Fall 12-2022

Panopticon: A Privacy Revelation

Kexin Wang

Zhexu Yang

PANOPTICON
A Privacy Revelation

2023 Thesis Preparation Research Book
ARC 505
Syracuse Architecture
Students: Kexin Wang & Zhexu Yang
Instructors: Hannibal Newsom & Kiana Memaran Dadgar

pan

9:41

Panorama Pangaea Pancake Panacea

Panther Pantheon Pandora Panda

Abstract

Our thesis project studies and analyzes the control of Surveillance Capitalism over people's privacy, and how to make people realize the importance of privacy through the means of an architectural/design narrative. This concept comes from Shoshana Zuboff's The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, which explains how tech companies collect extra data, capture people's behavioral surplus and sell them to third party customers, such as advertising companies, thus the predictions about people's preferences accordingly. In this process, technology companies can make tremendous profit by stealing users' personal information and then selling it to third parties for advertising and prediction products. With the rapid development of technology, big data monitors and collects people's personal information and privacy indefinitely. In the traditional sense, privacy in buildings only needs physical walls to enclose the space. Now, thanks to big data, privacy is no longer subject to physical boundaries, location, etc. and the limitations of distance. This has become a growing and terrifying contemporary issue, but many people are not aware of its severity and privacy implications. Our thesis aims to design a narrative in which people's privacy has been completely deprived to the extreme in future cities in order to serve as an apocalypse, warning people of the data panopticon they are living in.

Contents

Chapter 01

pan

Pan inc. dedicates on a better future by assisting daily activities, making accurate predictions, and providing life changing suggestions and services. Pan inc. has developed a series of applications that use the data collected from the pan microchip implant to make life better.
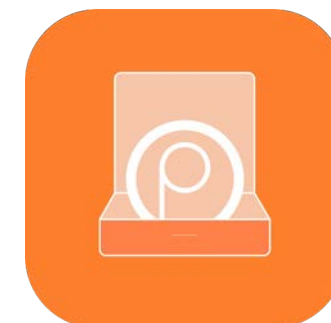

Panorama

Pangaea

Pancake

Panacea

Panther

Pantheon

Pandora

Panda

pan

TERMS AND USER AGREEMENT
or
"Just agree, no one cares about your privacy"

These terms and conditions create a contract between you, the User, and the Company (Pan, Inc.). Please read the terms of the Agreement carefully. To confirm your understanding and acceptance of the terms herein, click **Agree**.

1. INTRODUCTION TO OUR SERVICES

Thank you for trusting Pan, Inc. and choosing our services. We strive to make your future better! With our Pan Microchip Implant and Pan Apps, you can enjoy a lifelong predictive service and personal assistant that helps manage every detail of your daily life. This Agreement governs your use of the Company's services ("Services"), through which you can purchase, license, rent, subscribe, install, or implant content, apps ("Pan Apps"), microchips, and other services (collectively, "Content"). By using the Services, you are entering into a binding legal agreement with us, in which you agree to be subject to and bound by these Terms. Ok, this is long enough, you probably get tired reading this already. I mean, who even read these Agreements? It's not like you can do anything after reading this right? Yeah, you don't really have a choice, to be honest. We even find this document too boring to read, and it is too boring to write as well. Just scroll to the bottom and click agree. If you are unwilling or unable to be bound by these Terms, sure you can opt out anytime, but oh poor man, we will erase all your previous memories and identities that are connected to our microchip implant, and you won't be able to use these amazing apps that everyone in this world is using! Can you really afford being left out of this technological world? Come on, just, I mean, just stop reading already, click agree, easy peasy lemon squeezy.

2. USING OUR SERVICES

DATA POLICY

A. To use our service, you will need to join the Pan Microchip Implant Program. You agree that the implant will be connected to the cranial nerves and able to monitor and access the information you feel, touch, see, hear, smell, taste, and facial expressions and memories. Yes, this is really happening. This means through this little chip inside your brain, we are able to monitor and know everything about you. We know all your sense, how you feel, and even what you are thinking. Read on, if you are still reading, which I highly doubt, and you will discover more about how we use your data. It's fun.

B. You agree that your personal information is collected and uploaded to our drive through the Pan Microchip Implant. How else could we possibly obtain all of your personal information? Of course the little chip would send it back to our server and we can store it.

C. You agree that our designed algorithm turns the collected information into data and makes connections between them in order to predict preference and behavior. Not only do we know you, we also know your next moves! Sounds a little scary and insecure, but hey, think of it the good way. We plan things for you! You don't need to worry about your life anymore, what a relief! Let us take control.

D. You agree that the personal data collected by the Company belongs to us and becomes our legal property. Yes, you've read it right. It's our data. We reserve the right to use, modify, copy, share, display the data. Again, I've said it once and I'll say it again, there is nothing you can do. We can do anything we want with our data.

E. You own the intellectual property rights, copyright, trademark, of any content you share through the Apps, but you grant the Company a non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to do with your data whatever we wish. What do you think? You are sharing it! Doesn't matter who you are sharing to honestly, you are sharing with us ultimately.

F. Personal data collected includes identifications, credit card information, text messages, voices, activities, locations, habits, food intakes, health conditions, thoughts, memories, and many other things not listed in this document. Yeah, I know you probably don't care about what kind of information we collect, and I'm too lazy to list all of them. There's a whole range of them. And you know what, there is no way you've read this far. Well, if you do, let me tell you more.

G. You agree that we disclose your information for certain purposes and to third parties. How do you think we make money while providing you with this lifelong predictive service for free? We are not philanthropists. We will sell your information to others if profitable.

H. The third parties we cooperate with include government agencies, The FBI, The CIA, police departments, hospitals, health supplement providers and others. Remember that we know what you are thinking. If you are attempting to commit a crime, we will predict that and there is a chance that we report to the law enforcement, depending on whether we want or not.

I. There is no guarantee on the security of your personal information. As we stated above, we have the right to do whatever we want with your information. But if it is stolen or hacked, well, unfortunately there is nothing we can do, and we do not hold the responsibility.

J. You waive your right to bring or participate in any class, group, or representative action or proceeding. You can't sue us, ever, for any reason!

PAID FEATURES

A. You may be required to pay a certain amount of fee to utilize some built-in features of the Service. You expressly allow us or our payment procedure to charge the payment method you provide. You agree that all fees are non-refundable and will be proceeded by Pandora Pay. You really think we would give the money back to you once we have it?

B. We reserve the right to revoke or suspend your access to paid elements of the Company at any time and for any reason, without incurring any liability. If you choose to opt out from our service, you will not be entitled to a refund for any fees you paid to us for these features. Yes, it is really our products, our money, our everything. Imagine if you opt out from our services, you wouldn't be able to use Pandora Pay which everyone is using for paying. How are you going to buy things? No one uses cash anymore.

