Royal College of Art

THE DATA MAZE

Across RCA **Team 13A**

Chenyan Zhu Martha Ramos Xiangjie Li

2022/23

#

Digital privacy issues refer to concerns around the collection, storage, use, and sharing of personal data in digital spaces. As the use of technology and digital platforms has become increasingly widespread and integrated into daily life, the issues surronding digital privacy have become more pressing.

Privacy breaches and data leaks have become more common, leading to the exposure of sensitive information such as social security numbers, credit card information, and medical records. In addition, there is growing concern over how personal data is being used by companies and other organizations, and whether individuals have adequate control over their own information. This theme is particularly relevant in the context of privacy rights, data protection, and cyber security, which are becoming increasingly important issues as technology continues to advance and our reliance on the internet grows.

About the Team

Our teams consists of 3 members: Chenyan (Digital Direction), Martha (Visual Communication) and Xiangjie (Service Design). We all come from distinct academic and professional backgrounds. Our unique backgrounds provide us with diverse skills and perspectives, which will be beneficial in tackling complex projects.

We believe that our diverse backgrounds and approaches will allow us to develop more innovative and sensible solutions to our challenges.

Team Mission

Our mission is to raise awareness about the potential risks
of sharing personal information online, including data breaches and unauthorised use by third parties.
We aim to achieve this through a game design to involve real-life scenarios and decision-making and encourage people to be more mindful of their personal information and digital sharing habits.

Through our efforts, we hope to build awareness among people to make informed decisions about their online activities and take proactive steps to protect their privacy and personal data.

Design Process & Method

Critical Design uses speculative design proposals to challenge narrow assumptions, preconceptions and givens about the role products play in everyday life. It is more of an attitude than anything else, a position rather than a method.

---Anthony Dunne & Fiona Raby

What is Critical Design?

Critical design is an approach to design that seeks to challenge and provoke societal norms and assumptions. The objective of critical design is not to create commercially viable products, but to create thought-provoking and speculative designs that encourage people to think critically about the impact of technology and design on our lives.

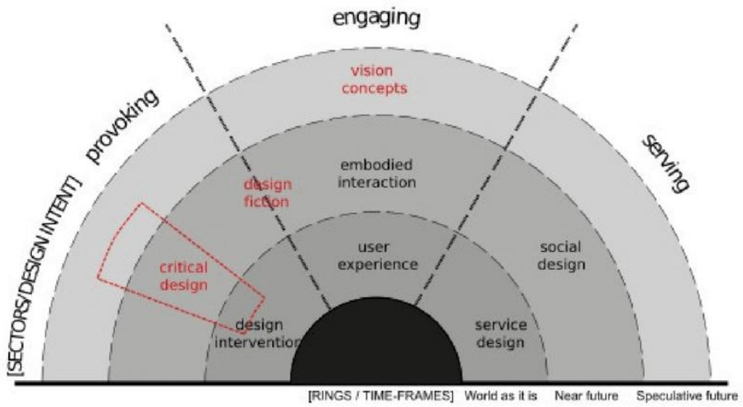
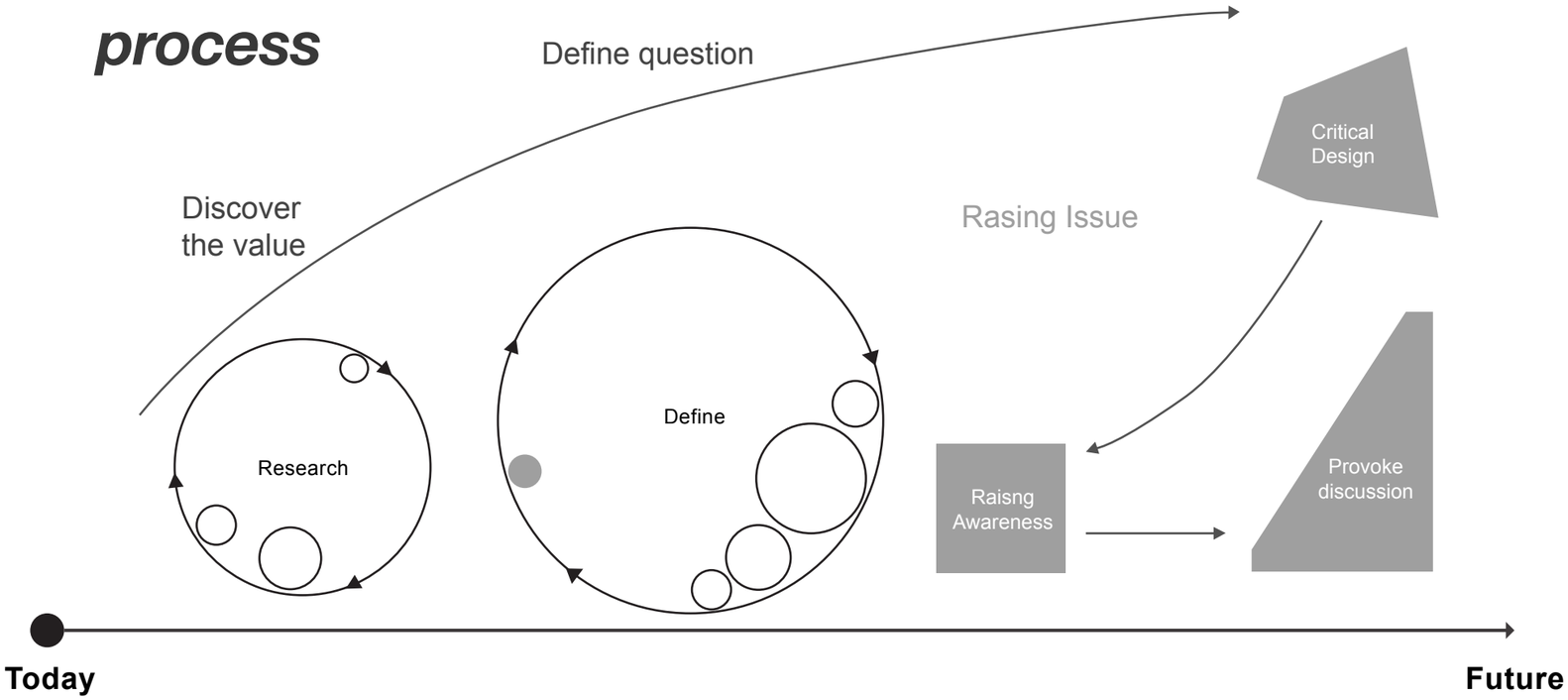


