Design for Privacy

How will the ePrivacy Regulation affect the design and user experiences of digital services?

Prepared by

Normally

Prepared for

Centre for Information Policy Leadership

Contents

Executive Summary

This report was prepared by Normally Ltd for the Centre for Information Policy Leadership in April 2018.

Normally is a data product and service design studio. They solve complex design problems for some of the world's largest organisations including the BBC, Barclays, Facebook, Nokia and Spotify.

In this report you will find their perspective on how the ePrivacy Regulation (ePR) may affect the design of digital services. Key points are summarised here:

Lets create genuine transparency and choice
ePR – particularly Articles 6 and 8 – asks for consent before a service is used but transparency and individual choice may be better ensured by enabling users to experience services.

Lets move from avoiding risk to serving users
Currently, design for privacy is more concerned with managing regulatory risk than genuinely serving the users' need for comprehension and control.

Lets broaden our vocabulary for 'good' design
Whilst we are equipped with principles for 'good' design in general – being *timely*, *efficient*, *personal* and *convenient* – we lack a common vocabulary for design which respects privacy.

Lets develop and share successful design tools
Beyond abstract vocabulary we need more design tools and examples of best practice. Thinking of design for privacy as a series of notices and opt-in or opt-out controls paints a limited and flawed picture of how trust may be built and maintained.

Lets allow for demonstration of value contextually
It may be difficult for service providers to obtain any meaningful consent as required by Articles 6 and 8 if they are less able to demonstrate their value contextually. Transparency and control for indivuals

can be ensured in better ways than by asking for consent before a service is used.

Lets avoid the ‘cookie wall’
Article 8 risks replacing cookie banners with highly obtrusive ‘cookie walls’ and risks creating ‘wall fatigue’. Whichever solution is found – we need to ensure that it actually informs and enables meaningful choice.

Lets ensure the gatekeeper isn’t a complete barrier
Article 10 poses a promising solution to the cookie wall problem – with the browser as gatekeeper – but we must consider how service providers may make timely communication of value via this approach.

Lets encourage thoughtful comms and contols
To achieve the values of the ePrivacy Regulation (ePR) – transparency and control of personal data for users – design needs to be encouraged to select and sequence privacy communications, and controls, throughout the user experience (UX), not just during first use.

Introduction

In the discourse on regulation of digital services and the proposed ePR, design has been missing from the discussion. In this study we'll make the case for why we all need design to take a seat at the table. We'll begin by evaluating the current UX landscape, explore the challenges of designing for law and propose some principles on designing for privacy. We will then review the proposed ePR in light of this context paying particular attention to Articles 6, 8 and 10. To conclude we will explain why design should be harnessed to both inform policy and create digital services which take into account user needs, business goals and societal values.

The Case for Design

What is UX design?

User experience (UX) design is the practice of designing products with particular focus on how people will use them and how their relationships with them will evolve over time. It has a long history and can be traced to Henry Dreyfuss' 1955 text "Designing for People" if not before.

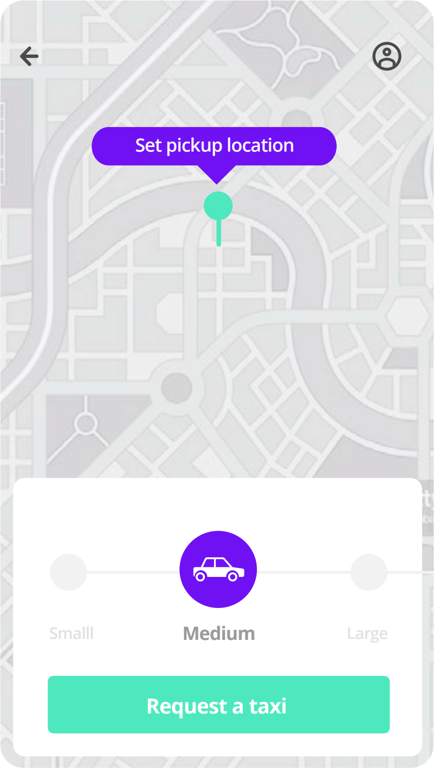
The field of UX design has changed drastically since 1955 and considerably so in recent years. Designers of today's digital services find themselves creating products at epic scale for thousands, if not millions, of unique users who's digital literacy can vary vastly. Technical advances in processing personal data have also made it increasingly feasible to tailor services on an individual basis. Furthermore, the nature of technology now allows for the continuous deployment of incremental improvements – meaning the work of a UX designer is never finished, always evolving.

What are ‘design principles’?

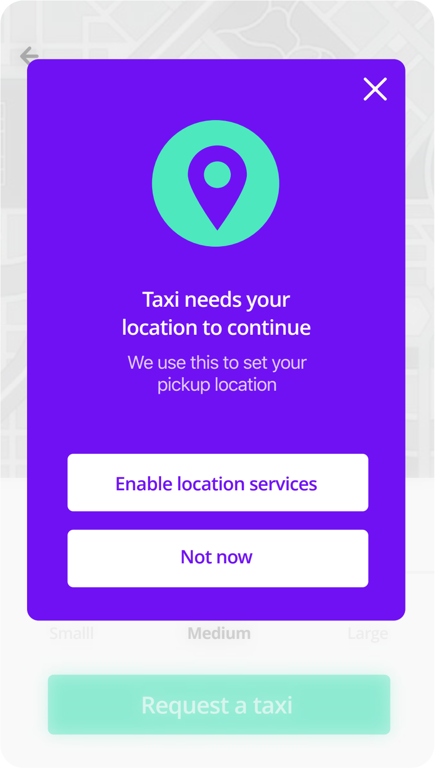
Despite these profound changes – some things remain consistent. UX has always sought to establish ‘design principles’ which guide our work. These serve as tools to both inspire and evaluate design, regardless of the experience they are applied to, and can adapt to technological change. Here are some key design principles and how they manifest in today’s UX.

Timely

Timely designs serve relationships not single interactions. They identify the best moment for you, as a service user, to take action in recognition of where you’ve been and where you’re going. When location sharing is required at the point you request a ride – that is timely.