C. The Company may offer downloadable content, upgrade voice assistant, or any other virtual features which are issued by the Company in the future. Depending on the features, you may purchase or gift these virtue items in applications we offer, such as Pandora, Panda, Panther, Pantheon, Panorama, Pangaea, Pancake, and Panacea. For example, you may use Pandora Pay to purchase virtual games, skins, and other game features for Panda Metaverse Gaming System. By using these applications, you agree to accept the then-current purchase prices at the time you purchase. You understand that while you purchase, earn, gift, or receive virtual items, you do not legally own them. We may modify, suspend, eliminate, or substitute virtual items at any time and in our sole discretion. Even if you choose to terminate our service, you are not permitted to a refund.

3. TERMINATION OF SERVICE

You have the absolute right to opt out of the Pan Microchip Implant Program at any time. When you decide to opt out, you will contact our Erasure Department by emailing *erasure@pan.com* to make an appointment or visit any Pan Store to make your request. We are happy to assist you. By opting out of the Pan Microchip Implant Program, you forfeit your right to any of your previous memories. Your personal identification and history will be permanently erased along with the removal of the implant from your brain. We preserve the right to retain your personal information previously uploaded by the microchip implant in our data center. I'd be surprised if you actually read this far. Anyways, we do not care if you want to stop using our Apps and the little chip that tracks you. We only care about your data and the profit it brings. And guess what, if you choose to opt out, you don't get to keep a single bit of your information. I know it is hard starting your life all over again and finding out you don't even fit into this society that's entirely technologically driven. So why bother? Just sit back, relax, and accept our service.

4. CHANGES TO THE AGREEMENT

We may update our Agreement from time to time. We will not notify you of any changes and just update and post it on our website. By continuing to use the Services after such posting you agree to any changes. In our sole discretion, we may edit, discontinue, or alter any aspect of the Pan. This may include but is not limited to (i) alternating any feature or functionality provided by the Pan, (ii) removing or modifying content, (iii) restricting access to parts or all of the Pan. Yes, yes, yes, that's right. We can change this Agreement how ever we want and there is absolutely nothing you can do. And we don't even have to tell you. Once you click agree, it is all done, no need to worry about anything. Let the professionals handle the business here my dear users. And I bet you won't even read this last sentence. You just scrolled down to the very bottom right?
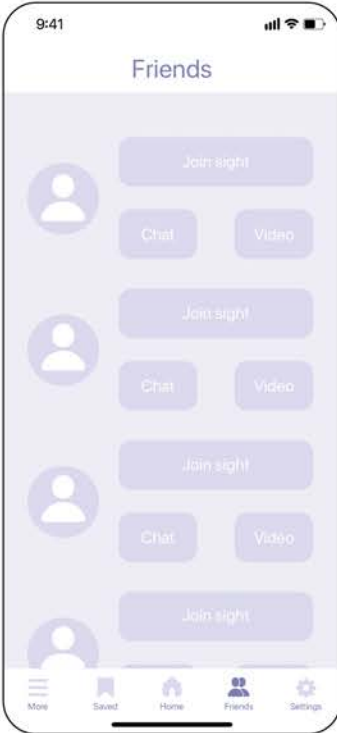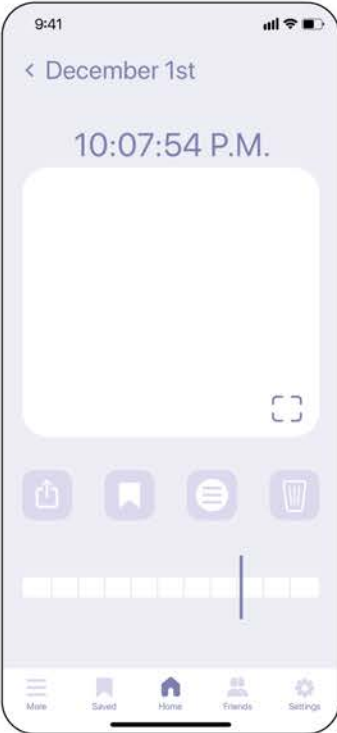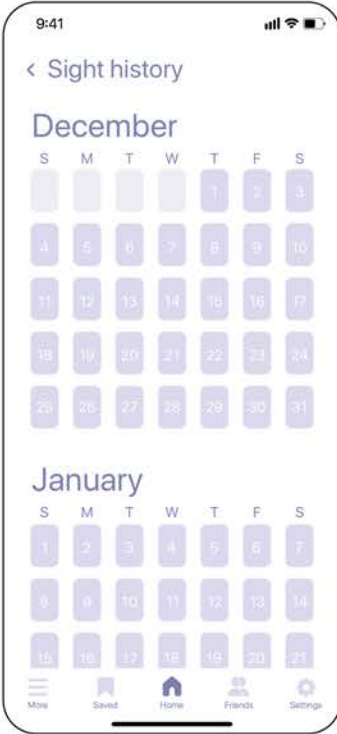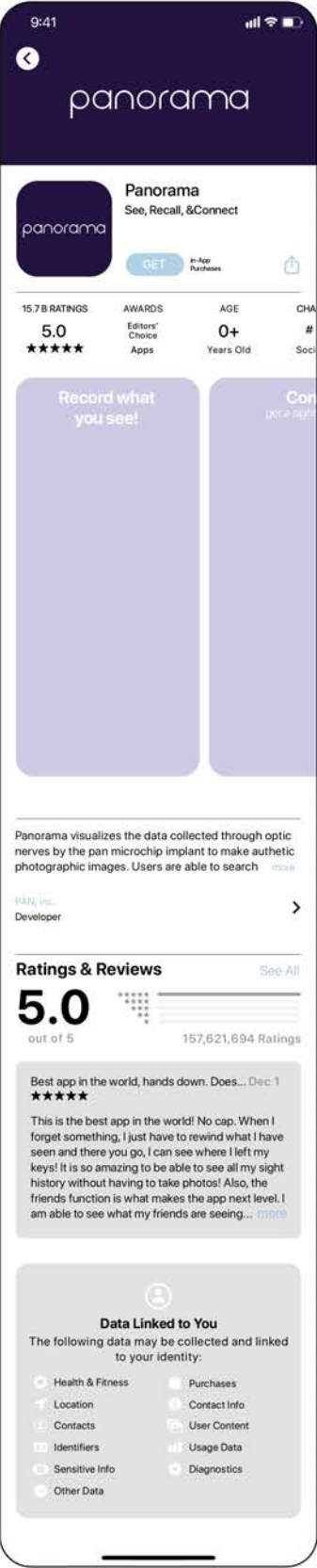
Agree