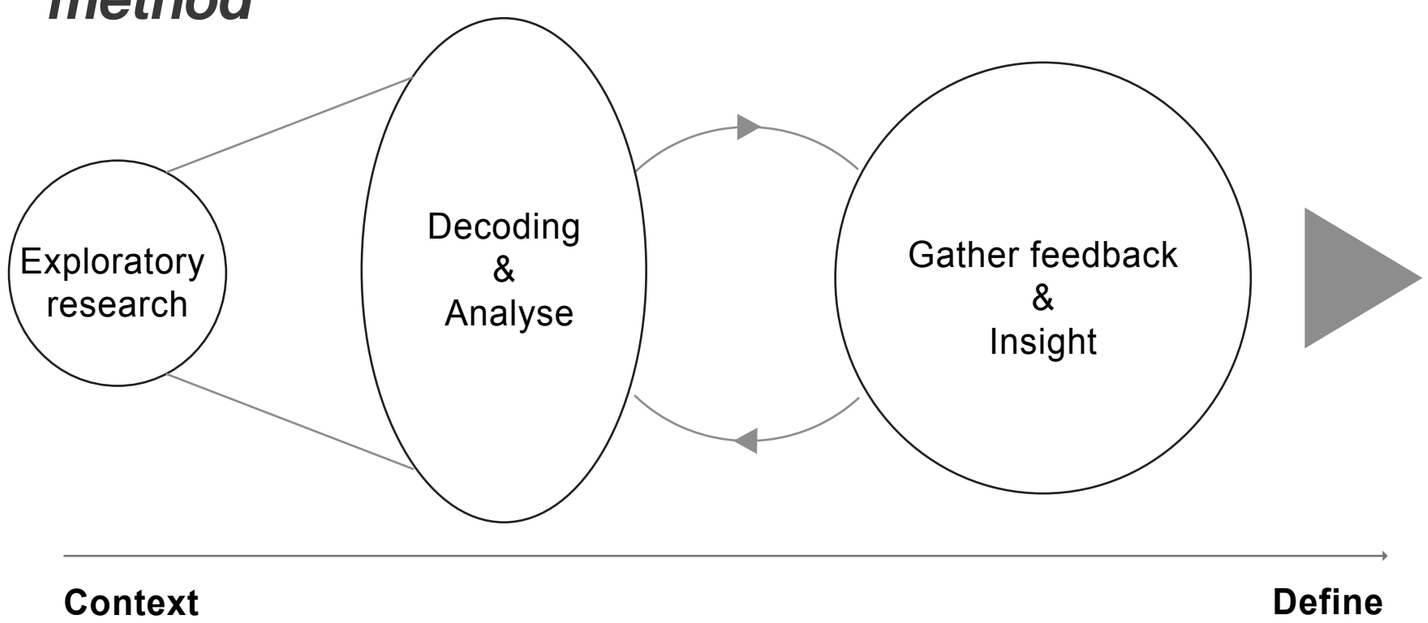
Fig.1

The ultimate goal of critical design is to encourage the audience to question the status quo and to imagine new possibilities for the future, ultimately leading to a more thoughtful and reflective society.

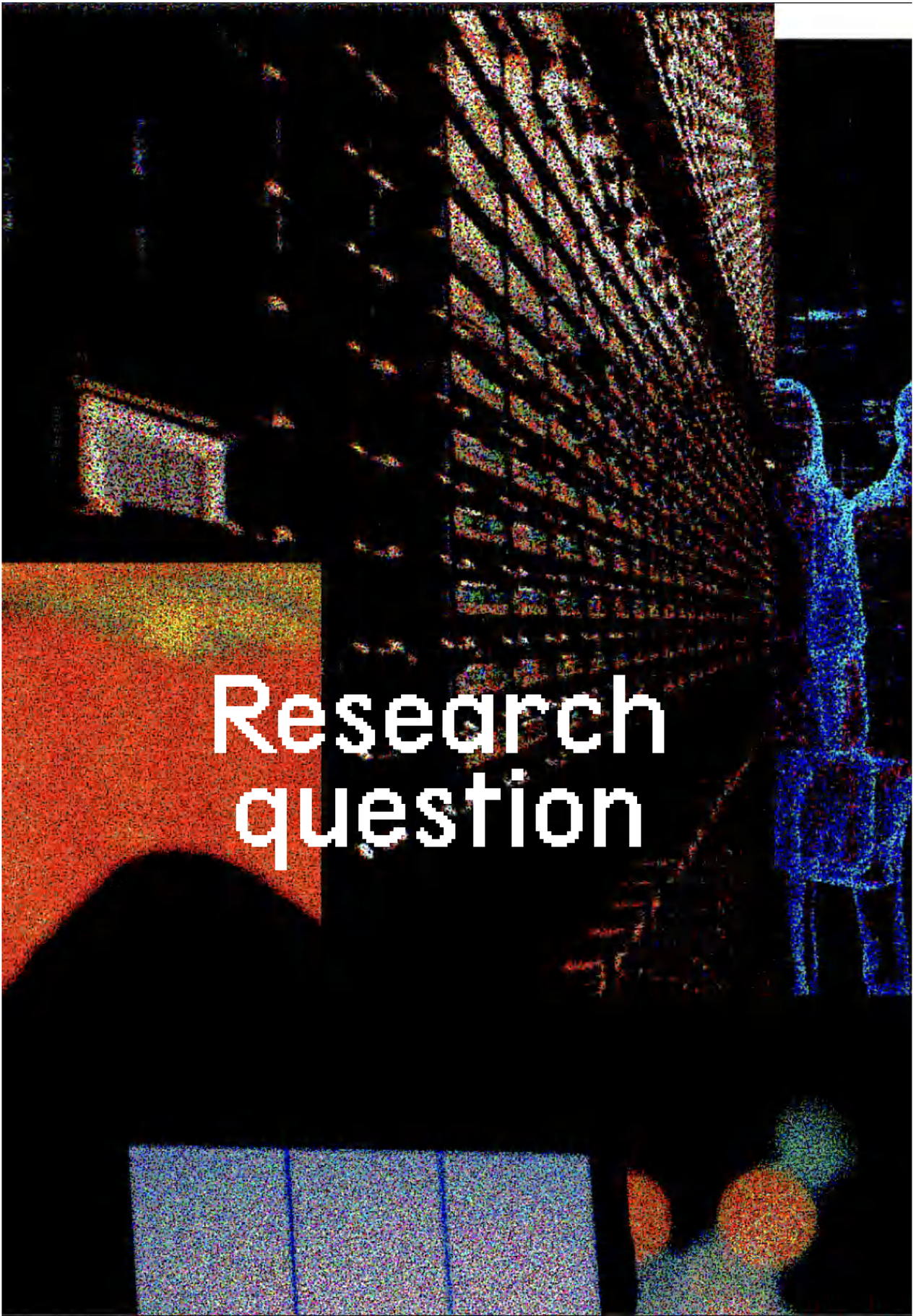
process



method



By creating provocative designs that challenges dominant ideologies or highlight societal issues, critical design aims to provoke discussion, stimulate debate, and promote reflection among our audience.



How can we educate social media users on the importance of privacy, data protection, and digital literacy?

#

The research aims to provide information for the project and ensure that the project takes into account the risks and potential consequences related to data privacy, data breaches, and social media algorithms.

Why choose instagram as our research platform?

