

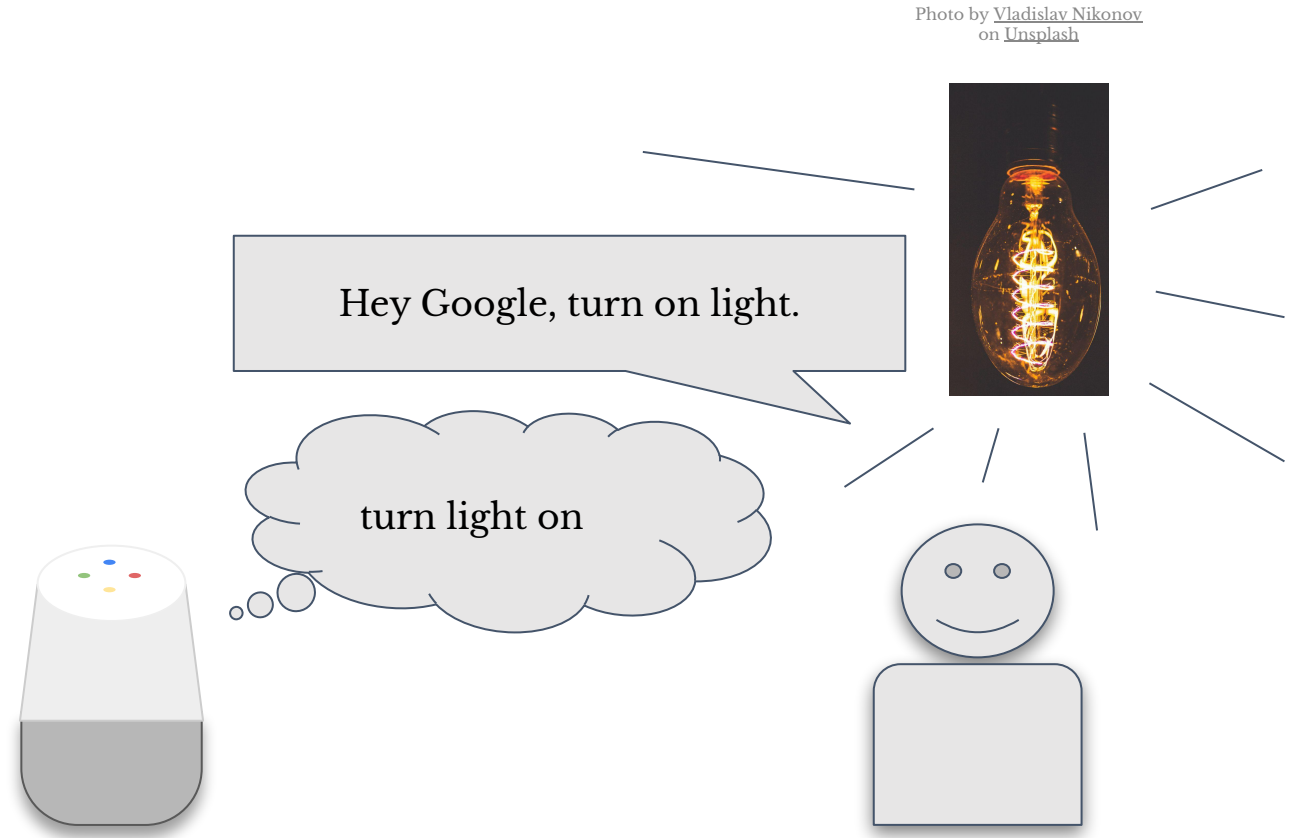
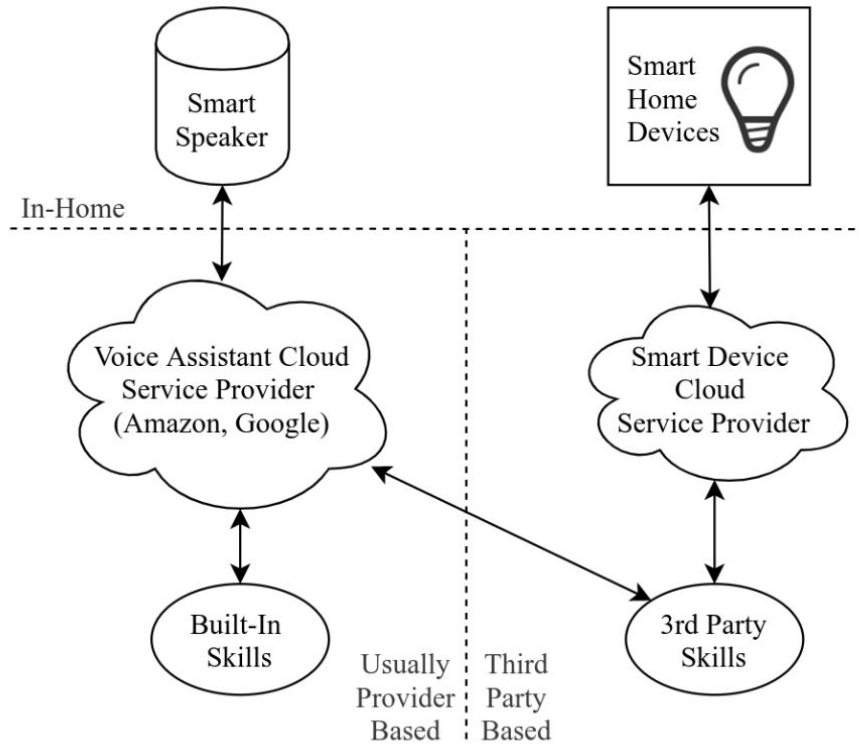