Panorama

See, Recall, and Connect

Panorama visualizes the data collected through optic nerves by the pan microchip implant to make authentic photographic images. Users are able to search back in time to pin point an imagery captured by the optic nerve system at a specific moment. Users are able to share their images and chat with friends through Panorama.
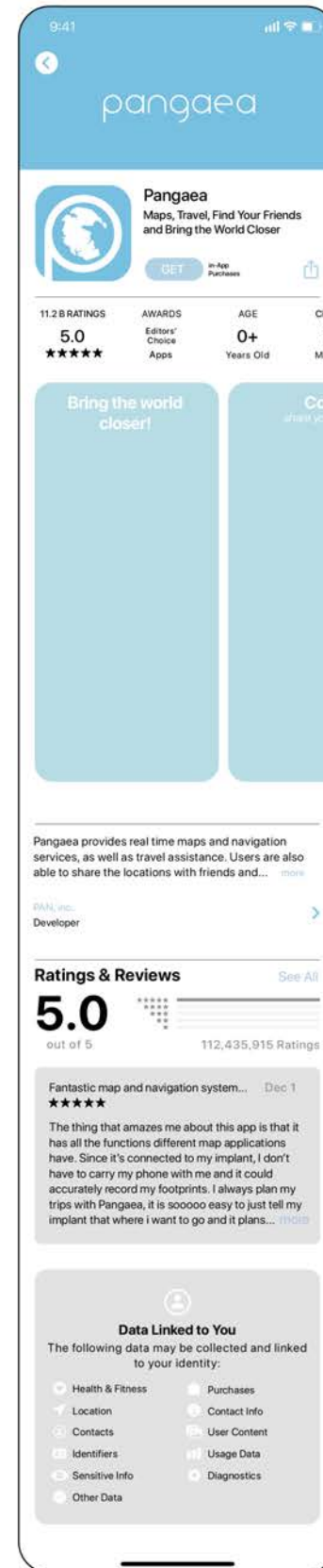
Pangaea

Maps, Travel, Find Your Friends
and Bring the World Closer

Pangaea provides real time maps and navigation services, as well as travel assistance.
Users are also able to share the locations with friends and discover any wonders in any
location in Planet Earth.

Pancake

Food, Recipe, Delivery, and Your Personal Food Expert

Pancake analyzes the data collected through Glossopharyngeal nerves and Olfactory nerves by the pan microchip implant to provide personalized food suggestions and recipes. With Pancake, users are able to order food delivery, customize their meal plans, and receive an accurate food report.
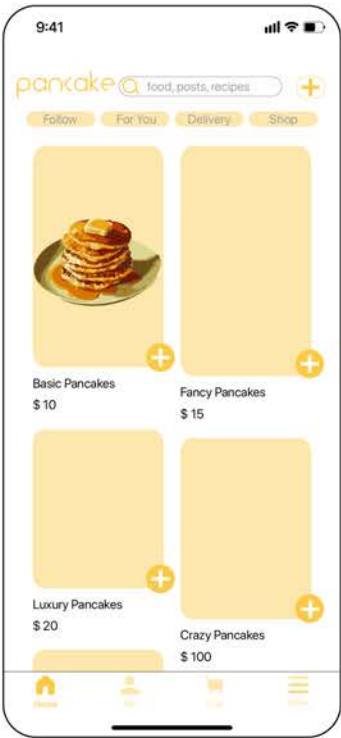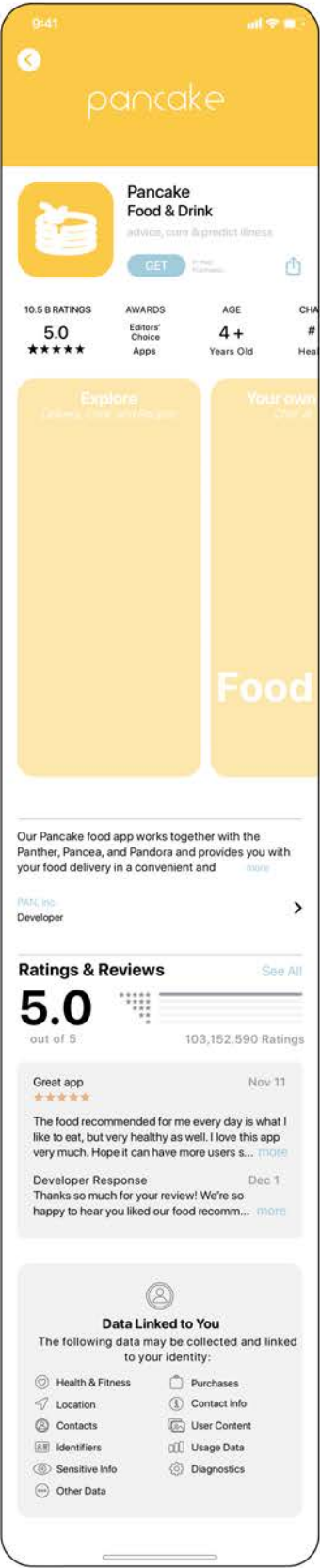
Panacea