01



Taxi needs your location to continue

We use this to set your pickup location

02

01 and 02
Timely Location Consent
Here a taxi service provider requests location permissions in the context of the first trip rather than during registration.

Efficient

Efficient designs recognise time is precious. They do the hard work for you and avoid repetition. When a form auto-completes or a basket saves items for later – that is efficient.

03

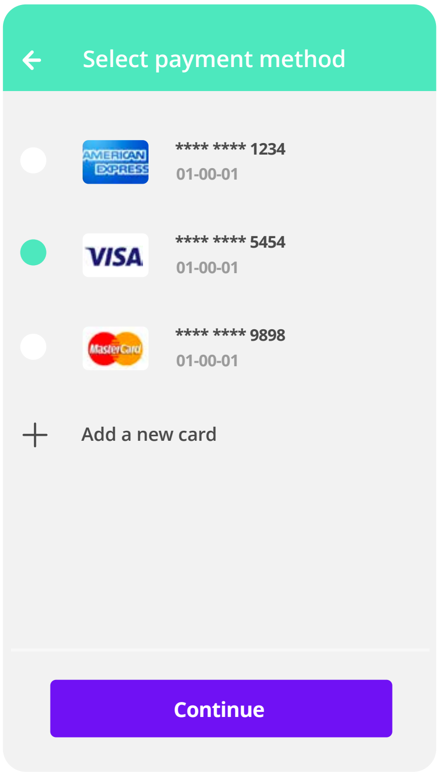
Efficient Autofill

The eCommerce provider has stored the user's card details from a previous transaction to make future payments more efficient.

04

Efficient Basket Memory

An eCommerce provider may use cookies to remember items you have added to your basket if you leave before completing the purchase.



Select payment method

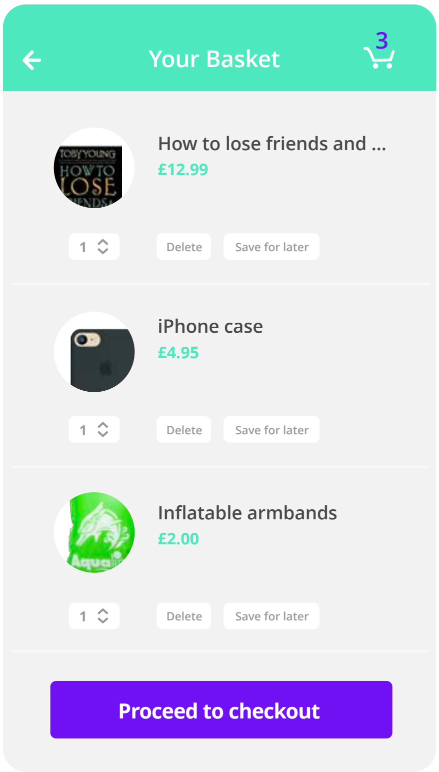
○ **** **** 1234
01-00-01

● **** **** 5454
01-00-01

○ **** **** 9898
01-00-01

+ Add a new card

03



Your Basket

How to lose friends and ...
£12.99
1 Delete Save for later

iPhone case
£4.95
1 Delete Save for later

Inflatable armbands
£2.00
1 Delete Save for later

04

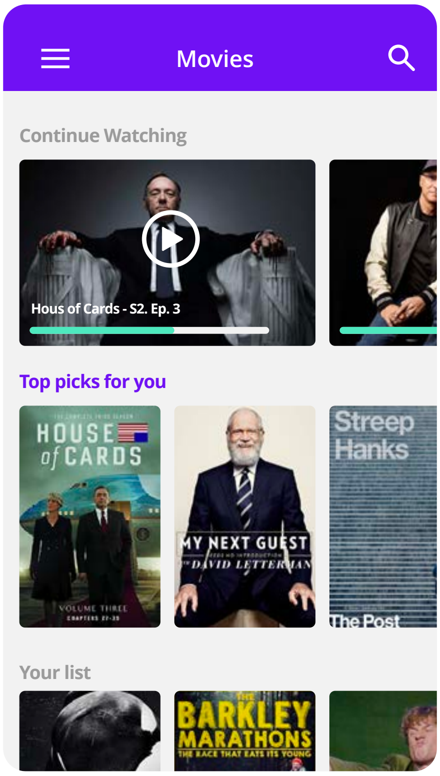
Personal

Personal designs understand their users. They notice your preferences and serve experiences to match. When a service curates recommendations for you – that is personal.

05

Personal Recommendations

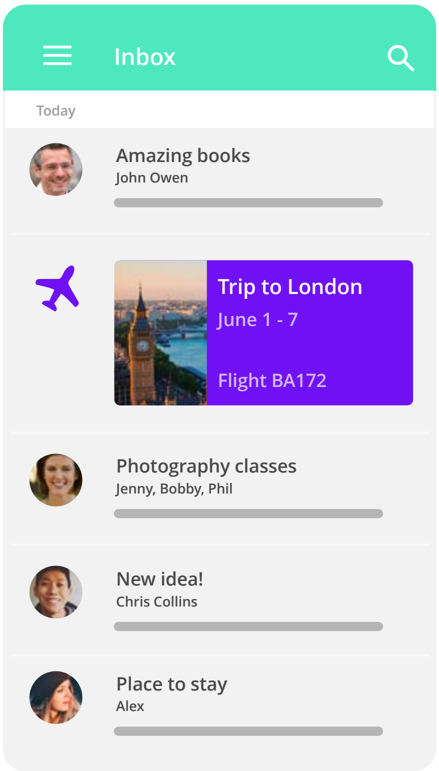
A video streaming service may monitor your viewing habits to enable them to recommend other shows you might like.



05

Convenient

Convenient designs preempt user needs. They recognise and respond to your context. When your email highlights your flight details or a smart messaging app offers to book tickets – that is convenient.