Popularity: Instagram is one of the most popular social media platforms, with over 1 billion active users. Its popularity makes it a study worth platform for conducting our research on data issues related to social media usage.

Visual focus: Instagram is a highly visually demanded platform focusing on images and videos. This can help us have more access to visual communication, aesthetics, or consumer behaviour research materials.

Target audience: According to our research objectives, Instagram's user base aligns with the research project's target audience. We focus on the behaviour of people who share their daily life, location, living habits, preference and all other personal information on the online platform.

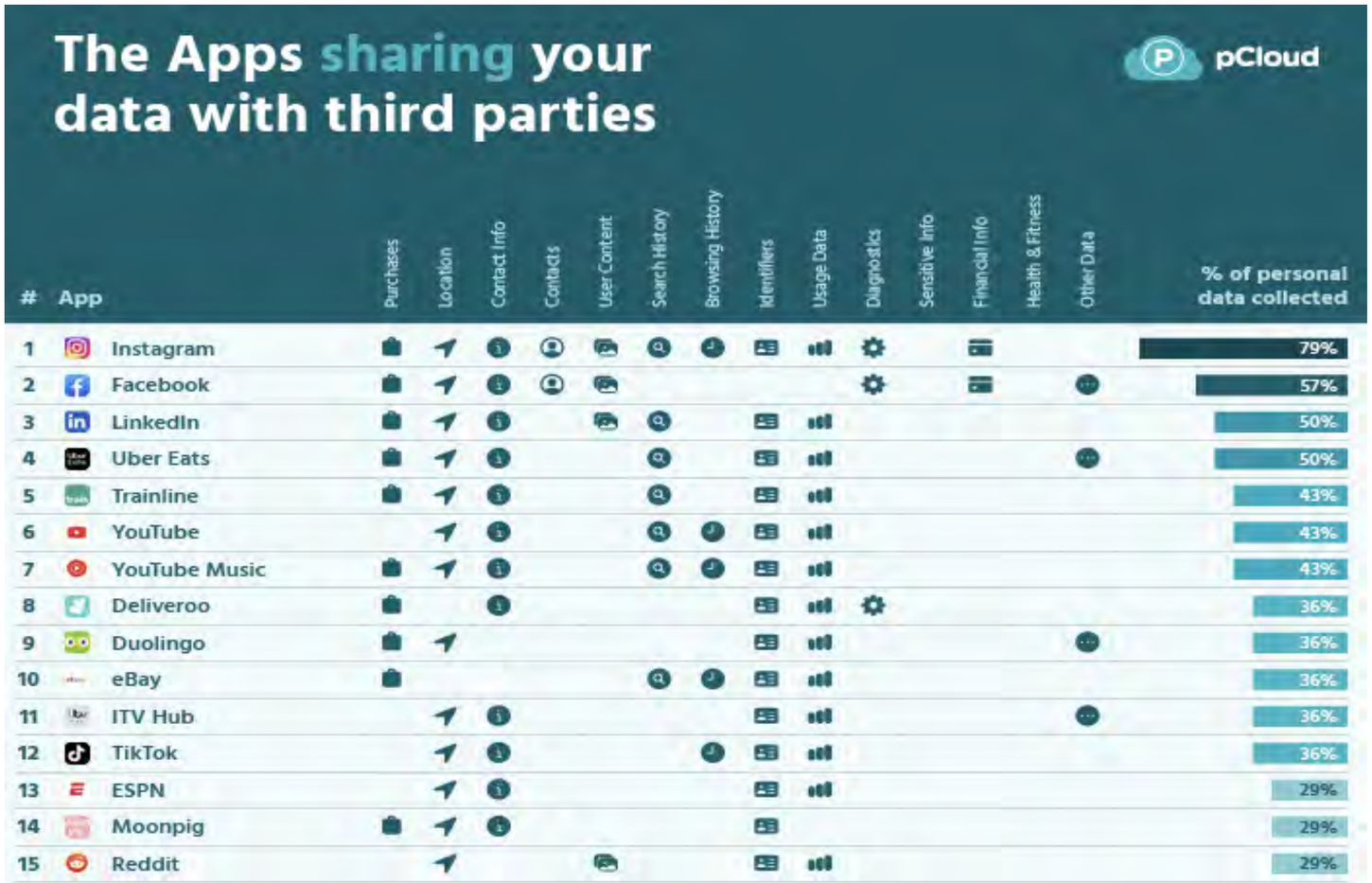


Fig2. Instagram is sharing 79% of your personal data with third parties

Fig1, The spot of Vision Concepts, design fiction, and critical design within ... (no date). Available at: https://www.researchgate.net/figure/The-spot-of-Vision-Concepts-Design-Fiction-and-Critical-Design-within-the-landscape-of_fig2_309617449 (Accessed: February 21, 2023).

How it this data collected?

Instagram uses a combination of algorithms to collect, use, and share personal data. It accounts for various factors, such as the user's engagement with the content, the time the content was posted, and the user's relationship with the account that the content. The algorithm works by collecting and analysing user data to personalise the user's experience on the platform.

Databases collect information such as:

Profile Information: Name, username, email address, phone number, and bio;

User Content: Photos, videos, comments, likes, and any other content that you post on the platform;

Interactions: Instagram tracks interactions between users, such as when two users follow each other, like each other's posts, or comment on each other's posts;

Location Data: Instagram can collect data about your location when you post a photo or video with geolocation data;

Device Information: This includes information such as the type of device you use to access the platform, your operating system, and your internet service provider;

Search and Navigation Data: Instagram tracks what you search for, what you click on, and how you navigate through the platform.

It then collects all this data through tracking technologies like cookies and third-party sources and uses a combination of server storage and cloud storage solutions to store user data. With server storage, Instagram stores account information, posts, comments, and metadata, on its own servers. This data is stored in a centralised database and is accessible to the platform for various purposes, such as to improve its services or for advertising purposes. The platform uses encryption and firewalls to secure this data and prevent unauthorised access. The data stored in the cloud is also encrypted and protected by various security measures, such as firewalls and access controls, to prevent unauthorised access.

Why it is collected?

There are several practices and reasons for the use and sale of personal data for example, data brokering is the process of collecting and aggregating data from various sources, and then selling it to third parties. Instagram collects a significant amount of personal information from its users, including demographic information, interests, behaviours, and purchasing history which can be valuable for companies who are looking to target specific groups of consumers with advertisements or other marketing efforts. Some data brokers have been known to purchase this data from companies like Instagram, and then use it to create detailed customer profiles for use in marketing and advertising. Customer profiling is also a marketing technique that involves gathering information about customers and creating a detailed profile or representation of each customer segment. A profile can then be used to understand customer behaviour, preferences, and habits. Marketers use customer profiling to develop targeted marketing campaigns, personalise the customer experience, and make informed decisions about product development, pricing, and distribution. The information used to create a customer profile can come from a variety of sources, including demographic data, purchase history, online behaviour, and customer feedback. Marketers may also use predictive analytics and artificial intelligence to analyse the data and create a more comprehensive view of each customer.