Health Analysis, Prediction, and Cure

Panacea monitors and analyzes the data collected through cranial nerves and the user's body by the pan microchip implant to make health predictions. Panacea also provides advices, cure, and treatment to predicted and existing illness, diseases, or accidents.
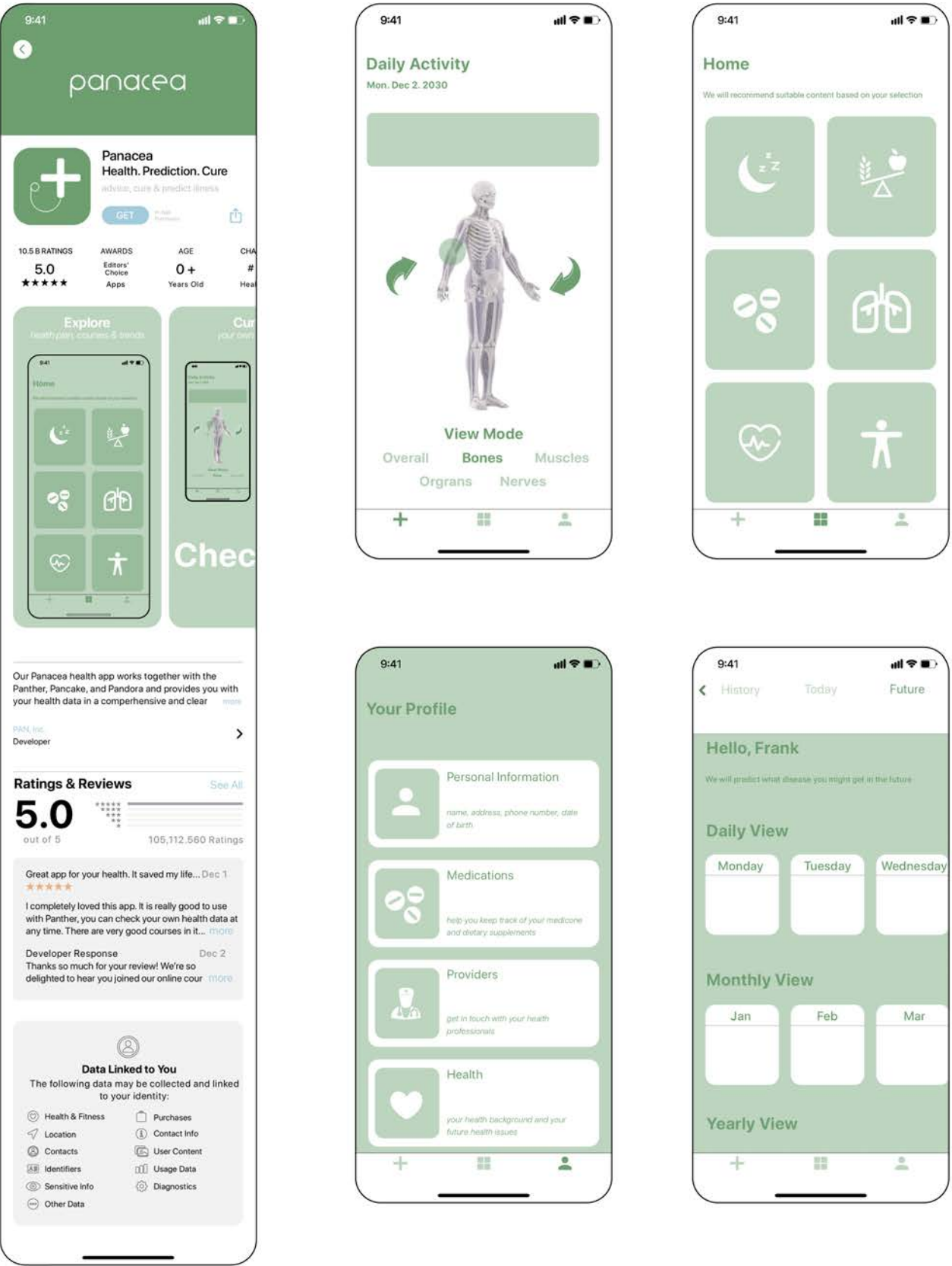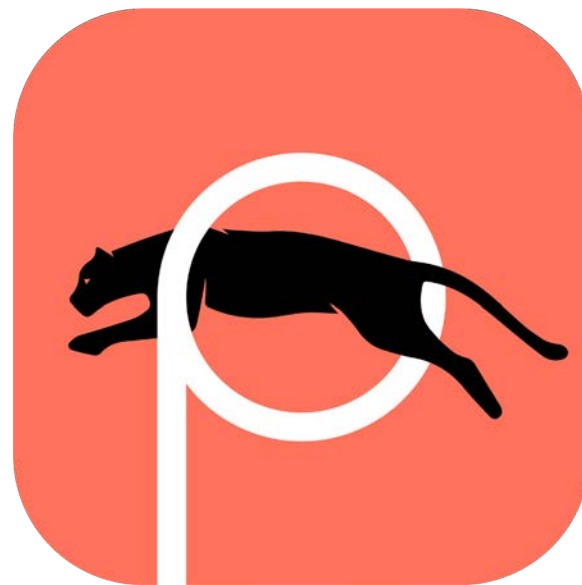
Panther

Sports and Activity Tracker

Panther tracks and analyzes data from users' sporting habits and body conditions when doing sports. Users are able to create a personalized sporting agenda and workout with friends. Panther also provides sporting analysis, suggestions, and load management to users.
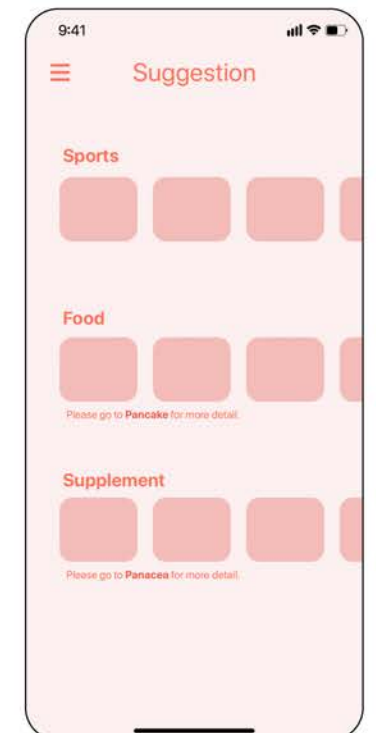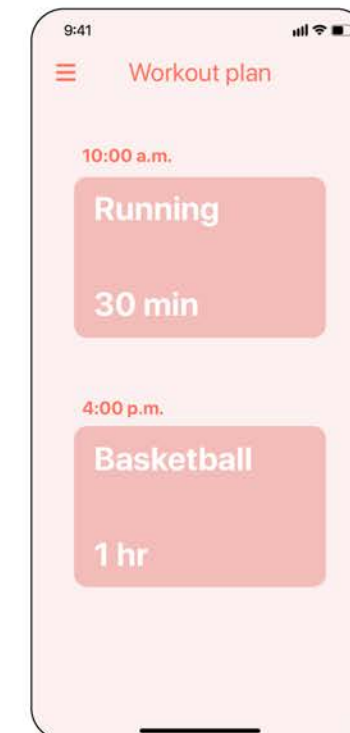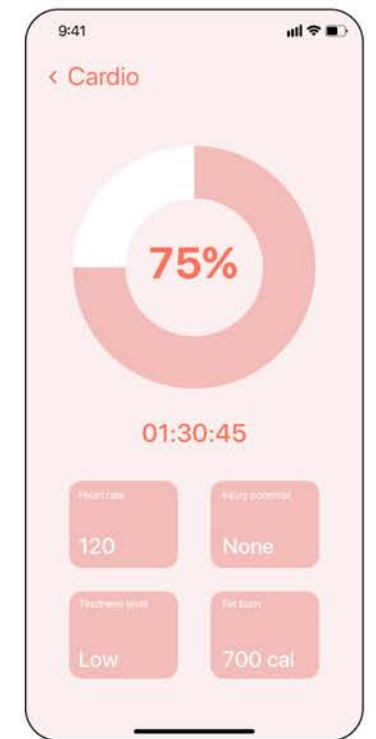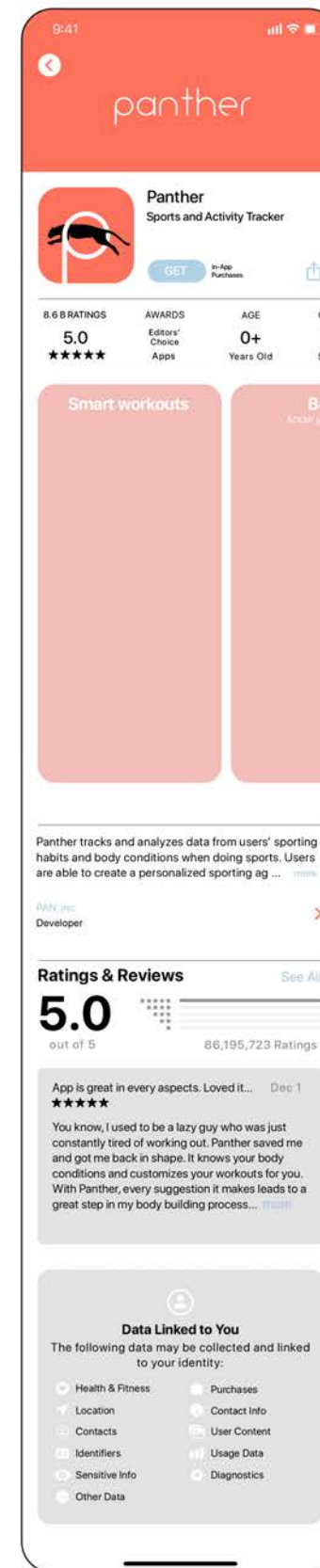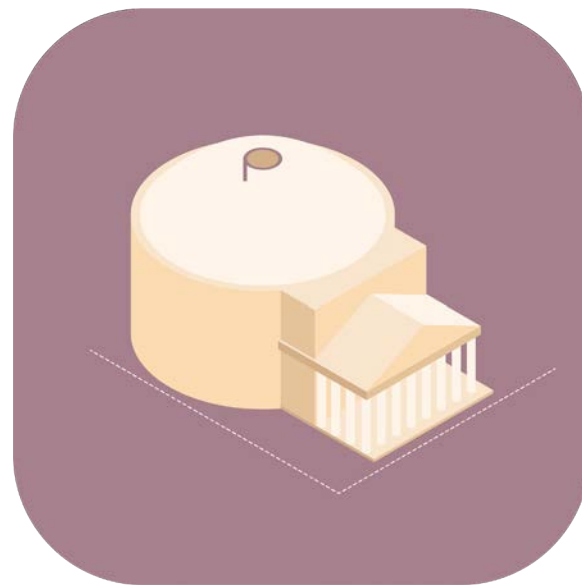
Pantheon

