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) said that organizations implementing cookie walls do not comply with GDPR. The authority is on the lookout for cookie walls and has already contacted firms asking them to better align with GDPR consent rules on this front. The European Data Protection Board (EDPB) has taken the same stance. The message is clear for consumer service providers and other organizations: if you have implemented cookie walls, you should look to remove them. They are a clear cause of frustration for consumers and put you at risk of being in breach of GDPR consent rules.

More complexity on the horizon

AI will make consent more complex in certain scenarios

In *Making Data Privacy an Asset in the AI Era: Mastering Market Dynamics*, Ovum examined how AI has the potential to bring new complexity to consent and other GDPR principles, and it is worth recapping the key points here. For example, it is possible for AI machine learning algorithms to act in ways not initially anticipated or directed by programmers, which could surface unexpected data sets and outcomes. This kind of AI black-box scenario goes against the principles of data transparency and is certainly at odds with GDPR stipulations on data purpose (data must be used for explicit purposes) and data minimization (data must be relevant and limited to the purpose for which it is collected). Taken together, this all poses challenges for the GDPR definition of consent, and strict adherence could be difficult if an organization is not fully aware of how an AI system may eventually use the data.

Be explicit; consumers must know what they are consenting to

GDPR requires that organizations are completely clear about consent, not just making people fully aware of when and how they are providing it but also telling them what it means and covers. In January 2019 France's data protection authority, the Commission nationale de l'informatique et des libertés (CNIL) served Google with a €50m fine for violating various aspects of GDPR including issues relating to consent. The complaint and subsequent ruling relate to data privacy in the context of setting up a Google account on Android smartphones. CNIL's observations on its ruling against Google stand as a lesson in what not to do when handling consent.

CNIL ruled that the way Google went about obtaining user consent to process data for advertising personalization was invalid for two key reasons:

- **User consent was not sufficiently informed.** Google did not make users sufficiently aware of the extent of its data processing activities when obtaining consent. More specifically, users were not made aware of the huge range of combined data used for ad personalization that is collected across multiple Google properties (e.g., YouTube, Google Search, Google Play Store, Google Maps, etc.).
- **The collected consent was neither specific nor unambiguous.** Google used a blanket, opt-in consent tick box that CNIL ruled was too broad and therefore not specific as per GDPR stipulations. Moreover, the consent box was presented to users as already ticked, but under GDPR, consent is only unambiguous when a clear affirmative action is given by the user (i.e., the user ticks the consent box).

Champion transparency

Clarity, simplicity, and reduced friction are paramount

Navigating data privacy should not be a labyrinth for consumers, with policies buried in small print or made so complicated that consumers become confused and do not actually understand what they are consenting to. Service providers must make encounters with data privacy policies and consent easy, expressing them in a language consumers understand and making interactions frictionless. This could be further enhanced by using visual elements that help make information easier to comprehend and/or help break it down into more manageable elements, for example, by using infographics, visual icons, or short video clips to explain and clarify points. Actions of this kind create a positive experience around the data privacy encounter, building goodwill toward and trust in the service provider.

Lessons from CNIL's ruling on Google

CNIL's ruling on Google also included violations against GDPR's stipulations on transparency and once again help to illustrate what to avoid. Salient points flagged by CNIL include the excessive distribution of essential information across multiple documents and the use of multiple links that consumers have to click through to access associated information. CNIL notes that in some cases the relevant information was only accessible after several steps that sometimes involved five or six actions. The information snared by this cumbersome process included fundamental points that should be easily surfaced, for example, information about types of personal data used for advertising personalization and targeting. Moreover, much of the information was described in a vague and generic manner.

Show consumers the benefits of sharing data

Benefits must be tangible and specific

Consent is presented to consumers as a compliance process where service providers tell people what they are consenting to but not about the benefits that giving consent can bring. This is a lost opportunity, because when the advantages of sharing data are communicated properly, it can help move the needle on consent and make it a positive experience for consumers. But to succeed in winning consent, service providers must express benefits in concrete, experiential terms not in the abstract or generically. For example, do not just say that consenting to share data will mean more personalized services; this is too generic and rather lazy. Instead, tell people exactly what form service personalization will take and why this will be a good thing; be as specific as you can. For example, show how sharing personal data will produce more precise recommendations better tailored to the individual's preferences, which brings benefits in terms of discovering new content they might otherwise miss, receiving early-bird access to tickets for their favorite band, or receiving offers based on things they like to buy.