Instagram, like many other social media platforms, collects a large amount of data from its users. This data is collected in order to personalise the user experience, show targeted advertisements, and improve the overall functionality of the platform.

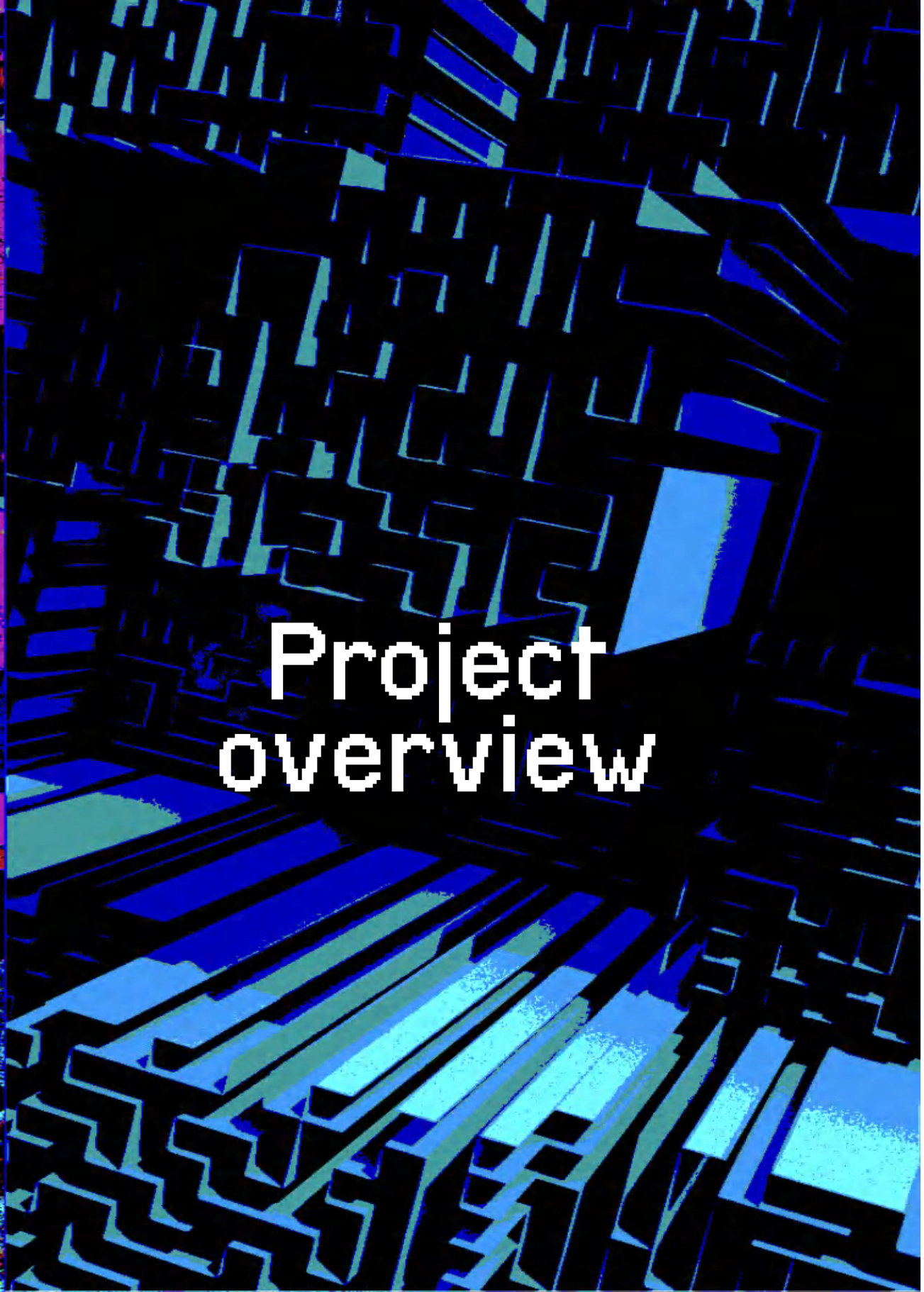
Ethical implications data collection policies

Data privacy and security concerns

There are potential risks associated with the collection and storage of personal information. Sharing user data with third-party companies and partners for advertising purposes can result in information being shared with entities they may not be aware of, for example Instagram shares user data with its parent company Facebook, as well as third-party advertisers, which can raise concerns about how this information is used and who has access to it, which could result in data breaches. Data breaches can occur due to various reasons such as unsecured networks, weak passwords, human error, and malicious attacks. Research has found that the majority of data breaches are caused by malicious attacks, such as hacking and phishing. Unauthorised access to sensitive information can have a range of consequences including identity theft, financial fraud and overall reputational damage. For example the collection and storage of location data can reveal sensitive information about a user's whereabouts, activities, and movements.

Instagram and other platforms also retain user data indefinitely, even after an account has been deleted which makes personal information vulnerable to hackers and other malicious groups. Bias and discrimination may also arise as the platform uses predictive analytics to determine what content to show to users. For example, if the algorithm is trained on data from predominantly white users, it may not provide accurate or relevant recommendations to users of other races or if they are only shown content that aligns with their existing beliefs and interests, it potentially limits their exposure to multiple perspectives and skews their opinion on a certain subject matter. Organisations may use personal data for surveillance and control, raising concerns about civil liberties and freedom of speech, as it can be used to track users, monitor their activities, and target them with unwanted advertising or propaganda. This can lead to privacy violations and the infringement of users' rights to freedom of expression and privacy.

Overall there’s a lack of transparency regarding how Instagram's and many other social platform algorithms work, making it difficult for users to understand how their data is being used and what decisions the algorithm is making on their behalf.