Envision a New 3D Modeling by Thoughts

Pantheon is a revolutionary 3D modeling application. With Pantheon, users are able to model 3D objects simply with a thought in their brain. The pan microchip implant will capture the thoughts and encode the data into 3D objects via artificial intelligence.
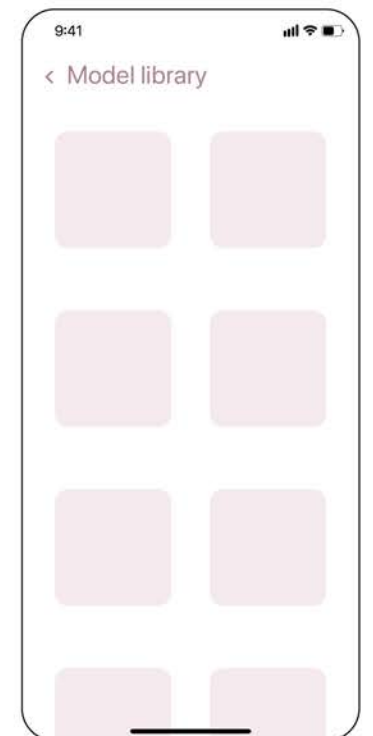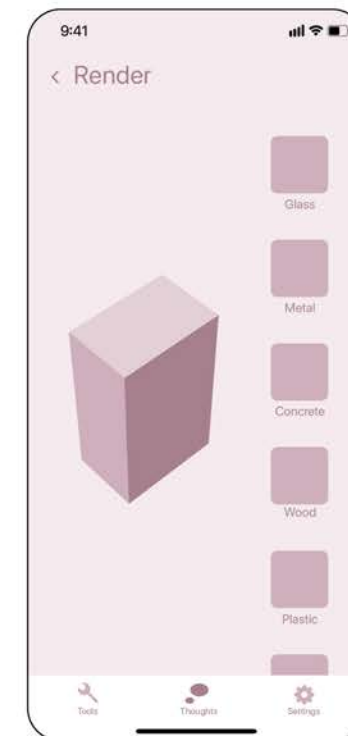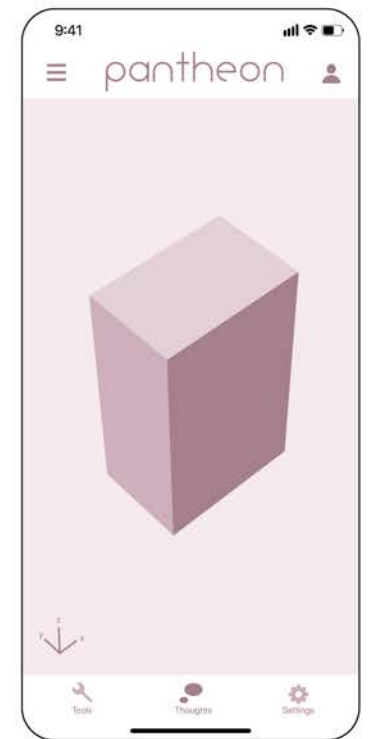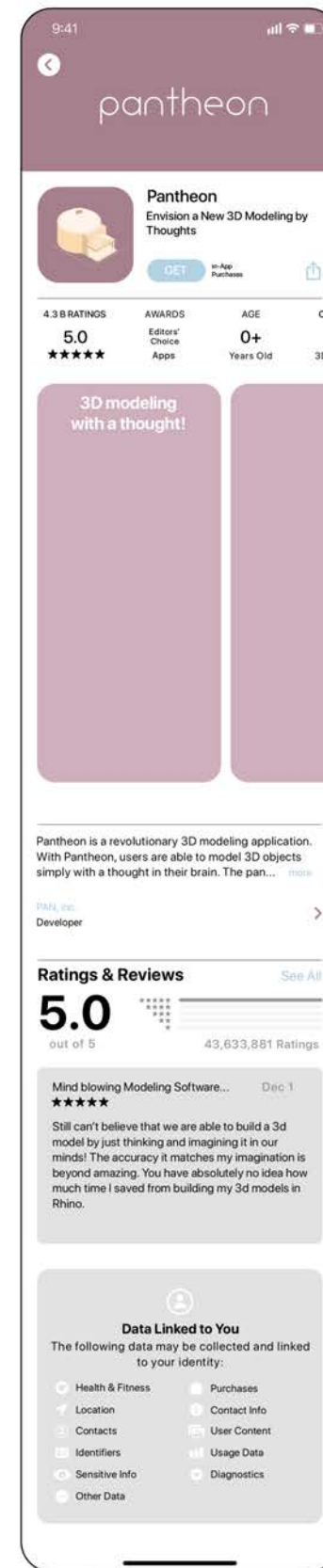
Pandora