Week 11: GDPR and HCI

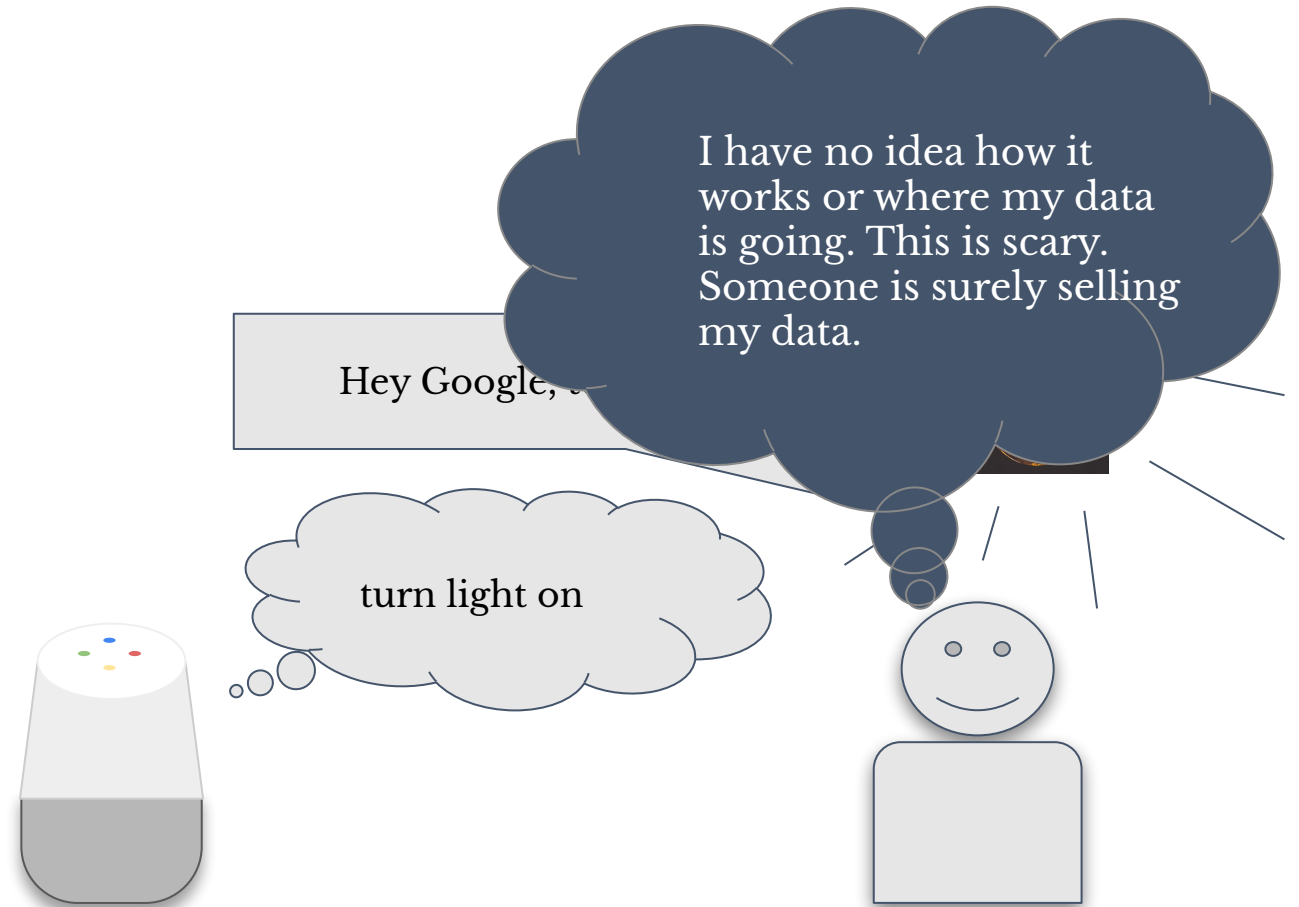
Nicole Meng-Schneider



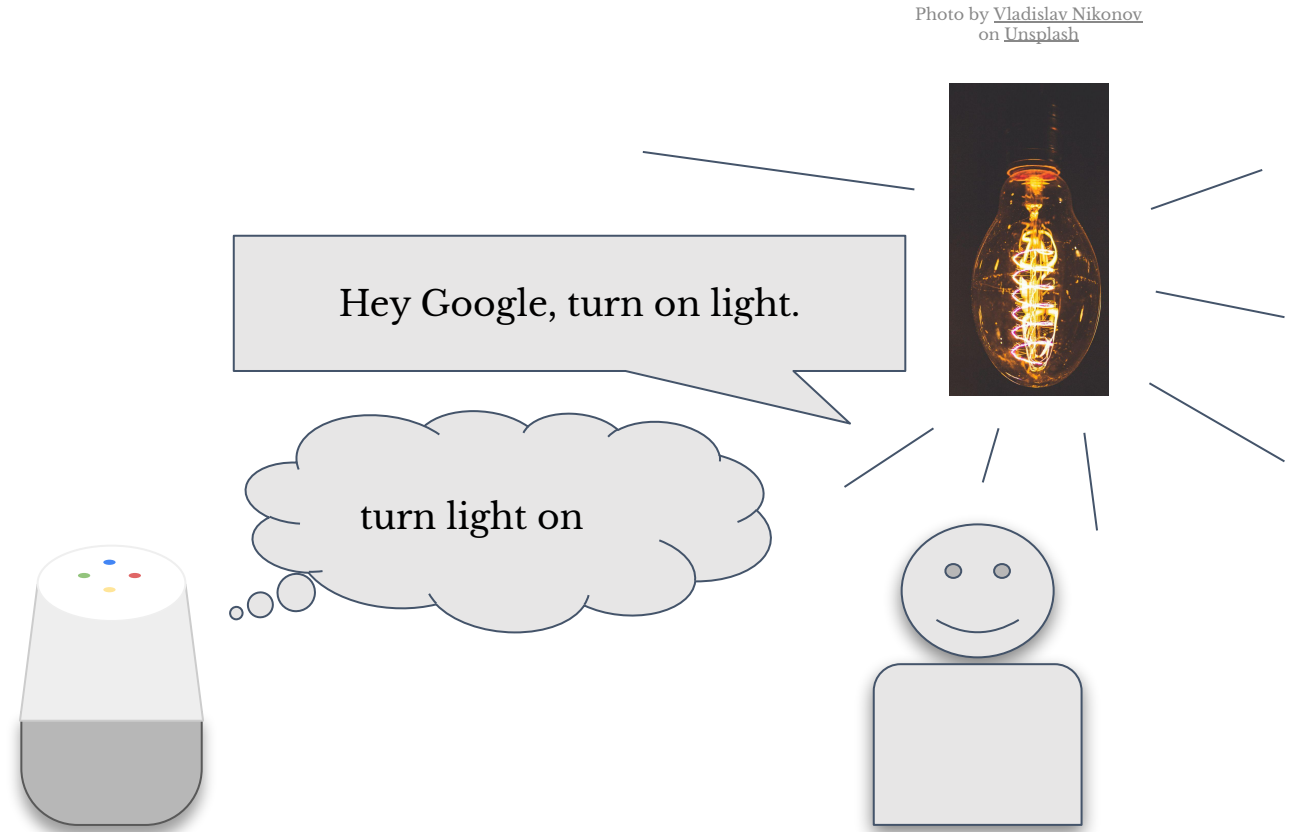
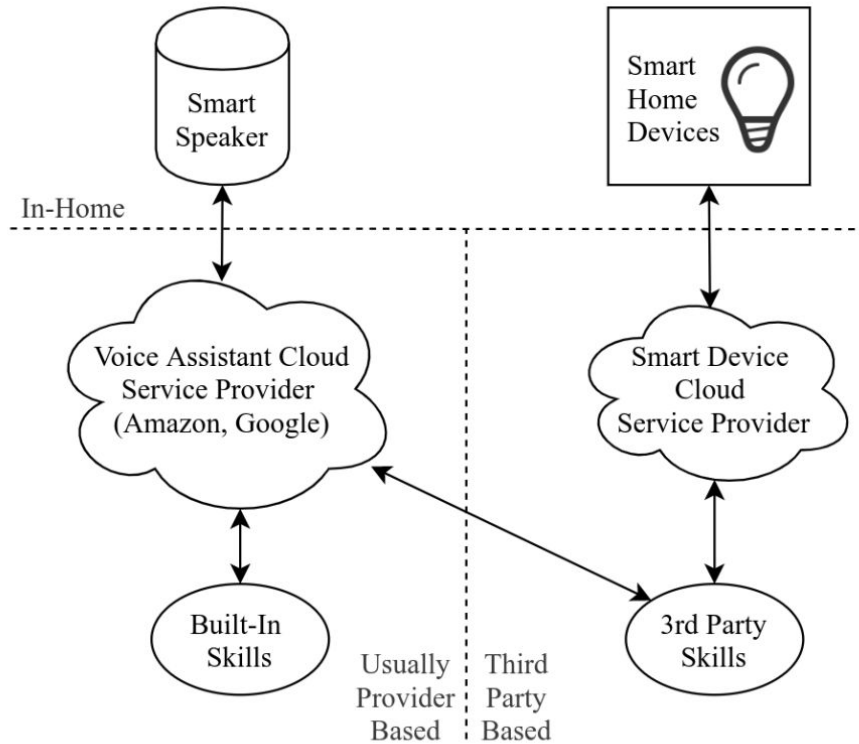
Remember how smart speakers work



Before GDPR: Little transparency and control



After GDPR: More Transparency and Control



What is GDPR?