Amazing books
John Owen

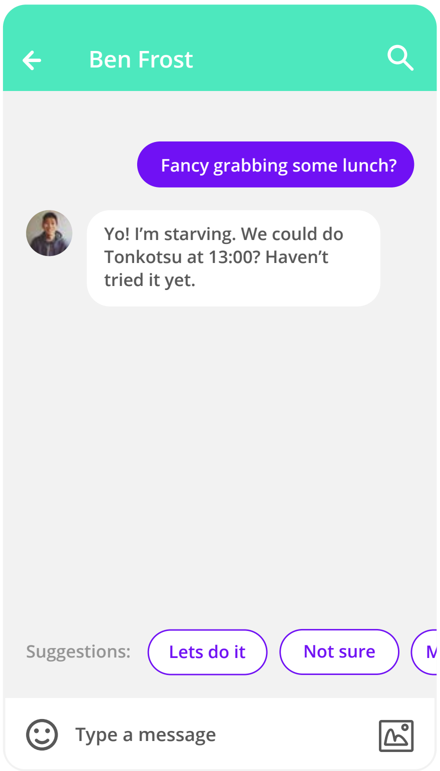
Trip to London
June 1 - 7
Flight BA172

Photography classes
Jenny, Bobby, Phil

New idea!
Chris Collins

Place to stay
Alex

06



Fancy grabbing some lunch?

Yo! I'm starving. We could do Tonkotsu at 13:00? Haven't tried it yet.

Suggestions: Lets do it | Not sure | M

Type a message

07

06
Handy Email Highlights
An email provider may process your email contents to detect and highlight important content such as flight details.

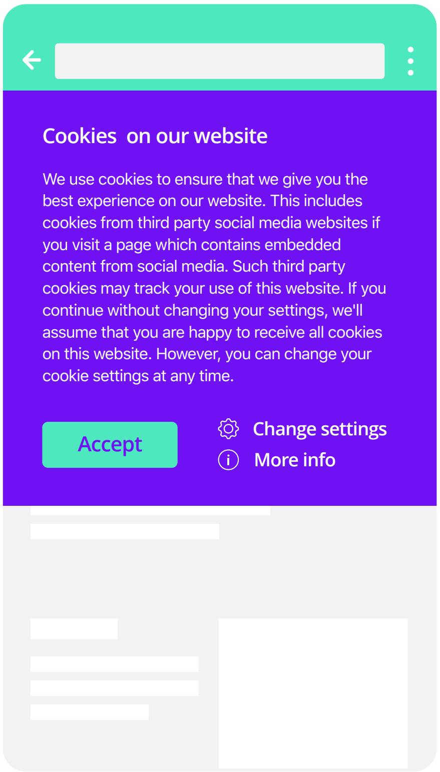
07
Handy IM Suggestions
An IM provider may process your messages to suggest a quick response.

How do we design for law?

When done well – design is elegant, engaging and adept at solving problems. Designers are well positioned to create solutions which fulfil user needs within the constraints of business goals and legislation. Unfortunately, design isn't always done well or done at all. When it comes to law, experiences often default to an exaggerated implementation. UX is suffering as a result and so too is the intent of the legislation.

It is difficult to identify examples of design which tackle privacy successfully. We continue to see obtrusive cookie banners, repetitive consent notices and bloated terms and conditions. It is doubtful that these experiences are engaging users and providing them with meaningful choices about how their personal data is used.

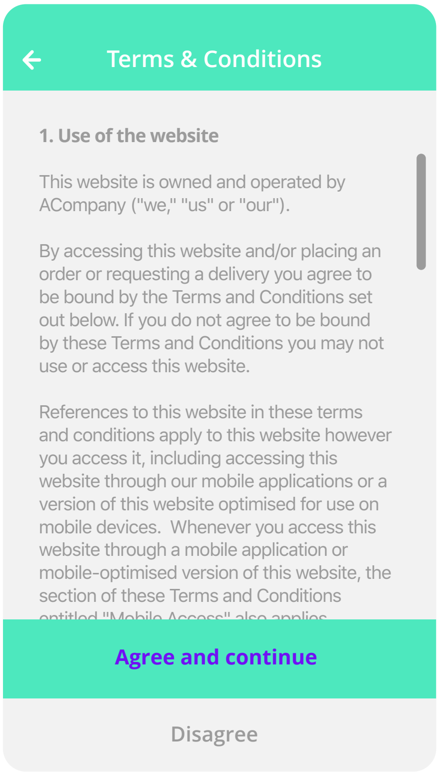
08, 09 & 10
Existing UX for Privacy
Example cookie banner, terms & conditions and consent notices.



Cookies on our website

We use cookies to ensure that we give you the best experience on our website. This includes cookies from third party social media websites if you visit a page which contains embedded content from social media. Such third party cookies may track your use of this website. If you continue without changing your settings, we'll assume that you are happy to receive all cookies on this website. However, you can change your cookie settings at any time.

08



Terms & Conditions

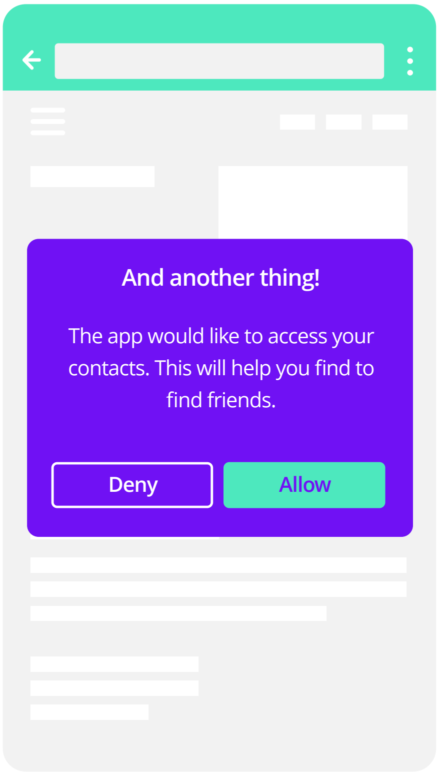
1. Use of the website

This website is owned and operated by ACompany ("we," "us" or "our").

By accessing this website and/or placing an order or requesting a delivery you agree to be bound by the Terms and Conditions set out below. If you do not agree to be bound by these Terms and Conditions you may not use or access this website.

References to this website in these terms and conditions apply to this website however you access it, including accessing this website through our mobile applications or a version of this website optimised for use on mobile devices. Whenever you access this website through a mobile application or mobile-optimised version of this website, the section of these Terms and Conditions entitled "Mobile Access" also applies.