Shopping, Banking, and Your
Personal Wallet

Pandora is an online shopping and banking application that allows users to save and
spend their money with a few clicks. Users are able to make payments with Pandora
Pay.
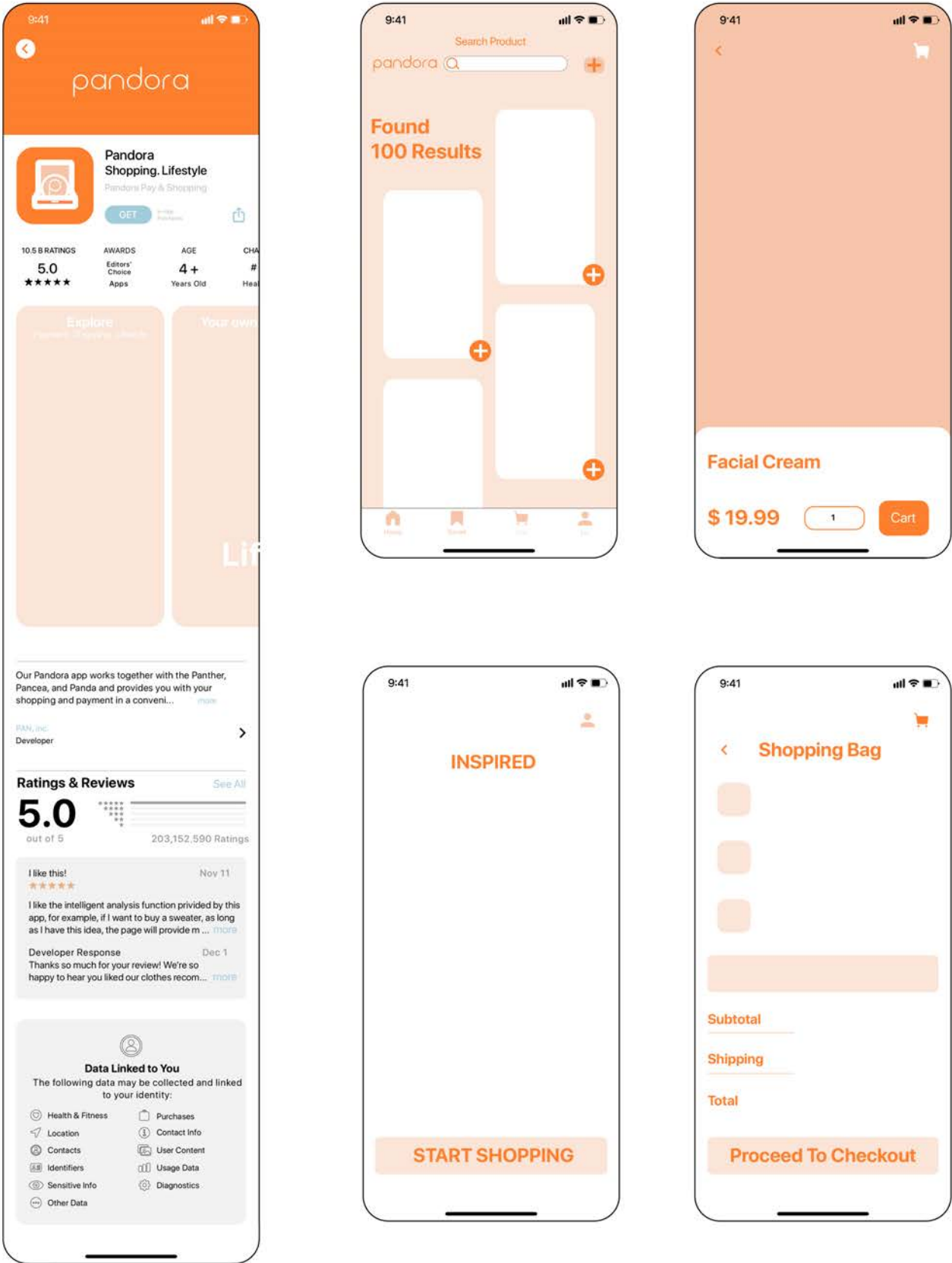
Panda