General Data Protection Regulation (GDPR)

- In effect from May 2018
- Legal framework that governs data privacy and security across the EU and UK
 - i.e. how companies should collect, store, and handle our personal data
 - Applies to any organisation with ties to EU, even if based somewhere else
- Main Goal: Protect people's privacy by giving them more control
- Dictates:
 - Consent for data collection, handling and storage
 - Users should have control over their data
 - Data should be handled securely
 - Transparency of data use
 - What is personal data

What is personal data?

GDPR Art.4 (1) - Definition of Personal Data

- (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

GDPR Art.9 - Sensitive Data (special category)

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

GDPR Main Principles

- **Strong Data Subject Rights**
 - Right to erasure (Right to be forgotten)
 - Right of access
 - Right to rectification
 - And others

GDPR Main Principles

- **Strong Data Subject Rights**
 - Right to erasure (Right to be forgotten)
 - Right of access
 - Right to rectification
 - And others
- **Data Minimisation**
 - Collection of personal information to what is directly relevant and necessary to accomplish a specified purpose
 - Store only for as long as needed

GDPR Main Principles

- **Strong Data Subject Rights**
 - Right to erasure (Right to be forgotten)
 - Right of access
 - Right to rectification
 - And others
- **Data Minimisation**
 - Collection of personal information to what is directly relevant and necessary to accomplish a specified purpose
 - Store only for as long as needed
- **Consent**
 - When consent can be implied and when it has to be explicit
 - Right to withdraw consent
 - Freely given, Specific, Informed, Unambiguous

GDPR Main Principles

- **Strong Data Subject Rights**
 - Right to erasure (Right to be forgotten)
 - Right of access
 - Right to rectification
 - And others
- **Data Minimisation**
 - Collection of personal information to what is directly relevant and necessary to accomplish a specified purpose
 - Store only for as long as needed
- **Consent**
 - When consent can be implied and when it has to be explicit
 - Right to withdraw consent
 - Freely given, Specific, Informed, Unambiguous
- **Transparency**
 - Clear communication what data is collected and why

GDPR Main Principles

- **Strong Data Subject Rights**
 - Right to erasure (Right to be forgotten)
 - Right of access
 - Right to rectification
 - And others
- **Data Minimisation**
 - Collection of personal information to what is directly relevant and necessary to accomplish a specified purpose
 - Store only for as long as needed
- **Consent**
 - When consent can be implied and when it has to be explicit
 - Right to withdraw consent
 - Freely given, Specific, Informed, Unambiguous
- **Transparency**
 - Clear communication what data is collected and why
- **Security measures**
 - Strong security measures in place to protect user data (e.g. Encryption and pseudonymisation)
 - Immediate notification in case of data breach

GDPR Main Principles

- **Strong Data Subject Rights**
 - Right to erasure (Right to be forgotten)
 - Right of access
 - Right to rectification
 - And others
- **Data Minimisation**
 - Collection of personal information to what is directly relevant and necessary to accomplish a specified purpose
 - Store only for as long as needed
- **Consent**
 - When consent can be implied and when it has to be explicit
 - Right to withdraw consent
 - Freely given, Specific, Informed, Unambiguous
- **Transparency**
 - Clear communication what data is collected and why
- **Security measures**
 - Strong security measures in place to protect user data (e.g. Encryption and pseudonymisation)
 - Immediate notification in case of data breach
- **Responsibility**
 - Dedicated Data Protection Officer to ensure compliance (large companies only)

Full legal text: <https://gdpr-info.eu/>

Think Pair Share

What does GDPR mean for us as designers and developers?