09



And another thing!

The app would like to access your contacts. This will help you find to find friends.

10

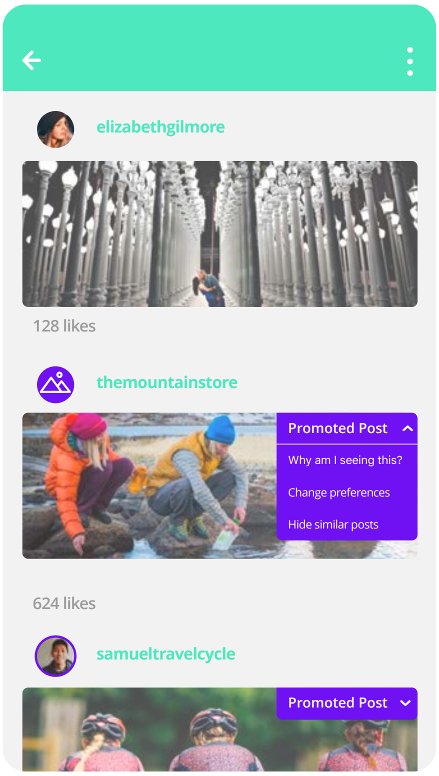
Prescriptive regulation – and risk averse interpretation of it – is inhibiting the value which UX can bring to privacy and data protection. Design needs to be given the flexibility and encouragement to tackle these challenges creatively. With this switch in approach – from prescriptive to principled – we may begin to see the thoughtful innovation in privacy which we've come to expect elsewhere in the products we use.

How can we design for privacy?

If we were to establish and evangelise a principles-led approach to designing for privacy – what might those principles be? As well as being *timely*, *efficient*, *personal* and *convenient* – here are some other principles we believe would be useful for privacy.

Transparent

Transparent designs don't gloss over details and refrain from resorting to 'dark patterns' (a practice where service providers exploit UX conventions to trick users into doing things they normally wouldn't choose). They ensure that you're informed to engage meaningfully. When you are given a clear option to scrutinise the origin of a targeted ad – that is transparent.



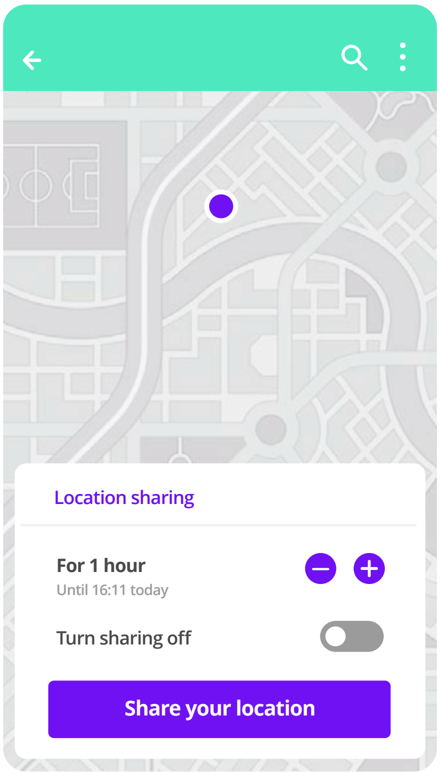
11

11
Transparent Advertising
An image sharing service may show paid for content from 3rd parties. This could be clearly labelled for transparency.

Empowering

Empowering designs enable users to make active choices and really control their personal data. They don’t make it all or nothing, and they allow you to change your mind later. When data sharing tools give you expiry options – that is empowering.

12
Empowering Location Sharing
This service provider gives users the option to specify a time period when sharing location.



Location sharing

For 1 hour
Until 16:11 today

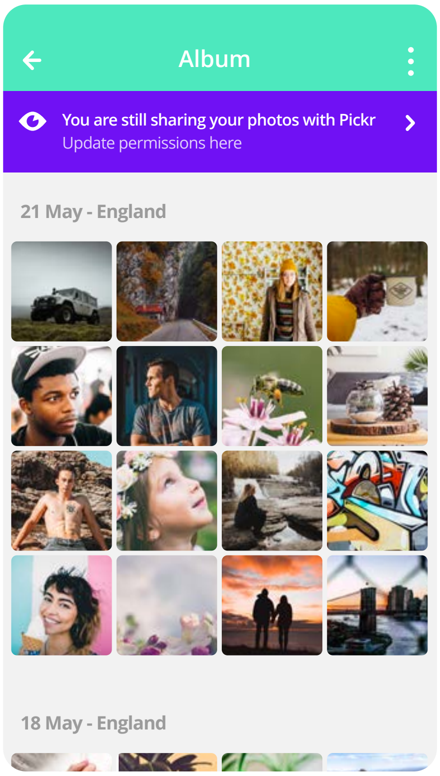
Turn sharing off

12

Conscientious

Conscientious designs take their duty of care seriously. In recognition that users can be lax with their privacy, conscientious designs choose not to take advantage. When a service proactively reminds you of previous choices you made and gives you the option to control or adjust – that is conscientious.

13
Conscientious Photo Sharing
A notice is shown to alert the user that they are still sharing photos with a 3rd party app.



13

Evaluating the ePrivacy Regulation

Overview

To evaluate the effect of the ePR on the design of digital services and their user experiences we will explore key articles through example applications. The ePR has a heavy emphasis on the browse-based internet and can fail to provide clear guidance for digital services which take other forms. Whilst in the past digital services were usually confined to websites and accessed through a web browser – we now find ourselves accessing services via mobile and desktop apps, voice assistants, wearables and other interfaces.

For Article 6 we will examine the implications of data processing restrictions on non-browser-based services such as instant messaging (IM) apps and pay particularly attention to the emergent trends of ‘smart messaging’ and conversational interfaces. We will then examine Articles 8 and 10 to understand how restrictions on placing cookies and carrying out other device-based processing may affect the browsing experience across the web.

How might Article 6 affect design?

What does it say?