Metaverse Gaming System

Panda is a metaverse gaming platform allowing users to log into a virtual world to explore countless possibilities. When users are in Panda, the microchip implant will temporarily pause the movement of the physical body and manipulate the cranial nerves of the users thus their senses. Users are able to experience the virtual world with real senses.
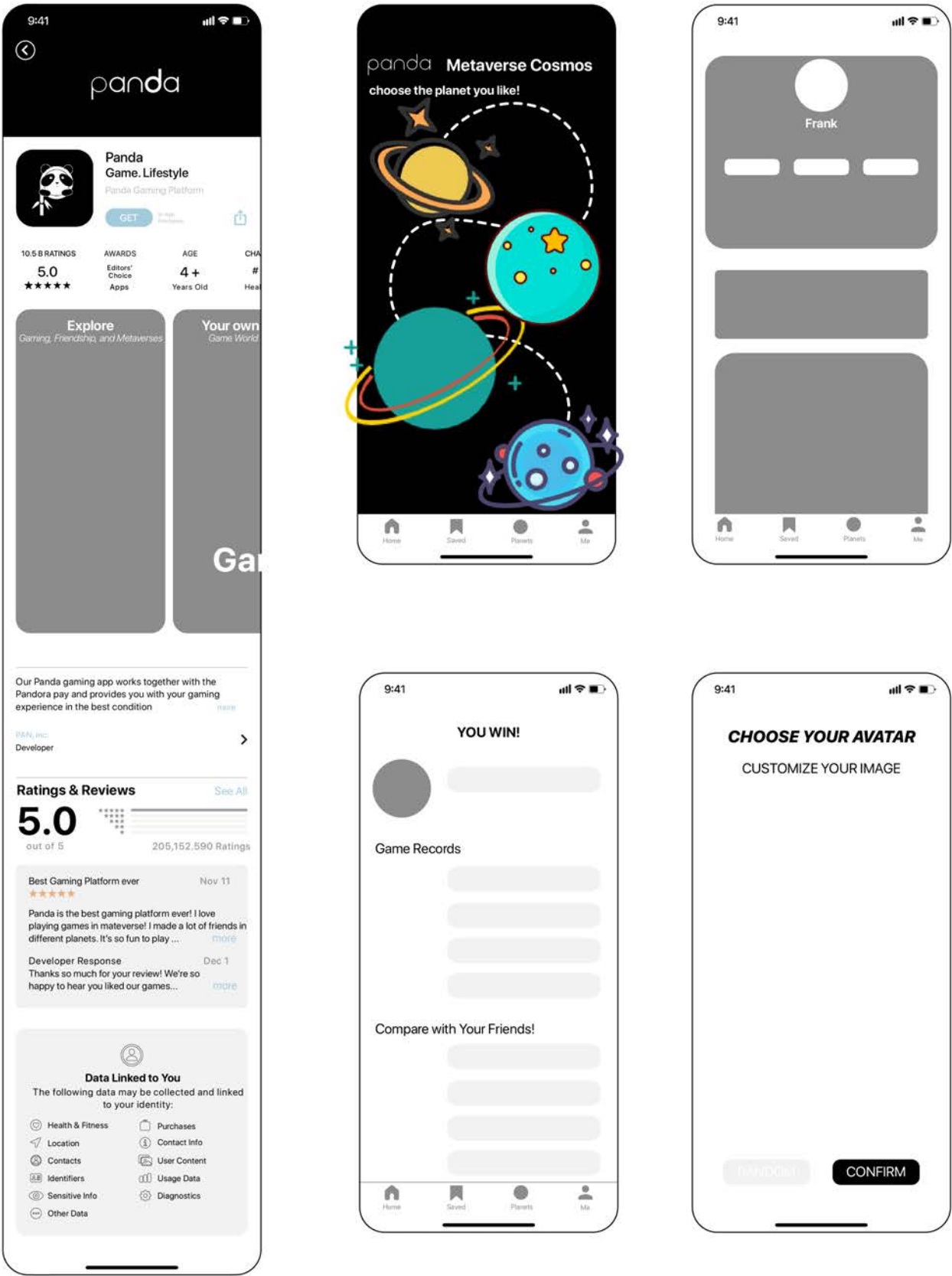
Chapter 02

BACKGROUND

This chapter consists of the background research which the development of the Pan company and apps is based on.

Panopticon
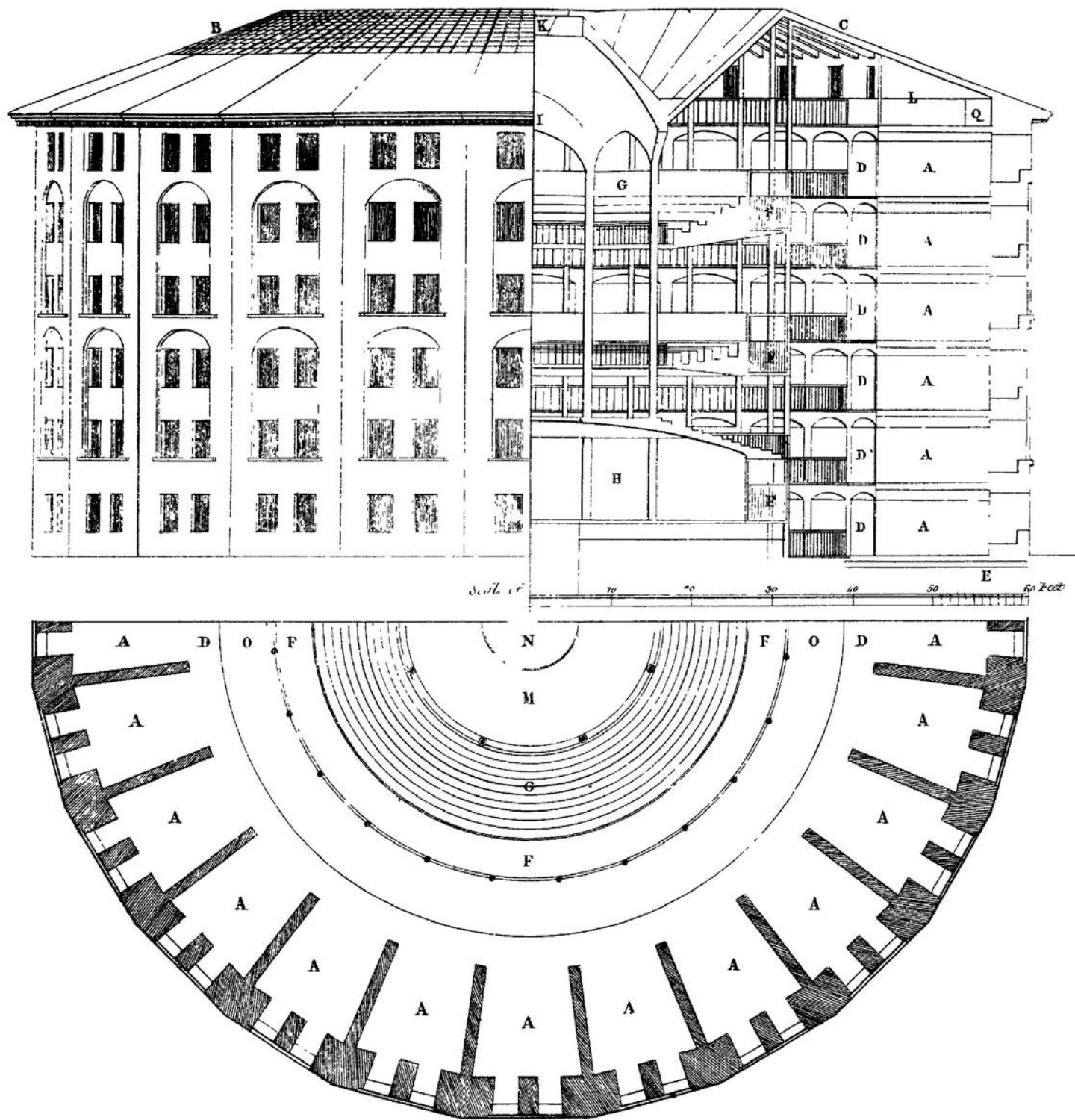
Plan of Jeremy Bentham's panopticon prison, drawn by Willey Reveley in 1791

The idea of panopticon was first introduced by English philosopher and social theorist Jeremy Bentham in 1785. It is a circular prison with cells arranged around a central watch tower, from which prisoners could be observed and surveilled at all times. The existence of the central watch tower gives the prisoners a conscious effect that they are being constantly surveilled even when there is actually no one actively watching. Bentham imagined it to be a way of social control as this type of surveillance requires fewer guards as possible to control and regulate a maximum number of prisoners.