Think for 1 min

Pair for 3 min

Share for 5 min

GDPR Principles

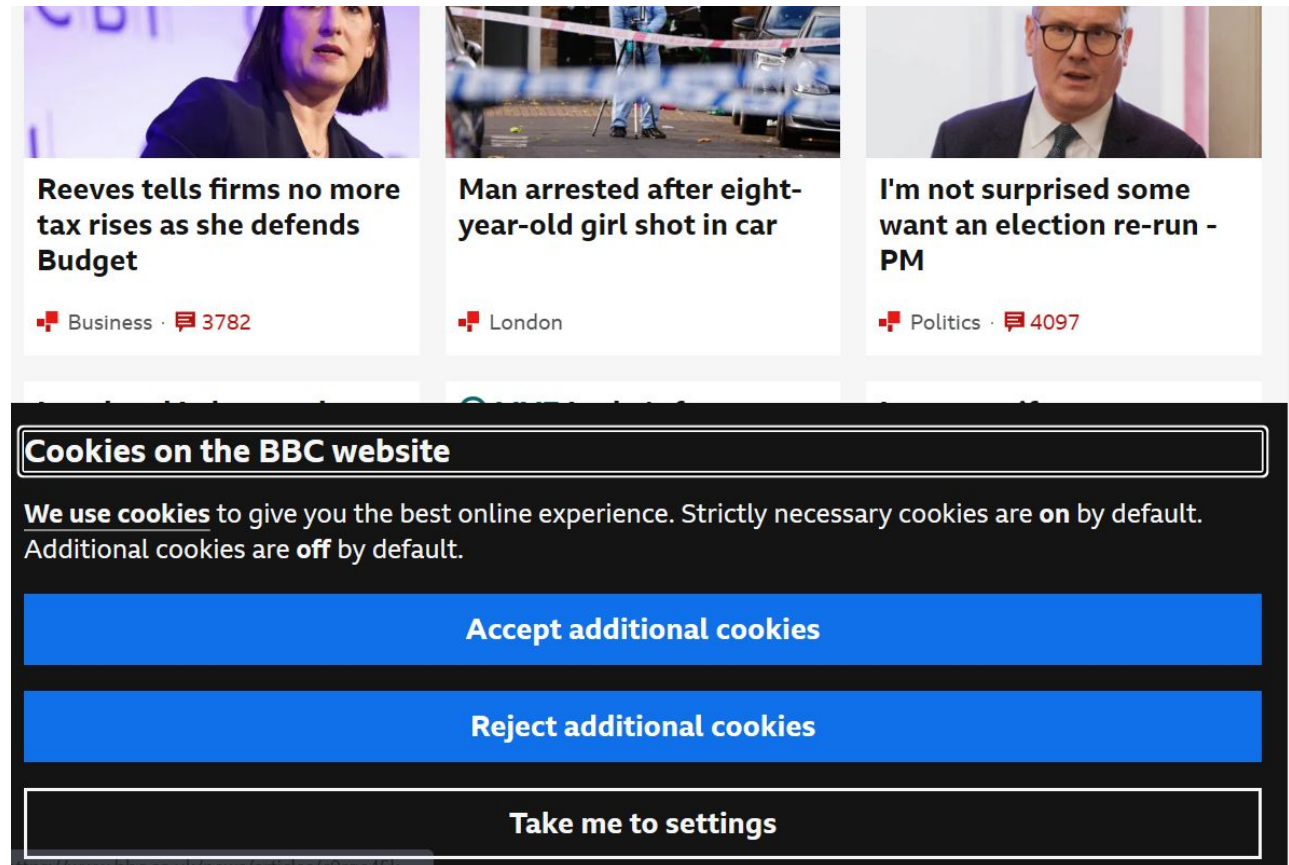
- Strong Data Subject Rights
- Data Minimisation
- Consent
- Transparency
- Security measures
- Responsibility

A good designer
translates these legal requirements
into clear, usable features to help build
safe and trustworthy technology

So how can we
do that?

Clear Consent Mechanisms

- Accept and decline option
- Way to get more information
- Unambiguous: consent is not assumed through pre-ticked boxes or ambiguous phrasing
- User makes an active choice



The screenshot displays the BBC News homepage with three news stories:

- Reeves tells firms no more tax rises as she defends Budget**
Business · 3782
- Man arrested after eight-year-old girl shot in car**
London
- I'm not surprised some want an election re-run - PM**
Politics · 4097

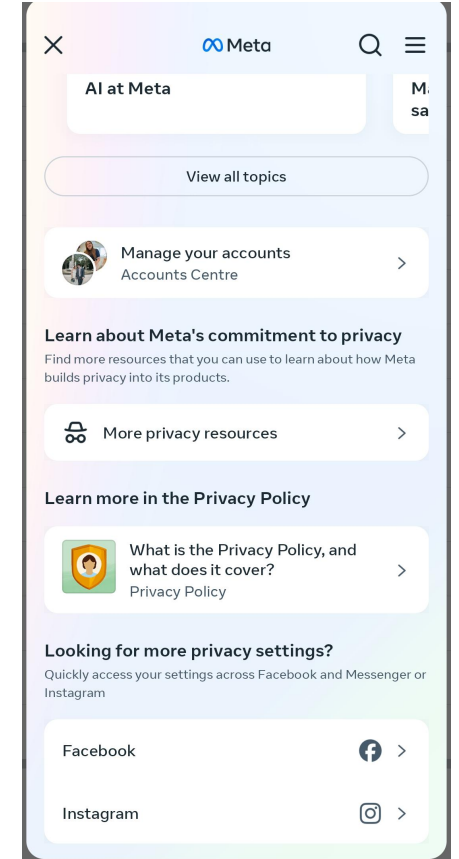
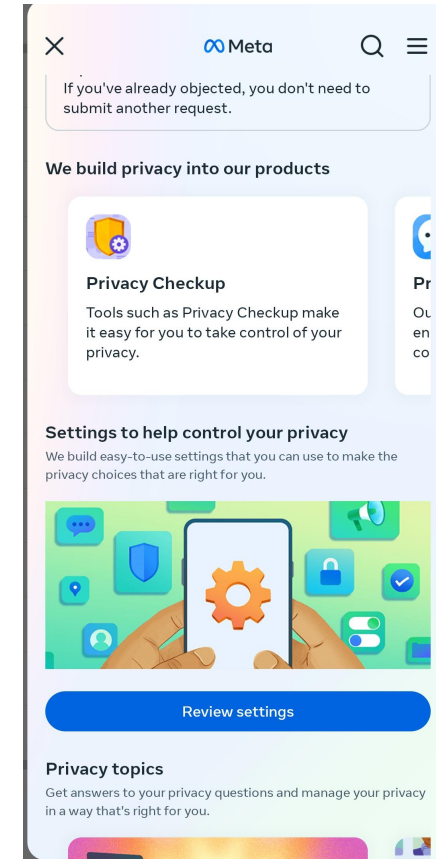
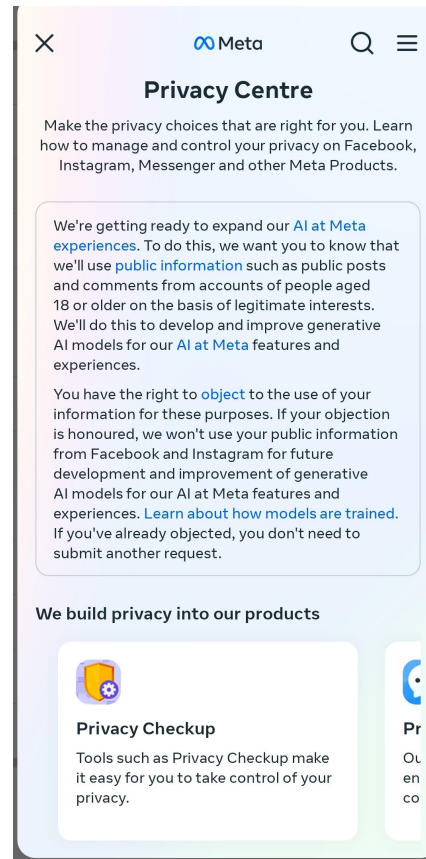
Below the stories is a cookie consent banner titled "Cookies on the BBC website". The banner states: "We use cookies to give you the best online experience. Strictly necessary cookies are **on** by default. Additional cookies are **off** by default." It includes three buttons: "Accept additional cookies", "Reject additional cookies", and "Take me to settings".