Article 6 – that should be read in connection with Article 5 - governs the processing of electronic communications data. Its intention is to protect the privacy of service users and ensure the confidentiality of their communications. Point (1) of Article 6 states that service providers may only process data if it is technically essential for the service or if it is required for security reasons. Point (2) and (3) of Article 6 further state that **content may only be processed with consent** for a specific purpose and metadata data may only be processed without consent under limited circumstances.

Some service providers, such as IM apps, currently process both metadata and content. This is usually detailed in their terms of service but express consent is not always sought due to more flexible data protection rules. The GDPR will not change this. However, in the scenario laid out by Article 6, the service provider will need to obtain express consent for each distinct purpose prior to data processing.

How might this affect services like instant messaging?

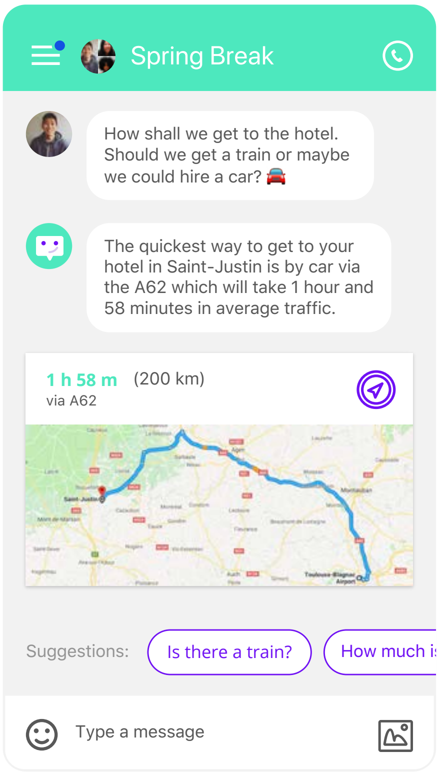
On the surface Article 6 seems like a logical and welcome stipulation. If you make a telephone call, the provider may process the number you call, the duration of your call and the time at which you make it (i.e. the metadata) but they may not listen to your call or record your conversation (i.e. the content). If you post a letter, the postman may not open and read your letter (the content) but they may read the delivery address and ensure sufficient postage has been paid for the size, weight and destination of the letter (the metadata). However, IM services are not post and their providers are not postmen.

There has been a proliferation of new IM services in recent years – think iMessage, Whatsapp, Facebook Messenger or WeChat. These bring with them increasing breadth, sophistication and complexity. Not least because they enable group based communication. People are moving between several communication threads – often across multiple apps – with different participants and purposes. It is clear that electronic communications are increasingly many-to-many rather than one-to-one but it's not clear what this group dynamic means for regulation and compliance. How should a provider obtain group consent? And what can we do to avoid that being a complex, frustrating or even disabling process?

IM is also often used as an interface to other services – a design trend known as 'smart messaging' or 'conversational interfaces' depending on context. Whether your IM is suggesting a route to your destination, booking a restaurant for you or chatting with your bank – it is common to find other services embedded within IM and vice versa. It's unclear how ePR should be adopted for services of this nature. If these services are considered less as traditional IM and more as 'smart messaging' – is expressed consent expected, necessary or desirable? If so – at what point in the experience and at what level of granularity should that be obtained? Many of these smart features – such as the route planning illustrated – provide real value.

14
Smart IM Features
Here a 'bot' has processesed user messages to provide smart assistance such as travel advice.

15
Smart IM Restricted by Consent
If group consent is required prior to processing the users may see a warning notice like that shown here.

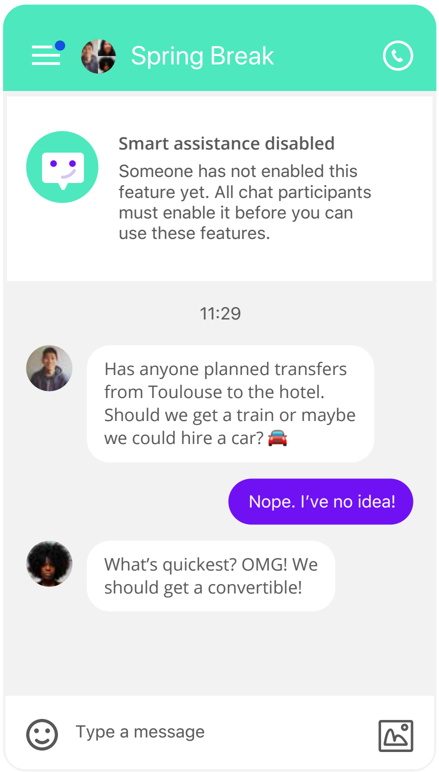


How shall we get to the hotel. Should we get a train or maybe we could hire a car? 🚘

The quickest way to get to your hotel in Saint-Justin is by car via the A62 which will take 1 hour and 58 minutes in average traffic.

1 h 58 m (200 km)
via A62

14



Smart assistance disabled
Someone has not enabled this feature yet. All chat participants must enable it before you can use these features.

11:29

Has anyone planned transfers from Toulouse to the hotel. Should we get a train or maybe we could hire a car? 🚘

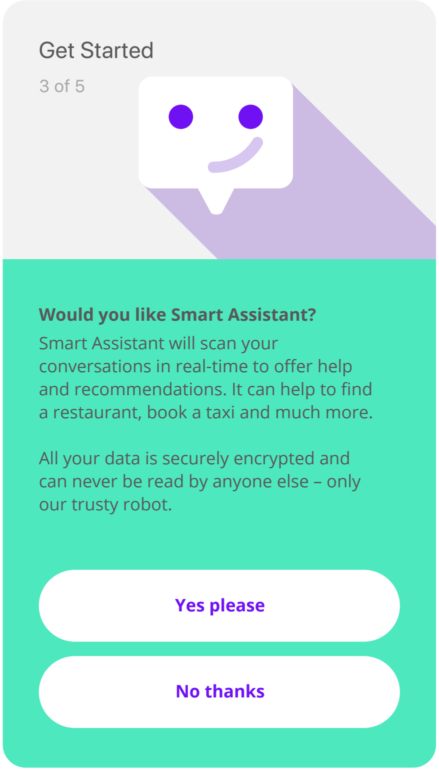
Nope. I've no idea!

What's quickest? OMG! We should get a convertible!

