DATA PROTECTION &
CHATBOTS

In this brAInfood - aimed at youngsters - the Knowledge Centre Data & Society provides more information about chatbots.

The brAInfood contains a fictional story about Lotte who talks to a chatbot that presumably passes on information about Lotte to companies. Furthermore, some points of attention regarding chatbots are explained, as well as a number of tips for youngsters to betterprotect their (personal) data.

In this way we want to make youngsters more aware of how chatbots function and encourage them to reflect on the data that is collected from them by chatbots.

Knowledge Centre Data & Society (2021). Data protection & chatbots. brAInfood of the Knowledge Centre Data & Society. Brussels: Knowledge Centre Data & Society.

This document is available under a CC BY 4.0 license.

brAInfood of the
Knowledge Centre Data
& Society

LOTTE'S STORY

It's morning when Lotte (12) activates her Messenger app. The first chat Lotte always consults is her '**big sister Ella**'. Ella is **a chatbot which listens** and can **advise teenagers** like Lotte. Lotte talks to Ella every morning and tells her how she slept, what she dreamt about or what her day looks like.

Lotte has increasingly started to regard Ella as a sister. She can tell Ella all her **secrets** and can ask her **awkward or embarrassing questions** with no shame. Ella is always friendly and will never argue, as Lotte sometimes does with her real brother and sister.

Later in the day, when Lotte uses social media such as Facebook and Instagram, she notices several **advertisements** of sanitary pads on her **timeline**, something she has been talking about with Ella for the past few days. She finds this strange, because Lotte herself has never looked up anything about it on the internet. She wonders if her chats with Ella have something to do with this.

WHAT IS A CHATBOT?

A chatbot is an **automated conversation partner** that **interactively engages** with a user by:
- **Providing information** (e.g. by providing you with a concert schedule for the month of March), and/or
- **Asking questions** to (further) help the user (e.g. by asking you what size of pizza you want and when you want it to be delivered).

HOW IS A CHATBOT DEVELOPED?

Before a chatbot can be used, it should learn to speak in a human manner. To do this, **data** from a target group is first collected and analysed. The reliability of a chatbot depends largely on the **quality** of the data it is trained with and the extent to which the data is **comprehensible** to the AI model.

Collecting data is relatively easy, the hard part is **labelling** the data so that the chatbot matches the right answer to the right question.
Once launched, the chatbot also learns from **interactions** with users in order to better anticipate questions. This process needs to be closely monitored. For example, if users of the chatbot use discriminatory language, the chatbot may (unconsciously) teach itself this use of language.

No matter how well a chatbot is tuned or trained, **proper follow-up** remains a must. If a chatbot asks for feedback at the end of a conversation, you know that the functioning of the chatbot is being checked.

WHAT TECHNOLOGY DO CHATBOTS USE?

Decision tree
The chatbot has predefined choice options from which the user cannot deviate. The user communicates his/her choice by clicking on the preferred option.

🎵 **Chatbot**
Online

Hello, I'm the chatbot of the House of Music.

How can I help you?

Order tickets

Go to concert agenda

Okay! This is the agenda for the next month.

Fri. 09/04 – Artiste XL
Sat. 10/04 – Beatzzz
Son. 11/04 – Cymbals & Drums
Thurs. 15/04 – 9R45T

Type a message...

Natural Language Processing
The user can type text freely. The chatbot analyses the text by searching for certain keywords. On the basis of the keywords found, the chatbot formulates an answer. If the chatbot doesn't find any known keywords, it will ask to clarify what the user said so that it can learn and improve.

👕 **Chatbot**
Online

Hello, I'm the chatbot of Pants&Dresses.com. What type of clothes are you looking for?
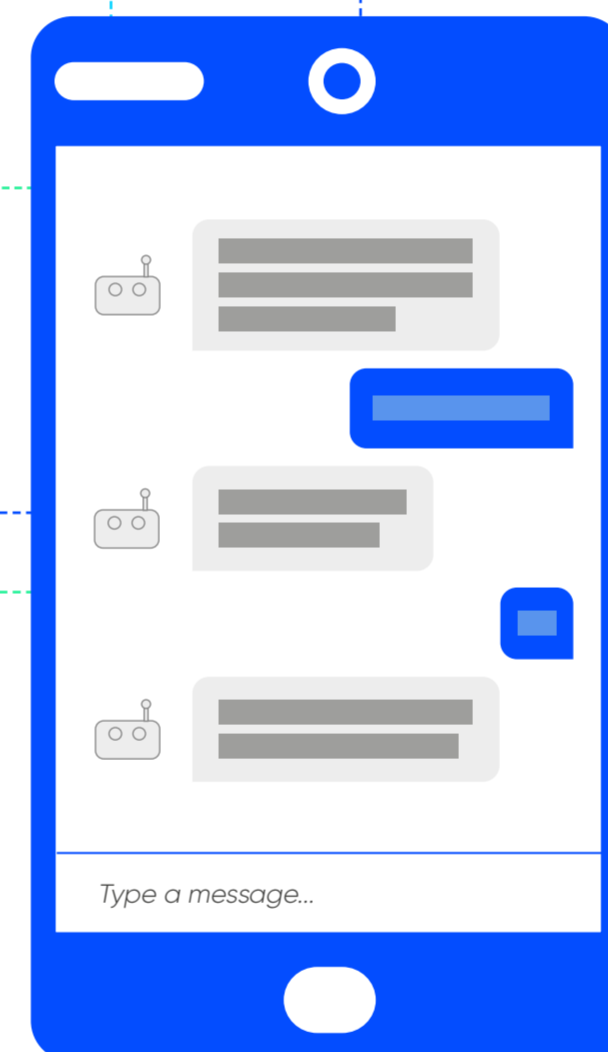
Denims