Cookie Dialogue on
<https://www.bbc.co.uk/>

So how can we do that?

Accessible Privacy Settings

- Privacy settings are easy to find and manage
- Intuitively organised and easily understood
- Allow users to easily update their preferences



Facebook Privacy centre

So how can we do that?

Transparent Language

- clear, straightforward language
- no jargon or complex legal language
- help users understand what data is collect, why and how it will be used

3. Personal data we collect about you

These tables set out the categories of personal data we collect from you. You can also watch our video about [Personal Data at Spotify](#).

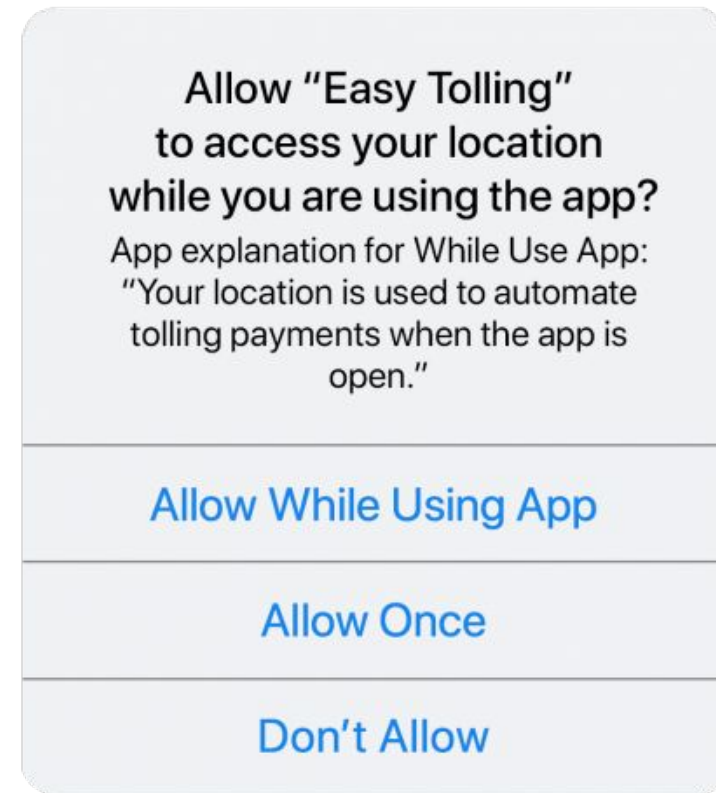
Collected when you sign up for the Spotify Service or when you update your account	
Category	Description
User Data	<p>Personal data that we need to create your Spotify account and that enables you to use the Spotify Service.</p> <p>The type of data collected and used depends on the type of Service Option you have. It also depends on how you create your account, the country you are in, and if you use third party services to sign in. This may include your:</p> <ul style="list-style-type: none">• profile name• email address• password• phone number• date of birth• gender• street address (see further details below)• country• university/college (for Spotify Premium Student) <p>We receive some of this data from you e.g. from the sign up form or account page.</p> <p>We also collect some of this data from your device e.g. country or region. For more information about how we collect and use this data, see 'Your general (non-precise) location' in the Usage Data category.</p>
Street Address Data	<p>We may ask for and process your street address for the following reasons:</p> <ul style="list-style-type: none">• to check eligibility for a Service Option• to deliver notices which are required by law• to deliver support options• for billing and tax administration• to deliver physical goods or gifts which you have requested <p>In some cases, we may use a third party application to help you verify your address, such as Google Maps.</p>