15

However, under the proposed ePR we risk excluding users from these smart features by making consent difficult to obtain. Most service providers are likely to bundle all consent requests into their sign-up or installation process. As well as adding friction to the process – this approach conceals important privacy details during a moment which is already information-dense. We know users are unlikely to fully engage with this content and make rash choices of convenience rather than informed choices as a result.

16
Upfront Consent
Consent could be obtained during an installation flow however lots of other actions are also taken at this point.



Get Started

3 of 5

Would you like Smart Assistant?
Smart Assistant will scan your conversations in real-time to offer help and recommendations. It can help to find a restaurant, book a taxi and much more.

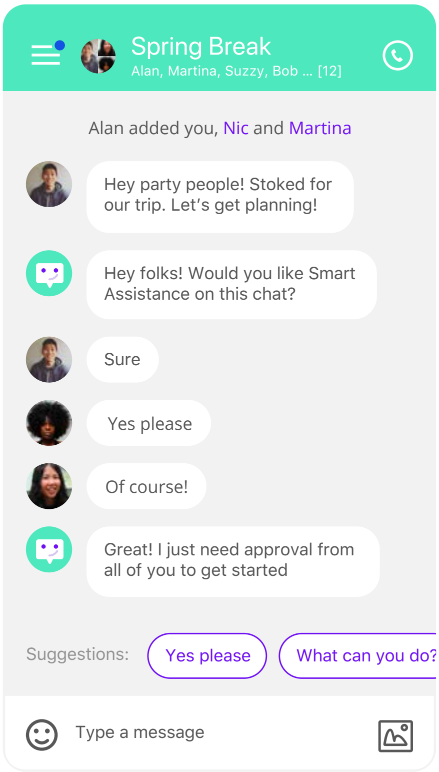
All your data is securely encrypted and can never be read by anyone else – only our trusty robot.

16

It's not as simple as selecting between opt-in or opt-out controls. Each may enable transparency and control for users depending on how successfully they are implented. Regardless of where you sit on the opt-in opt-out debate – we should be encouraging, and indeed requiring, that privacy notices and controls are thoughtfully positioned throughout the UX where they most clearly aid comprehension.

17
Contextual Opt-In
The smart 'bot' may offer its services without processing data. However if consent is required from all users this could be cumbersome in group chats.

18
Contextual Opt-Out
Alternatively the bot could introduce itself and the chat participants may ask it to stop or explain itself further.



Spring Break
Alan, Martina, Suzzy, Bob ... [12]

Alan added you, Nic and Martina

Hey party people! Stoked for our trip. Let's get planning!

Hey folks! Would you like Smart Assistance on this chat?

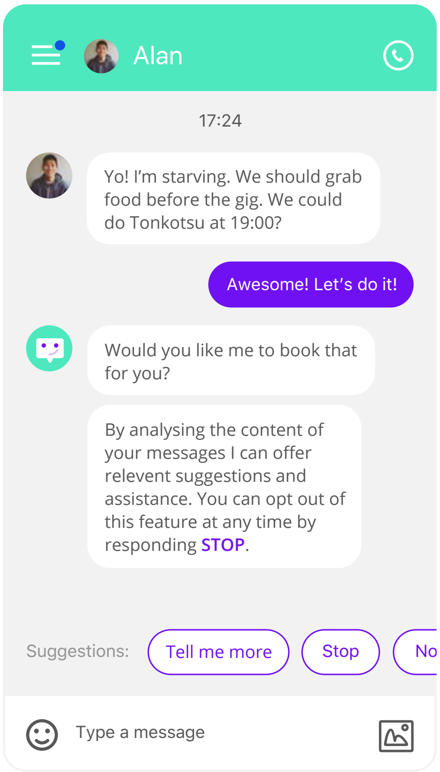
Sure

Yes please

Of course!

Great! I just need approval from all of you to get started

17



Alan

17:24

Yo! I'm starving. We should grab food before the gig. We could do Tonkotsu at 19:00?

Awesome! Let's do it!

Would you like me to book that for you?

By analysing the content of your messages I can offer relevent suggestions and assistance. You can opt out of this feature at any time by responding **STOP**.

18

Considering the smart messaging scenario – if we could deliver privacy details contextual to a moment, such as starting a new IM conversation, then we may more effectively communicate their value. This could avoid people making poorly informed choices or suffering unintentional self-exclusion. We could also utilise the qualities of the medium, in this case conversational interfaces, to deliver that more effectively than the tired consent notices users are so regularly bombarded with.

Given that processing of metadata and content is integral to the delivery of these smart features – we must consider how to best ensure transparency and control.

How might Article 8 affect design?

What does it say?

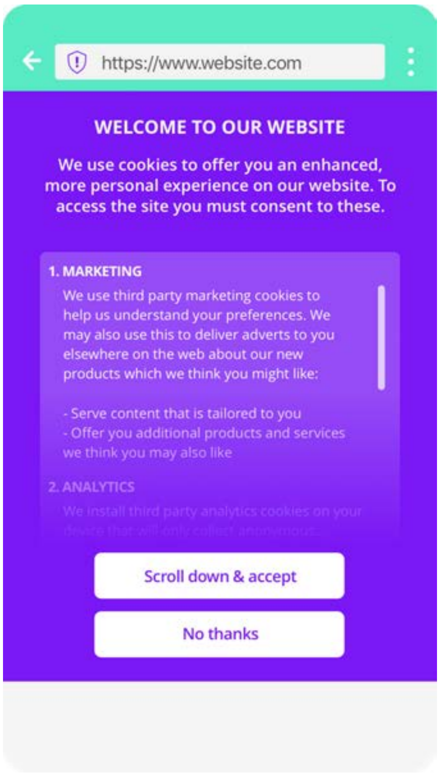
Article 8 governs the processing of data stored on or emitted by a user's device as well as the use of device storage capabilities by the service provider. It aims to protect people from unauthorised use of their device, particularly using cookies and other tracking technologies. Part (1) of Article 8 states that service providers may only collect information from a user's device or use its processing and storage capabilities if it is technically essential or if the user has expressed consent for a specific purpose.