Toward consumer-first data privacy management

The ultimate goal for service providers should be the creation of a personal data privacy management framework for consumers. This requires careful design, with education as part of the process, while key components include a front-end user interface; a data vault containing basic privacy settings, data storage, and data categories; and a data time line. The personal data privacy management framework should also include a selection of data privacy tools and value-added services. A holistic framework of this kind goes well beyond basic regulatory stipulations and creates positive, valuable data privacy experiences for consumers.

Create data privacy tools and value-added services

GDPR and similar rules on consent, transparency, and other data governance should be treated as the starting point for data privacy not the end game. Service providers need to think about how they can enhance the whole data privacy user experience, and the best way is to develop consumer-first data privacy management tools and services. This aligns with consumers' wanting more control over their dataand builds on all the recommendations and best practice discussed so far in this report. The goal of consumer-first data privacy management is to further raise the bar with tools and other initiatives that bring additional value to consumer data privacy. This also ties in with the data friending strategy outlined in *Making Data Privacy an Asset in the AI Era: Mastering Market Dynamics.* To recap, a data friending strategy is one where the focus is on proactively engaging with consumers to build a positive relationship around data privacy. In this scenario, data privacy becomes an asset for both consumers and service providers that can bring mutual benefit to both parties.

Personal data privacy management components

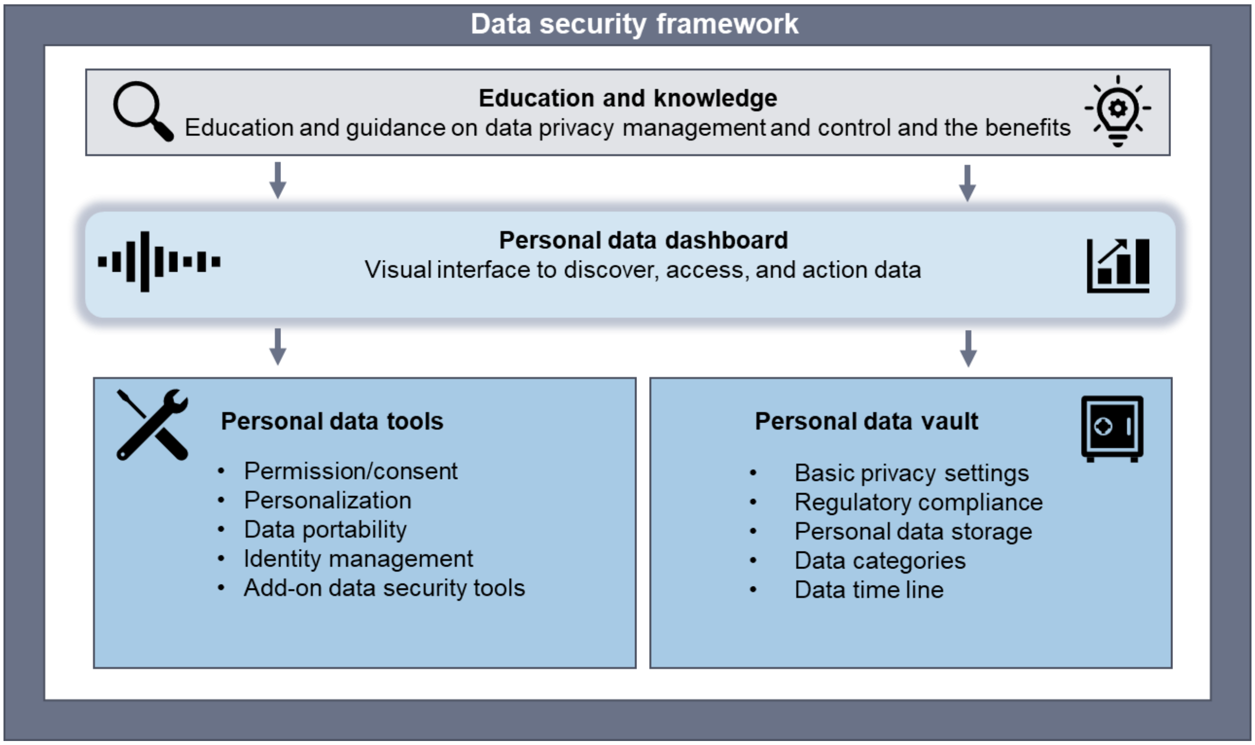
Plan ahead, but be careful not to overwhelm consumers at the outset

The exact components of a personal data privacy management framework can and will vary, but the essentials that service providers need to consider are captured at a high level in Figure 5. Ovum recommends that service providers start with a "less is more" strategy. Introduce the data privacy management framework gently, and do not be tempted to overstuff it with features and information; there is a risk that this will overwhelm consumers. Lead them into the experience, wait until they are confident and comfortable, and then introduce more elements.