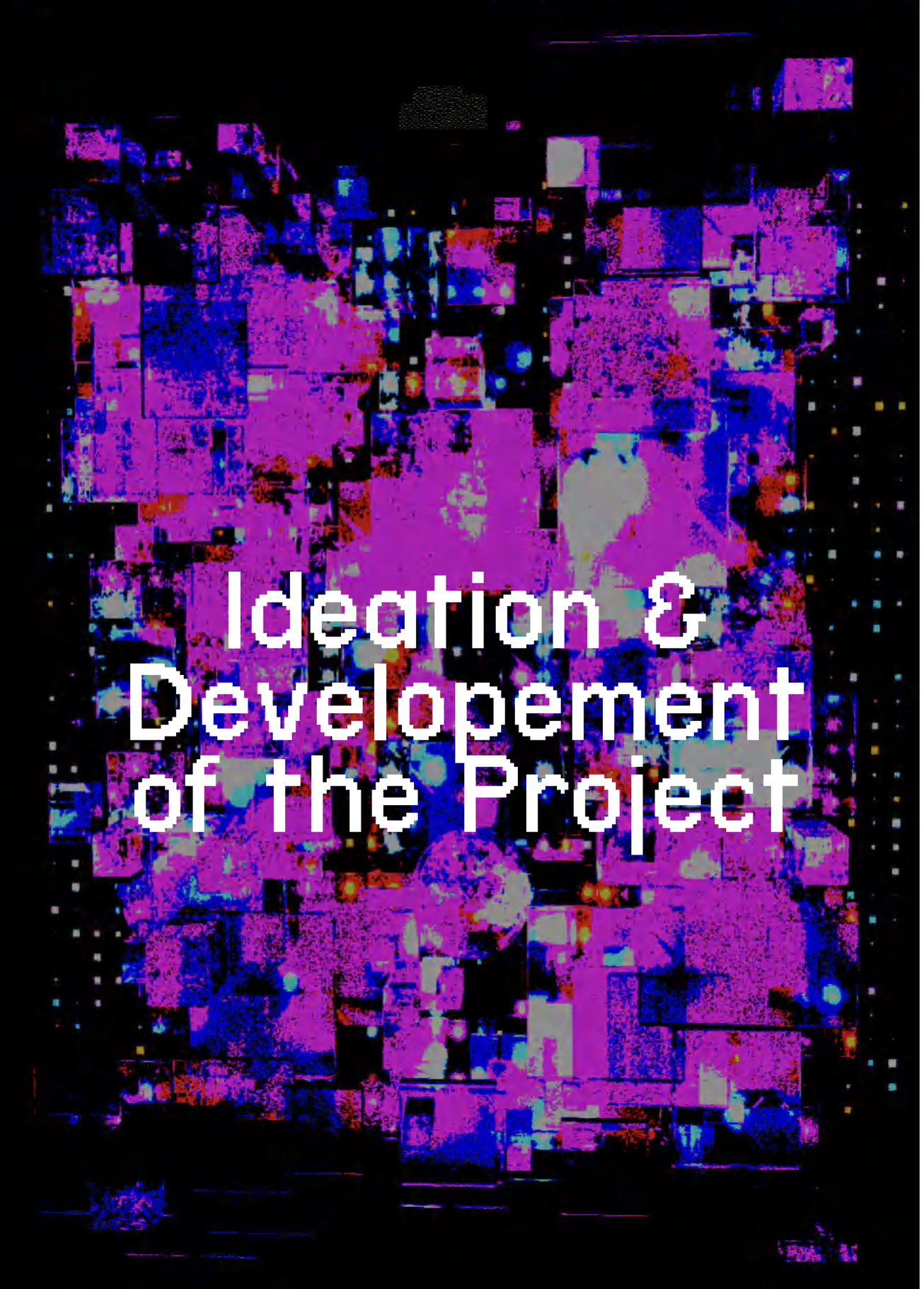


#

This project aims to raise awareness about the potencial risks associated with sharing too much personal information on social media platforms, specifically Instagram. Social media platforms like Instagram have become an integral part of our daily lives, and we often share a significant amount of personal information, such as our location, interests, opinions, and activities, without much thought. Instagram is a good example of the ethical issues regarding data storage because of the way it collects, uses, and stores user data. We aim to draw attention to the issues that may arise in the inherent politicisation and biases built into databases and their ever-growing hold on society and culture.

The main objective of the project is to inform people about the potential consequences of sharing personal information online, including data breaches and unauthorised use of personal data by third parties while also offering practical advice on how to be more mindful about personal information and encourage reflection on players' digital sharing habits.

In order to raise these questions we use the format of a game as a form of critical inquiry for the viewer to make their own reflections and deductions.



#

Finding a platform

We wanted to find a platform/medium that it can aid in understanding complex concepts, make decisions, and reflect on their own experiences in a way that is both entertaining and educational. Games have the unique ability to engage players in a way that other forms of media cannot. By incorporating elements of play and interaction, we can develop a format that allows players to explore the subject in a safe, low stakes environment where they can make mistakes, reflect on their choices, and learn from their actions. Developing a game meant that we could involve real-life scenarios and decision making without any actual risk while still challenging players to consider the potential consequences of their actions.

Target Audience

The game's focus on social media and data collection practices appeals to individuals who use social media platforms (especially younger individuals who have grown up with technology and social media) such as Instagram and are interested in learning more about how their data is collected and used.