Similarly to Article 6 – in many EU Member States, most service providers currently use cookies and other tracking technologies with only implied consent i.e. a cookie banner may be shown to alert their use but express consent for specific purposes is not sought as detailed information is provided in a privacy and cookie policies. However, in the scenario laid out by Article 8, the service provider will now need to obtain express consent for each distinct purpose prior to implementing the technology.

How might this affect the browsing experience?

The proliferation of 'cookie banners' is a good example of how regulation has resulted in the adoption of a UX pattern with little benefit to users. These banners rarely provide sufficient information for users to make an informed choice and, after frequent exposure, 'banner blindness' causes many users to simply ignore them. Furthermore, users are often unaware that continuing to browse a web page implies consent to the use of these technologies. All in all – cookie banners offer far from meaningful control.

For some use cases a cookie notice would not be necessary under the proposed Article 8. We welcome any such steps which remove pointless banners from the web. However, there are still going to be many cases where a cookie notice is required and in those instances the notice will have to provide much more detailed information than is currently provided in most existing cookie banners.



https://www.website.com

WELCOME TO OUR WEBSITE

We use cookies to offer you an enhanced, more personal experience on our website. To access the site you must consent to these.

1. MARKETING

We use third party marketing cookies to help us understand your preferences. We may also use this to deliver adverts to you elsewhere on the web about our new products which we think you might like:

- Serve content that is tailored to you
- Offer you additional products and services we think you may also like

2. ANALYTICS

We install third party analytics cookies on your device that will only collect anonymous...

19

19
Cookie Wall
To obtain consent prior to cookie implemetation service providers may be required to restrict access to those who consent to a detailed cookie policy.

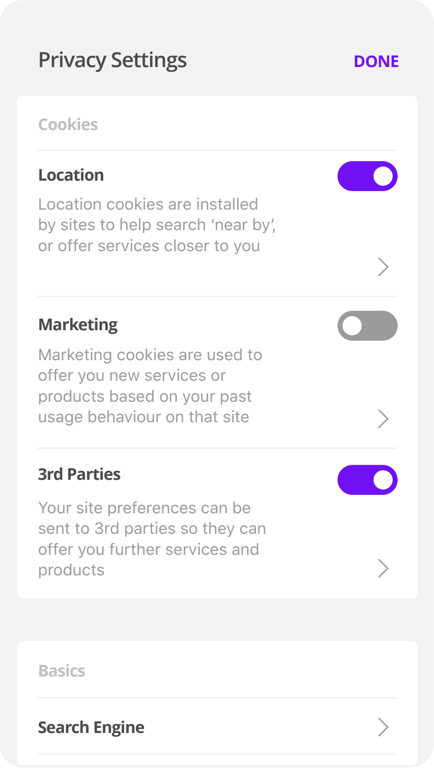
If we require users to actively consent to these technologies then we will need to restrict access. Users will face a ‘cookie wall’ – similar to an ad-blocking notice – rather than a banner. Not only will the UX be more obtrusive than existing banners (see page 7) but it will hinder the ‘open web’. We believe it’s important that the benefits of a democratic internet are accessible to all. However, it is clear that free services come at a cost to the provider. These providers have a legitimate need to monitise their services and cookies play an important part in enabling monetisation from advertising.

How might Article 10 affect design?

What does it say?

Article 10 acts as an extension to the aims of Article 8 – suggesting that software providers, including web browsers or mobile applications, have a responsibility to safeguard their user's device and personal data. Part (1) of Article 10 states that software providers must allow users to prevent third parties from collecting information from their device or to use its processing and storage capabilities. Part (2) of Article 10 goes on to suggest that the best moment to exercise this responsibility is at the moment of installation and that the software provider **must** have the user actively select their preferred privacy settings to complete installation.

20
Browser Privacy Settings
Article 10 suggests that the browser should allow users to restrict site's from implementing certain cookies.



Privacy Settings	DONE

Cookies

Location ●
Location cookies are installed by sites to help search 'near by', or offer services closer to you

Marketing ○
Marketing cookies are used to offer you new services or products based on your past usage behaviour on that site

3rd Parties ●
Your site preferences can be sent to 3rd parties so they can offer you further services and products

Basics

Search Engine

20

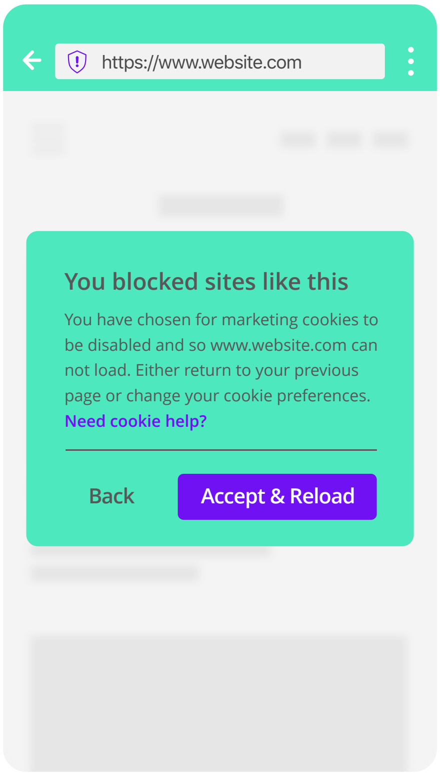
Currently – cookie usage and controls are usually explained on individual websites with brief cookie banners and detailed cookie policies. The scenario laid out by Article 10 suggests that privacy controls should be exercised at a higher level with the software provider acting as gatekeeper – by browser rather than by website. Rather than obtaining consent directly from the user – service providers will need to request that the user change their browser settings.

How might this affect the browsing experience?

When we consider the effect of Article 10 it may be wise to look at operating systems for inspiration. Operating systems – such as those made by Microsoft, Apple and Google – are the most prevalent software that people use to interact with third party services. These operating systems have been acting like the gatekeepers described in Article 10 for some time – controlling the access granted to third parties; to the camera, microphone and data etc.

It is promising to think of web browsers and mobile applications taking a similar role. By making privacy choices at a browser level we may avoid cookie banner 'blindness'. However, we need to be mindful of how this is done to ensure that we fulfil the underlying goals of ePR – to inform users and enable meaningful control.