At the start of this report, we recommended that service providers segment consumers based on their data privacy attitudes and needs, and this should inform the data privacy management framework that you build. Aligning the two means you will be in a position to introduce different tools and services optimized for the needs of the different data privacy segments identified.

Figure 5: Conceptual view of personal data privacy management components

Figure 5: Conceptual view of personal data privacy management components5



Data security framework

Education and knowledge
Education and guidance on data privacy management and control and the benefits

Personal data dashboard
Visual interface to discover, access, and action data

Personal data tools

- Permission/consent
- Personalization
- Data portability
- Identity management
- Add-on data security tools

Personal data vault

- Basic privacy settings
- Regulatory compliance
- Personal data storage
- Data categories
- Data time line

Make education part of the process

Consumers have little experience in controlling or managing their personal data; grappling with complex, difficult privacy settings is not what we consider meaningful, positive data privacy management. Ovum recommends that service providers lead consumers into a data privacy management framework by first educating them as to what managing their data means: why it is important and beneficial, what the various control tools on offer can do, and how they can bring value. This process must be handled very carefully; the last thing service providers want to do is overwhelm people so that they perceive a data management framework and tools as difficult and confusing, because this will lead to rejection.

Provide a personal data vault

A personal data vault is a central depository for personal data and related material and should at least contain the following:

- **Basic privacy settings.** These should be simple, transparent, and fast to complete with the focus on enabling people to understand and manage their basic data privacy choices.
- **Regulatory compliance.** For example, show compliance to any relevant regulations but, once again, in a way that is easy for consumers to comprehend. This will in part overlap with privacy settings but should not in any way confuse the process or make it more complex.
- **Data storage.** Have a secure storage vault for user data.

- **Data categories.** Offer easy access to segmented data sets such as service history, service usage, billing, and financial data.
- **Data time line.** The focus is on providing consumers with a time line that shows how interactions with various services generate data and of what types and how a service provider has used permission-based data insights. A data time line of this kind is a powerful articulation of data transparency.

Design an intuitive user interface

You may have built an impressive data privacy management framework, but unless you provide consumers with an easy way to discover, access, view, and action data and tools, they will not use it or, at best, will underuse it. You need to provide a front-end interface, and Ovum recommends an easy-to-use visual dashboard for data presentation and actions.

Empower users with value-added data privacy services

The objective is to provide tools that offer more control and other value benefits to the data privacy experience. There is a large range of options to consider, including the tools listed below (this presents a few examples but is not an all-inclusive list):

- **Permission/consent management.** This is an additional layer for managing consent beyond the basics of yes/no. The focus here is on different levels of consent that give users control over the type of data the service provider wants access to, who they may want to share it with, and use cases. It could also include ways of helping consumers to manage consent across multiple services and partners.
- **Personalization.** This is concerned with tools that allow people to control and share data points that enable personalization, for example, purchasing patterns, usage patterns, personal interests, and preferences. There should be support for various degrees of personalization for different services and scenarios. For example, allow a consumer to release high-level data insights for lighter-touch personalization or, conversely, deeper data sets for more tailored, targeted personalization.
- **Data portability.** This is a provision under GDPR and allows for consumers to transfer their personal data from one organization to another, a process that is typically cumbersome and needs to be better handled.
- **Identity management.** Consumers use an increasing number of different digital services, content, social, and messaging platforms, and this ratchets up identity management across these multiple services. There can be dozens of passwords to manage and multiple security and authentication steps to walk through, which is time consuming, can lead to mistakes by individuals, and can also leave the door open to malicious actions by third parties. Tools that make identity management easier, faster, and safer provide a valuable service for consumers.
- **Add-on data privacy and security tools**. Data security is outside the main scope of this report, but there is a wide range of options such as tools that provide additional security for location-based consumer data insights, which can be particularly sensitive. For example, Apple has introduced several new location privacy features in iOS 13, which include far more control over how often apps can tap into a user's location via the device as well as measures to stop apps from scanning nearby Bluetooth and Wi-Fi networks to determine location.