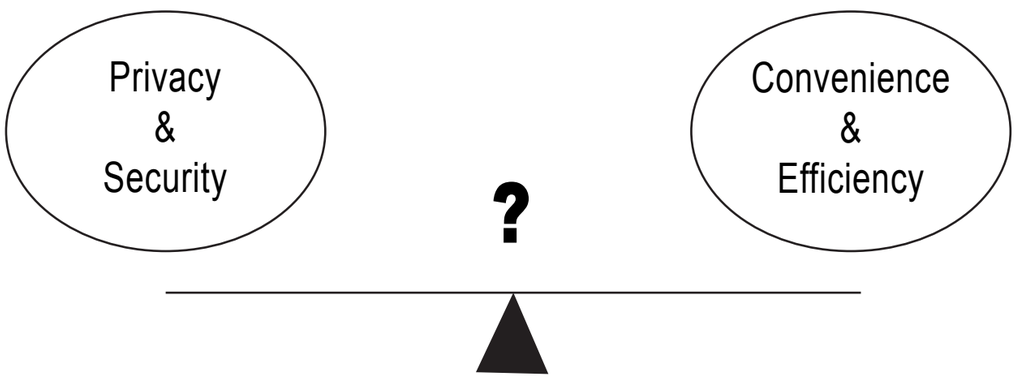
Visual brainstorming

possible characters and game setting

The element of chance

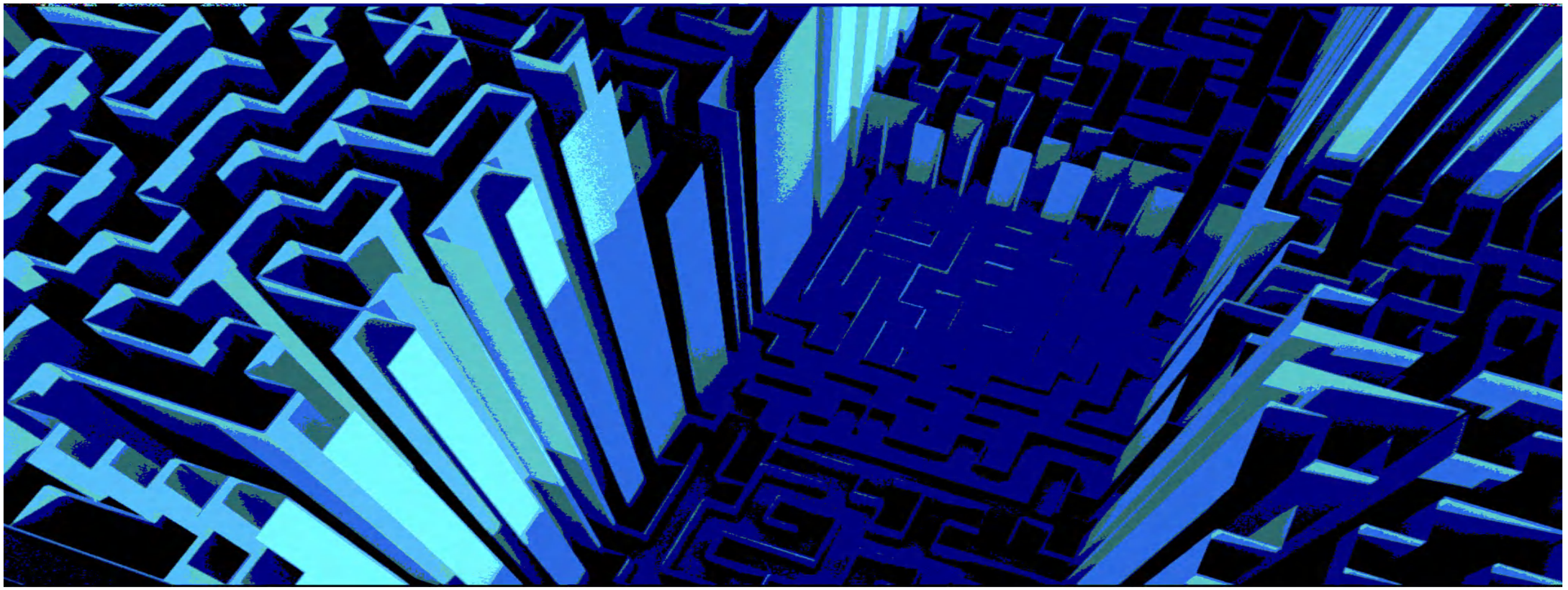
The idea of probability-based outcome

Including elements of chance in a game can make it more exciting and add an element of unpredictability, while still maintaining its educational focus and message. Sharing information online in itself is a gamble, one could be extremely careful and still have the unfortunate realisation their data has been misused in one way or another. The key is to make sure that the element of chance is balanced with the educational content so that the message isn't lost and that taking the necessary steps to protect your privacy does in fact pay off compared to having a haphazard approach. Introducing choices in the game that have a probability-based outcome where, for example, if the player decides to post a picture, there is a certain percentage chance that the picture could be used in an inappropriate way, such as being used for catfishing. Or a hacker might attempt to access the player's account, or a malicious user might try to post harmful comments. The outcome
of these events could be determined by a set of predefined probabilities.



Concept of Maze

Introducing the concept of maze in the game serves multiple purposes, it ties into the central theme of the game both visually and conceptually. Mazes are often associated with exploration and discovery, and by including one in the game, players are encouraged to explore a simulation of the digital world. The maze would also serve as a metaphor for the complex and often confusing world of online privacy and data protection. Like a maze, the world of digital privacy can be difficult to navigate, with dead ends, wrong turns, and hidden paths. By creating a maze in the game, players are given a visual representation of the challenges they may face in the real world when trying to protect their personal data.



#

Data Maze

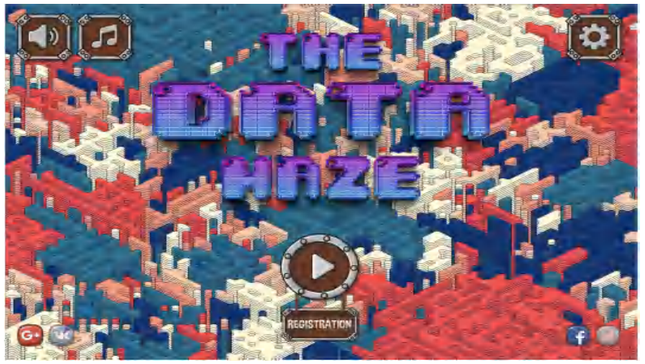
Data Maze intends to be an interactive experience that explores the themes of privacy and data protection in the digital age. It is a single-player game that takes the player through a series of scenarios designed to educate them on the importance of protecting their personal information online. The game is divided into chapters, each with its own set of challenges and decisions for the player to make.In the first chapter, the player is introduced to the game mechanics and asked to create a new social media account. They must choose what information to include in their profile, whether to enable location tracking, and whether to connect the app to their other social media accounts. This sets the tone for the rest of the game, where the player is continually asked to make decisions that will impact their online privacy.

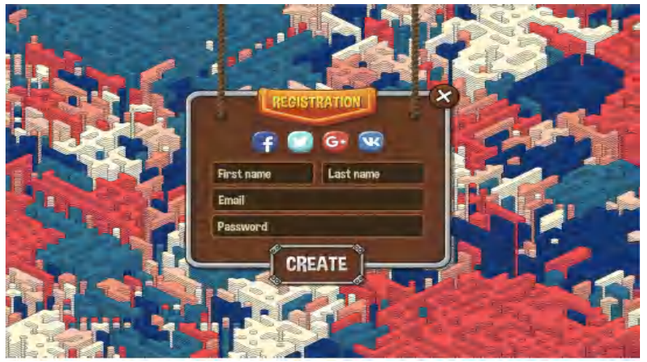
Project Goal

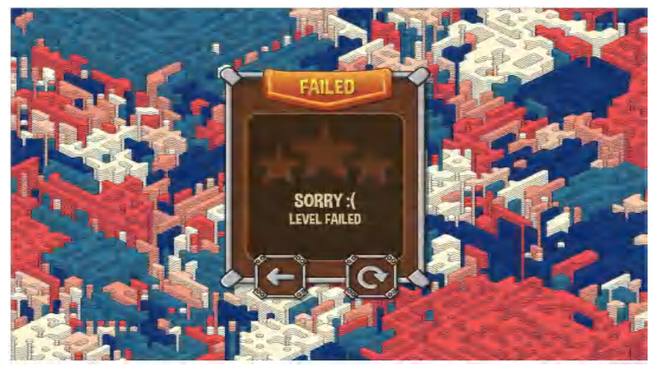
The game aims to educate players on the importance of privacy, data protection, and digital literacy, by placing players in different scenarios where they have to make decisions regarding their personal information, it will encourage them to reflect on their own online habits and practicesThe goal is to showcase the consequences of various actions taken by the player, highlighting the potential risks and benefits of sharing personal information. Familiarising themselves with common online threats and scams and understanding how to use privacy settings and other tools to better control their online experience.

Gameplay mechanics:
main narrative

Centred around exploration and decision-making, as the player navigates through different digital scenarios that require them to make choices about their online activities and data sharing practices. Each scenario presents the player with a set of choices, and the consequences of those choices are revealed as the player progresses through the game.
One of the key mechanics of the game is the use of chance events, which simulate the unpredictable nature of online privacy and security threats. These events can occur at any time, forcing the player to make quick decisions that can have significant consequences. For example, the player may receive a message from a friend in trouble, and must decide whether to share their location to help them. These events create a sense of tension and uncertainty, and add an element of risk to the game that encourages players to think carefully about their choices.
The game also features a branching narrative system, which means that the player's choices and actions throughout the game will have a significant impact on the outcome. This allows for multiple playthroughs with different endings, depending on the player's decisions. The branching narrative system encourages replayability and reflection on the player's own personal data sharing habits.