Additional data you may choose to give us	
Categories	Description
Voice Data	<p>If voice features are available in your market and where you've chosen to use a voice feature, we collect and process voice data. Voice data means audio recordings of your voice and transcripts of those recordings.</p> <p>For more information on how different voice features work, and how you can control and turn them off, see our Voice Control Policy.</p>
Payment and Purchase Data	<p>If you make any purchases from Spotify or sign up for a paid Service Option or a trial, we will need to process your payment data.</p> <p>The exact personal data collected and used will vary depending on the payment method. It will include information such as:</p> <ul style="list-style-type: none">• name• date of birth• payment method type (e.g. credit or debit card)• if using a debit or credit card, the card type, expiration date, and certain digits of your card number Note: For security, we never store your full card number• ZIP/postal code• mobile phone number• details of your purchase and payment history
Survey and Research Data	<p>When you respond to a survey or take part in user research, we collect and use the personal data you provide.</p>

So how can we
do that?

Limiting Data Collection

- determine which data is necessary for the service to run and which is optional
- Avoid collecting data when not absolutely relevant
- Ensure deletion when data is not needed anymore



Think Pair Share

Which other GDPR UI components can you think of?

Think for 1 min

Pair for 3 min

Share for 5 min

GDPR Principles

- Strong Data Subject Rights
- Data Minimisation
- Consent
- Transparency
- Security measures
- Responsibility

What changes followed GDPR?

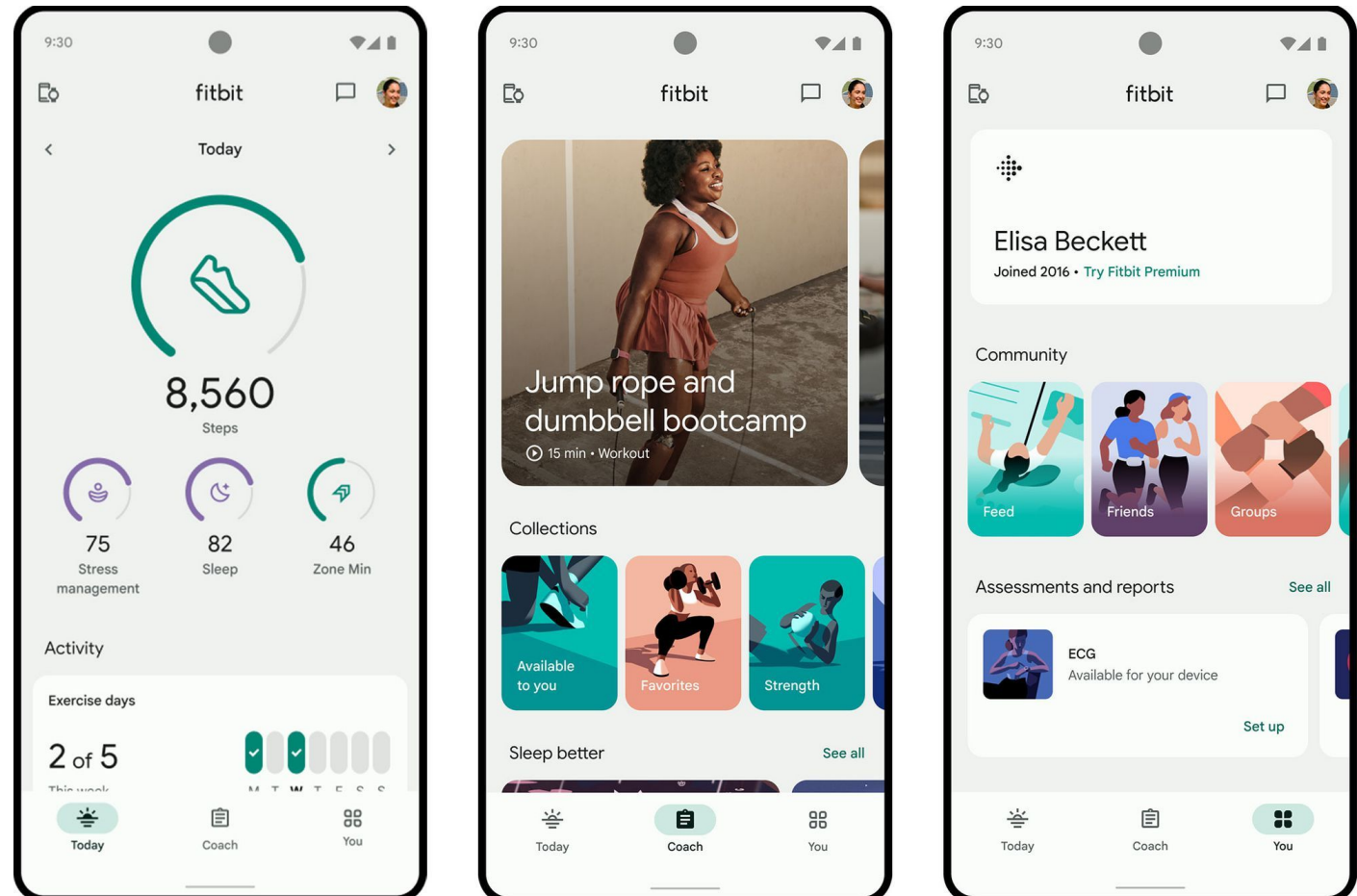
Internet of Things (IoT) Devices (e.g. smart home)