Leverage AI for data security and privacy

There is no doubt that AI poses fresh challenges for consumer data privacy, as examined in *Making Data Privacy an Asset in the AI Era: Mastering Market Dynamics.* But AI can also bring benefits to both data privacy and security in the following ways, although many are still nascent:

- AI tools can alert users in real time of scams, suspicious websites, or other malicious activity that could harm their data. The same tools should also be able to respond proactively in real time with the appropriate actions to protect consumer data that is under threat.
- AI can monitor and respond to fake accounts and inappropriate content on online platforms. This is a measure that Facebook for one has already undertaken.
- AI-powered analytics can monitor data patterns and detect anomalies and potentially fraudulent activity in real time.
- AI-powered privacy tools can remember an individual's privacy preferences and make them consistent across a single organization's services or even across multiple sites, although the latter is a much more challenging proposition.
- AI can help with compliance by scanning the increasing reams of legal and other data privacy-related material, checking the degree to which a company is adhering to stipulations and when it is in danger of falling short, before it happens.
- Associated with the point above, AI can continuously monitor a company's collection and use of consumer data, where consumers have provided consent or withheld it, and whether this is aligned with data privacy rules.

AI and predictive consent

Consumers have relationships with multiple services and service providers, and consent must be managed across all of them, which can be difficult and time consuming. We have already noted that tools to help manage this are appealing, and there is scope for AI to streamline the process further via predictive consent mechanisms. This involves ML solutions that tap into a consumer's data profile to learn about their service relationships, usage patterns, and behavior and from that model intent in the consent context, predicting and granting consent (or withholding it) at appropriate levels for different services on behalf of the user. ML predictive-consent models are nascent and, although appealing on the face of it, face a number of challenges, of which the main ones are lack of consumer trust in such models and the potential of the risk of inaccuracy and getting consent wrong. The latter could have a multitude of negative outcomes, particularly if it involves consent to access sensitive data such as financial or health-related information.

The role of personal data exchanges

A model with disruptive potential

A personal data exchange is in many ways an evolution of the personal data management framework examined earlier, the main difference being that a PDE allows a user not only to manage their data parameters but also to commercialize their data by consenting to share all or part of it with third parties in return for value of some kind. The shared data is not personally identifiable, so privacy is kept intact.

The idea is that users benefit directly from commercializing their data and are put in control of how this happens, rather than a content publisher, advertising network, social media, or other platform taking the lead and all the profit that comes from leveraging user data. It is essentially an incentives-based model for consent, and how users are rewarded varies. It could include monetary fees or discounts and vouchers.

Third parties benefit by gaining access to valuable data they might otherwise not get consent to access and, in theory, a deeper relationship with the consumer group that has shared that data. The data-exchange platform earns fees from the third parties signing up to the platform data and, possibly, from users if it also sells other associated value-added services (e.g., data storage, management tools), which many PDEs do.

The PDE market is still immature, but startups in this space have mushroomed over the past four years with some of the more established firms including CitzenMe, Meeco, people.io, Datum, and Digi.me (among others). PDEs are in theory highly disruptive to traditional internet monetization models that make their money from user data, advertising being the most conspicuous but not the only model on this front.

Significant barriers to clear before PDEs can take off

However, to be disruptive, PDEs need to be adopted at scale, and so far this has not happened. There is a range of significant issues that need to be addressed:

- Lack of trust. Consumers have little trust in the data privacy and data security credentials of most service providers beyond banks, so expecting them to place trust in young unknown startups is a big ask that will not be affirmed by many consumers.
- Most consumers are familiar with the idea that they have to share data to get free access to certain services, but this does not necessarily make PDEs a natural next step. The majority of consumers do not understand the value of their personal data or view it as an asset that can be traded and will need education and a high degree of hand-holding to make the leap.
- Consumers are hooked into the dominant data super platforms (think Facebook, Google, Amazon, et al.), and many may be too apathetic to change the status quo.
- Others will simply not be interested in the PDE concept and will view it as a hassle, another data privacy hoop they have to jump through. However, this does in turn raise the notion that some sort of managed-service PDE could be of interest to people who fall into this category.

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia’s consulting team may be able to help you. For more information about Omdia’s consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) and represent data, research, opinions or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness or correctness of the information, opinions and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees and agents, disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com