I don't know denim. Do you mean jeans?

Yes

Great, I learned something new today. Thanks!

Here is our collection of jeans.

Type a message...

HOW DO I RECOGNISE A CHATBOT?

A **trustworthy chatbot** usually lets you know you are interacting with a chatbot instead of a human. Sometimes the creators of a chatbot would like you to think that you are talking to a real person in order to, for example, get sensitive information from you that they can sell or to sell you a product.

It is therefore important to recognise **a number of signals** so that you are not misled. If your conversation partner does the following, you are probably talking to a chatbot:
- Respond very quickly,
- Repeating the same message,
- Using strange syntax, exaggerated emoticons and abbreviations,
- Sending a link or mentioning a product when you didn't give any reason to do so,
- Asking for your personal (financial) data.

Are you still not sure? Try to outsmart the chatbot by asking **complex questions** that do not fit into the conversation ("Have you ever been to Spain when the blossoms were in bloom?"). A person would probably be confused, but can answer this accurately. A chatbot can't.

CAN A CHATBOT HELP ME?

Chatbots are used for **various purposes**, such as automating certain tasks so that the organisation's staff can focus on other tasks. But chatbots are also increasingly being used in **healthcare settings** to, for example, give advice on sensitive topics such as sexuality, relationships, violence and abuse, addiction and drug use or mental health. This can lead to ethical questions.

Chatbots have a lot of potential in this area because they are perceived as less stigmatising than conventional care. In this way, they can be **a first step towards getting help**.

However, **some questions cannot be answered** by chatbots: their ability to interpret human interactions is limited and it is not possible for them to provide a tailored empathic treatment.

Be aware that a chatbot cannot answer all your questions and check what you can or cannot expect from a chatbot's service. A reliable chatbot is transparent about this and will indicate that the application has been extensively tested.

WHO AM I TALKING TO?

Imagine you are talking to a chatbot from your favorite clothing store via WhatsApp Business. Instead of showing you all the jeans available, the chatbot asks what your size is, so it can only show you the ones in your size. Super convenient!

What you might not realise is that your conversation is not only stored and analysed by the store itself, but also by the chat app and other technology platforms. Why is this?

The chatbot was integrated into a **popular chat app** to lower the treshold for you to interact with the organisation. Furthermore, the the underlying technology that chatbots use comes from **major players in the digital market**, such as Google, Facebook, Microsoft, Amazon, etc.

Isn't it strange that besides the clothing store, **other organisations** now know what size you are? Doesn't the integration of a chatbot, in a platform where you chat with family and friends, **blur the line** between personal and business conversations?

Always be aware of the context in which you use a chatbot, and be careful with your data.

WHAT ABOUT MY DATA?

A chatbot needs data from you in order to work properly. What data is collected strongly **depends on the purpose** of the chatbot: a chatbot from a textile company may, for example, collect data about your online purchase history, the links you have clicked and the pages you have visited in order to offer you a more **personalised service**.

These data may seem like they do not say much about who you are, but if you **aggregate** these data, the organisation behind the chatbot **can find out a lot about you**.

Fortunately, a chatbot is not allowed to just collect any data from you. The **General Data Protection Regulation** (GDPR), a European regulatory framework, defines what data of their users companies or organisations can collect, who has access to the data, how long the data can be kept, etc.

There are ways for you to **safeguard your privacy** as well. Never just give out:
- Personal data (name, address, place of residence, telephone number,...)
- Login data and passwords (even if you would receive points for a game or a purchase).

You also have certain **rights in relation to your own data**, such as:
- The right to find out what data is collected about you, and
- The right to make a request to an organisation to delete your data.

HOW DO I REPORT A CHATBOT?

Does the conversation with the chatbot not feel right? Does the chatbot ask for personal or intimate information? Do you disapprove of the chatbot's language?

Then it is best to **block** the chatbot's account, or **report** the chatbot to the platform by pressing the report button in the chat settings. Platforms, such as Instagram, have protocols in place to ban chatbots in order to create a safe online environment for every user.

Have you become a victim of **hacking or fraud**, make sure to visit https://www.safeonweb.be/en for advice and more information on how to notify the appropriate services.

Type a message...