- Enhanced Data Control (Retention, Deletion, Management)
- Transparency on Data Usage
- Clearer Consent and Privacy Notices
- Data Security Improvements



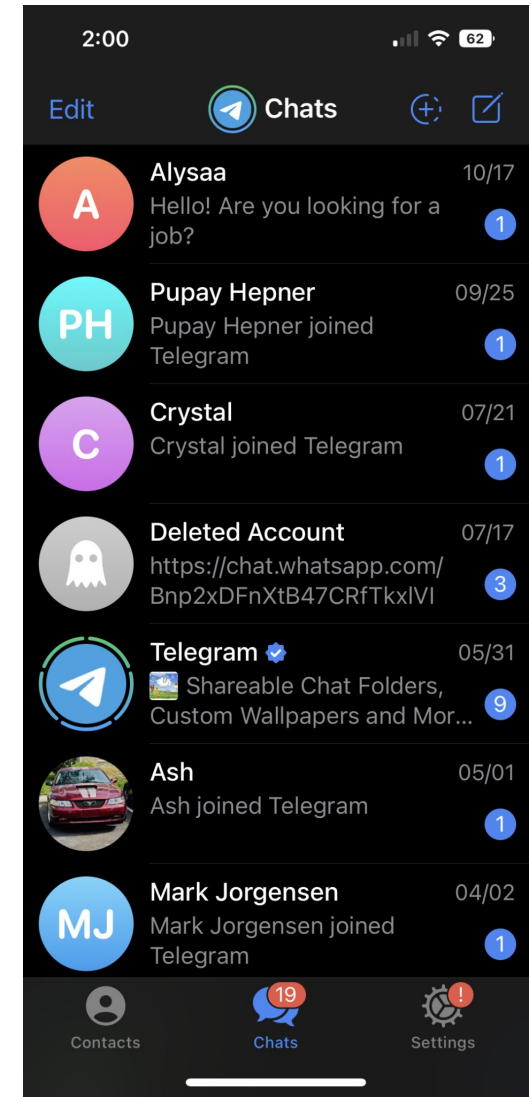
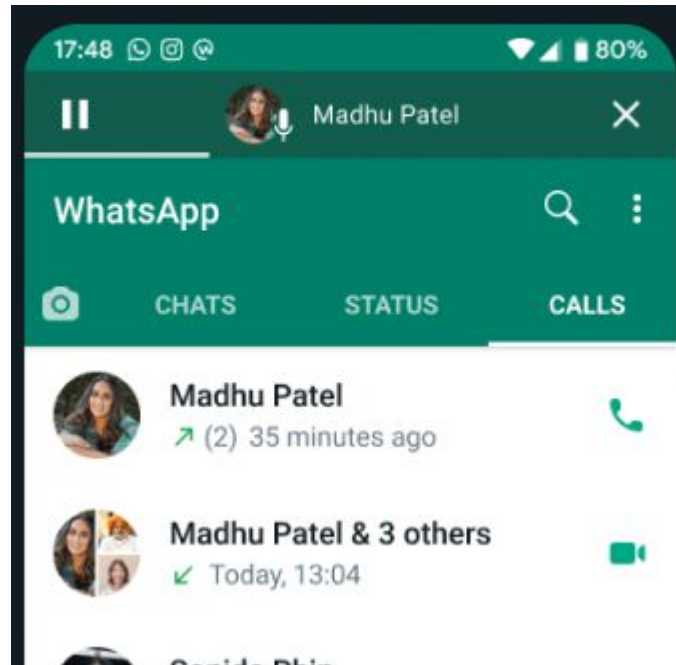
Mobile Apps (e.g. Health and Fitness Apps)

- Data Minimization
- Consent for Sensitive Data
- Anonymization of Data
- Parental Consent for Minors



Messaging Apps (e.g. WhatsApp, Telegram)

- Data Minimization
- End-to-End Encryption
- Deletion and Data Portability
- More Transparency on
- Data Processing



Summary GDPR

- **Greater Control Over Personal Data**
 - Data Access and Portability
 - Right to Be Forgotten
- **Clearer Consent and Privacy Settings**
 - Transparency and Consent Mechanisms
 - Better Privacy Notices and Settings
- **Protection from Data Misuse**
 - Minimized Data Collection
 - Clear Purpose Limitation
- **Improved Security Standards**
 - Stronger Data Security Requirements
 - Data Breach Notifications
- **A Culture of Accountability in Tech Companies**
 - Increased Accountability
 - Privacy by Design

Any questions?



Week 11: GDPR and HCI

Nicole Meng-Schneider