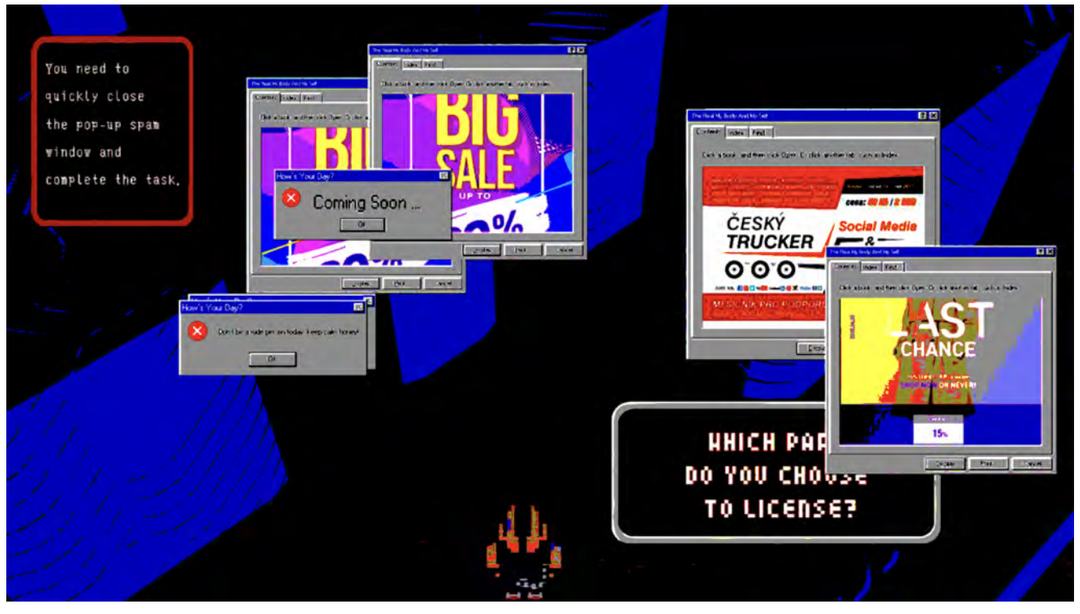


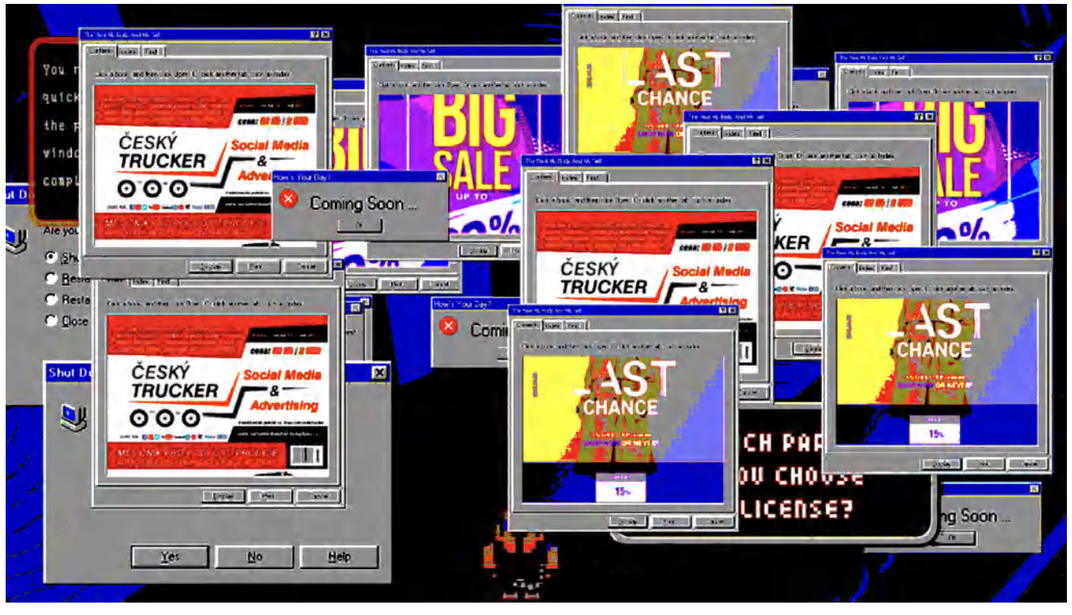
Possible endings

A positive ending: The player takes all the necessary precautions to protect their data, avoids risky behaviours, and successfully navigates through the maze, leading to a positive outcome where their data is secure, and they are not vulnerable to any potential privacy breaches.
A negative ending: The player makes poor decisions, does not take necessary precautions, and ends up being a victim of data theft or privacy breach, leading to negative consequences such as identity theft or financial loss.
An open-ended ending: The game may have an open-ended ending where the player is not explicitly told whether their data is secure or not, as some of their choices were possibly ambiguous (which many of the times is the case in real life) and the game ends with a message that encourages the player to play again and reconsider some of their choices.

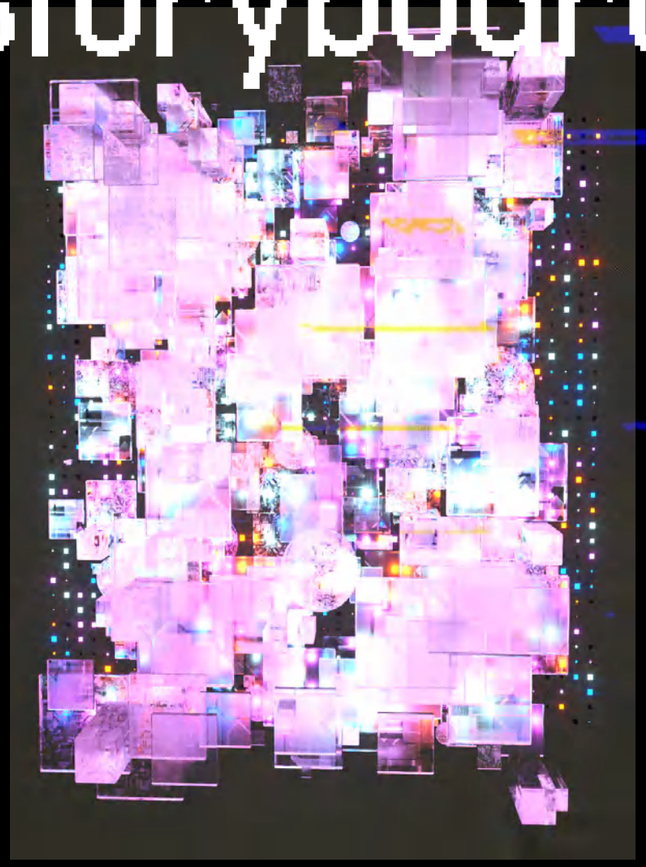
Game mechanics:
Mini games

Including mini games throughout the main narrative the game in order to better simulate navigating social media: multiple pop-ups and spam that ends up distracting a person from other important things like protecting their privacy online.
Tap to Close: players have to quickly tap on the X button to close multiple pop-up ads that appear on the screen. The ads could be designed to look like actual pop-up ads, and the game could get progressively more challenging with the ads appearing faster and in larger numbers.
Spam Filter: players have to sort through a sea of emails and identify which ones are spam and which ones are legitimate. The spam emails could be designed to look like the types of emails that are often sent to people, such as phishing emails or emails offering a free trial of a service.