Context is critical when making meaningful choices. By frontloading these choices at the point of installation, – user will be asked to make blanket privacy choices before interacting with the digital services that these decisions will affect. This lack of context could inhibit a user from making a fully informed decision, regardless of their technical expertise or privacy preferences. The 'cookie walls' described earlier could become commonplace if your browser settings fail to match the sites you wish to access. If we're not careful we risk replacing banner blindness with 'wall fatigue' which may lead to the rash choices we wish to avoid. Users may make a decision once, such as disabling a privacy setting to quickly access a site, that is then never revisited.



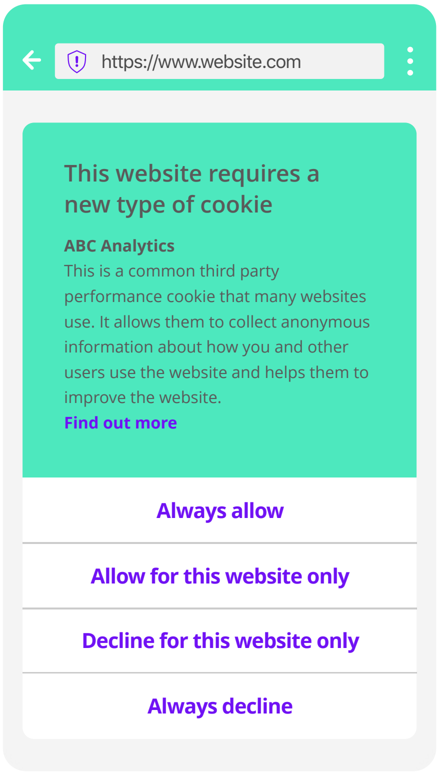
You blocked sites like this

You have chosen for marketing cookies to be disabled and so www.website.com can not load. Either return to your previous page or change your cookie preferences. Need cookie help?

21

21
Browser Cookie Warning
If users restrict certain cookies then the browser will need to alert the user whenever they try to access a site which doesn't match their settings.

Whilst we do see value in having the browser as the point of control – the moment at which these choices are made is crucial. They should be distributed throughout a user's experience with digital services, not just upfront, to provide information at relevant moments. The browser should be doing the hard work for users. For example, users could only be asked to make a choice about a specific type of cookie when they first encounter a website requesting it. Similarly, if users accept a type of cookie with one website, then perhaps the browser could offer the option to grant permission to other websites for similar usage – a like-for-like agreement.

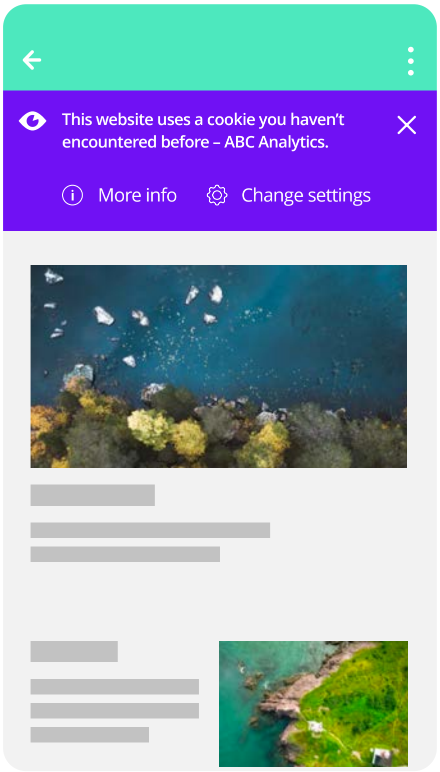


This website requires a new type of cookie

ABC Analytics

This is a common third party performance cookie that many websites use. It allows them to collect anonymous information about how you and other users use the website and helps them to improve the website.

22


This website uses a cookie you haven't encountered before – ABC Analytics.

23

22

Contextual Consent

Here the users is informed about a new cookie type by a prominent browser alert and must select from a number of consent options before continuing.

22

Contextual Alert

Alternatively the user may be alerted to a new cookie type by a less obtrusive browser banner which gives them the ability to judge the site itself as part of their decision.

The browser isn't the only way to offer this control. We could continue to do so on a website by website basis but encourage service providers to surface controls where and when contextually relevant. Whether opt-in or opt-out – this would mean that usage requirements are explained at moments when the surrounding experience aids comprehension and informs choice.

Conclusion

To conclude – we welcome the aims of the ePR and the values on which it is based. Transparency and control of their personal data are essential to user trust. However, the prescriptive nature of the regulation paints too narrow a picture of how transparency and control may be achieved. In fact, in some instances, it may even fail to do either. Furthermore, it does not support genuinely useful and important UX innovations and may stifle our potential to develop new ones in the future.

Greater flexibility in how the regulation is formulated would allow design that would enhance the options for the end users. To achieve great UX which delivers on the ePR values – designers need more freedom to select and sequence privacy controls throughout the UX, not just upfront. Distributing these controls across the user journey avoids overloading the onboarding experience, helps engage users with privacy settings through contextual relevance and allows for user understanding to build over time.

It is not useful to rely completely on opt-in control mechanisms, based on the high consent requirements of the GDPR. Experiencing a service can be one of the best ways to understand how it delivers value from your data. We are concerned that an over emphasis on opt-in will lead to people excluding themselves from services, due to a lack of understanding rather than as an active, informed choice.

We also need further guidance on how transparency and control may be achieved for applications which utilise new technologies. Whether it's voice interfaces, augmented reality, virtual reality, distributed ledgers or other emerging technologies – all pose new privacy challenges which have been insufficiently explored by neither businesses nor regulators.

It should also be noted that our voice is just one of many within the design industry. We welcome and encourage input from others in the field into this urgent and important conversation.

Overall – we value the freedom to create varied, creative and engaging experiences on the basis of principles instead of prescriptive rules. We know that moments of interruption or repetition cause disengagement. There needs to be scope to approach privacy communication with the same care, consideration and creativity users rightfully expect. This is how we will drive engagement, fuel transparency and enable truly informed choice.

Contact

Normally
48-50 Scrutton St
London
EC2A 4HH

hello@normally.com

www.normally.com