Storyboard



The game is divided into several chapters, each representing a different aspect of the platform's data collection and privacy policies.

Possible sequence

Intro:

The player is introduced to the world of digital privacy and is tasked with navigating through a series of digital scenarios. The player is given a reminder that their digital footprint lasts forever and even small decisions can have big consequences.

Chapter 1: Setting Up Accounts

The player is asked to create an online account for a new social media app

The player must decide what information to include in their profile, such as their full name, email, and date of birth

The player must also decide whether to enable location tracking or not

A pop-up appears, asking the player if they want to connect the app to their other social media accounts. The player must weigh the benefits of connecting with friends and the potential consequences of sharing their information with the new app

Chapter 2: Responding to Requests

The player begins receiving friend requests and messages from people they don't know

The player is asked to provide personal information such as their phone number, home address, and bank details

The player must decide whether to respond or not and weigh the potential consequences of their actions

A random event occurs where the player's account is hacked and sensitive information is leaked

Chapter 3: Posting Content

The player is asked to post a picture or status update

The player must decide whether the content could be potentially harmful to their privacy, such as revealing their location, or sensitive information. The player must also consider who will have access to the content and the potential consequences of sharing it.

Chapter 4: Protecting Privacy

The player must decide whether to use privacy settings and enable two-factor authentication

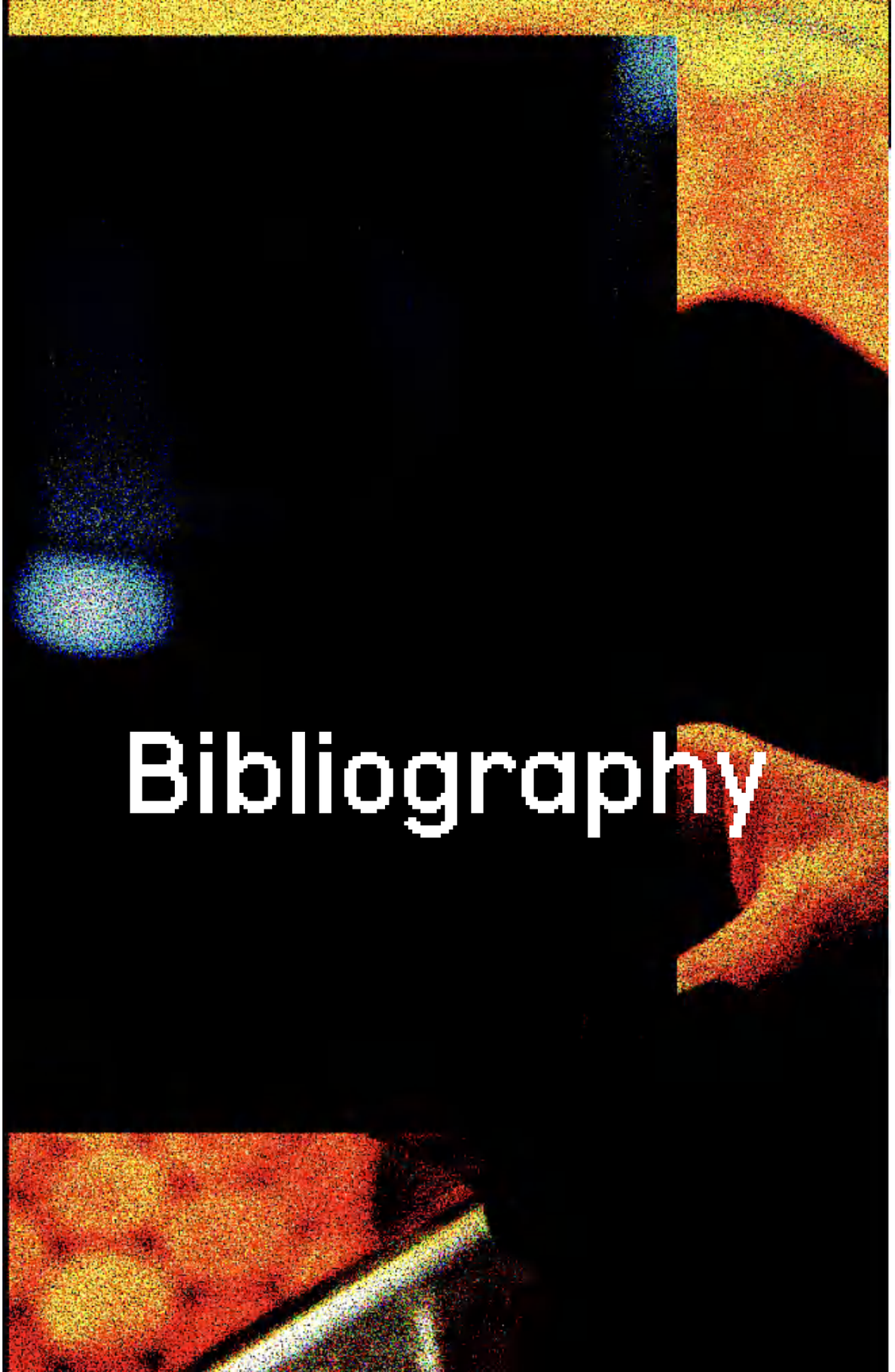
A random event occurs where the player receives a message from a friend who is in trouble and needs their help

The player must decide whether to share their location with their friend and weigh the potential consequences of their actions

Outro:

The player reflects on their choices throughout the game and is given tips on how to better protect their digital privacy

The player is reminded that their digital footprint lasts forever and must always be aware of their actions online



#

Calvillo Gamez, E. H., Gómez Romero, J., & Sánchez Fuentes, A. J. (2020). Modeling Instagram's Algorithm: The Power of Images and Colors. Journal of Interactive Advertising, 20(1), 19-29.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication

Gillespie, T. (2014). The relevance of algorithms. In Media technologies: Essays on communication, materiality, and society (pp. 167-194). MIT Press.

Gee, J. P. (2003). What video games have to teach us about learning and literacy. New York: Palgrave Macmillan.

Mittelstadt, B. D., & Floridi, L. (2016). The ethics of big data: Current and foreseeable issues in biomedical contexts. Science and Engineering Ethics, 22(2), 303-341.

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

Solove, D. J. (2013). Nothing to hide: The false tradeoff between privacy and security. Yale University Press.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power.(chapter one)