This idea was further elaborated and discussed by French philosopher Michel Foucault as a power structure in a disciplinary society in Discipline & Punish: The Birth of the Prison. According to Foucault, "panopticism" becomes a symbol that extents beyond the realm of prisons. It has become a social power structure in which "the conscious and permanent visibility assure the automatic functioning of power". People in the society are disciplined by this power structure to behave. We do not have to know when the authority is monitoring, neither do we know from where they are watching. One thing we do know is that there is this collective rule set up by the authority and someone will be watching. The surveillance process becomes automatic which leaves people no choice but to fear the punishment and obey the rules.

The effect of this power structure has become a social norm and can be seen in many everyday life aspects. For example, a student might behave very differently in school versus outside of school. Even when there are no teachers present, if a student is physically in a school campus, he or she tends to obey the school rules because the power structure suggests that the school authorities will be watching and regulating behaviors. The surveillance and discipline effect makes the student fear the punishment of not behaving, demonstrating a sociological and psychological value the notion of panopticon projects on society. Same situation can also be found in traffic lighting. The understanding that there might be police somewhere watching prevents drivers from running a red light even if there is no police car around. The fear of punishment and the sense of being constantly surveilled again show a powerful control ability towards people.

In today's digital world, data surveillance has become the biggest panopticon as there is countless information about everyone's personal data in online databases, and the authorities are hiding behind screens and constantly monitoring people's behaviors and information. In this online world, it is much easier to monitor people without them knowing when and where. The relationship between users of certain technologies, whether it is a smartphone, a computer, or apps, and the technology companies is just like what is described in the idea of "panopticism". In this data panopticon, the users are the prisoners, and the tech companies are the watchmen/authority. The slight difference is that this instrumental power structure shifts a little bit away from the purpose of discipline and punishment, but rather towards the idea of gaining maximized profit. Such an idea is theorized by Shoshana Zuboff as Surveillance Capitalism, which will be explained in this next section.
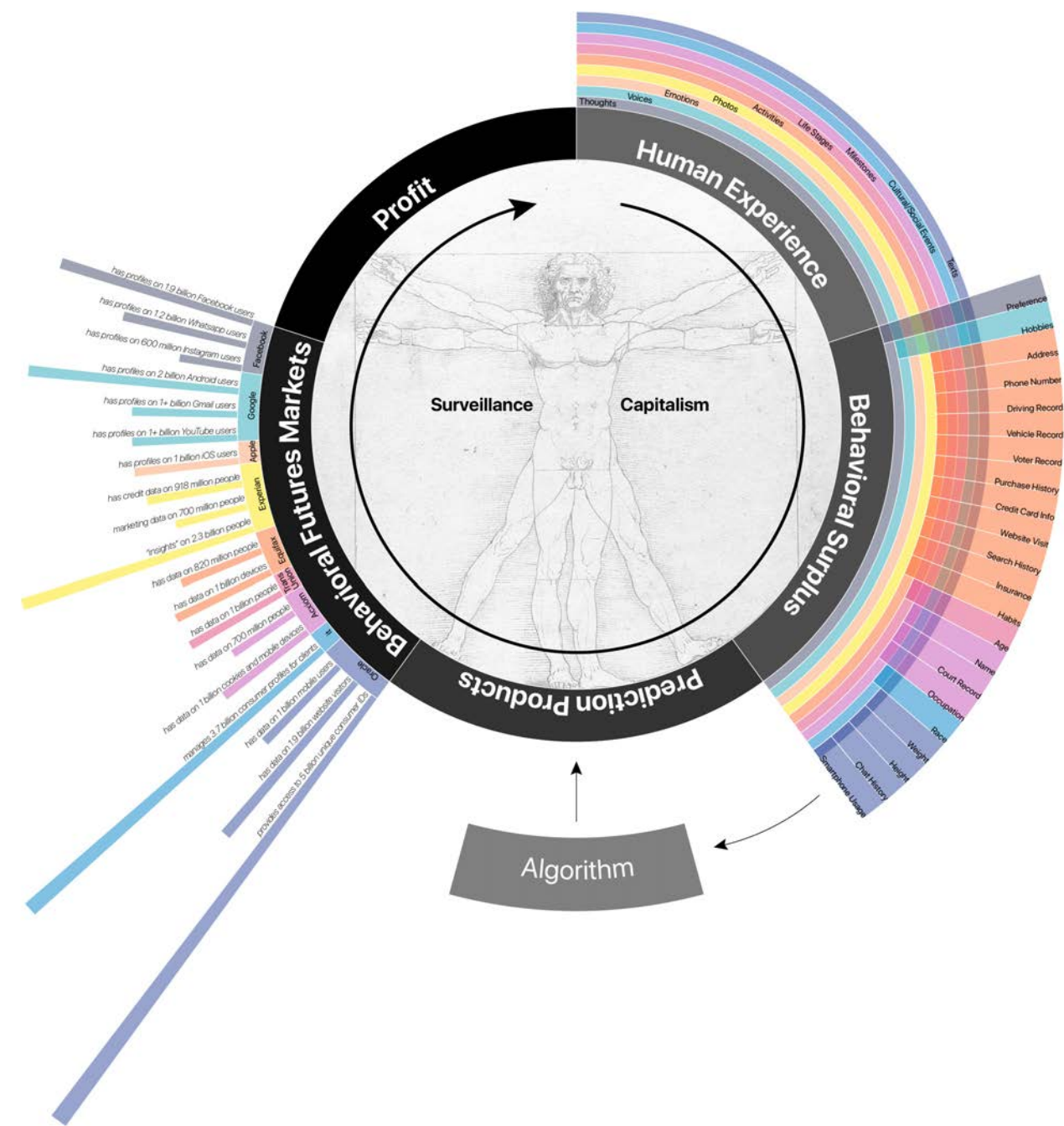
Surveillance Capitalism/Economy

Image by author

The idea of Surveillance Capitalism is introduced by Shoshana Zuboff in her book The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Zuboff argues that it is a new economic order in which technology companies and corporations collect a huge amount of data containing personal information from the users' behavioral surplus to make profit. Zuboff specifically listed Google and Facebook as two main tech companies that started Surveillance Capitalism. At the beginning, Google and Facebook were only using their collected data to improve services and products. However, in the process, they discovered there is an enormous amount of data surplus that they do not need for improvement but can turn into profit. The users are not real customers, as many apps, products, services are provided for free. The real profit-making process hides behind the selling of personal information to third parties such as advertising companies, so that they can precisely predict and target consumers by studying and analyzing their behaviors and preferences. In this case, the third parties are the real consumers that surveillance capitalists make profit out of, which opens up a huge market for behavioral surplus and personal data.

As we go through our everyday life, our human experience can be monitored, collected, and turned into data. These experiences include thought, voices, emotions, photos, activities, life stages, milestones, events, texts, and etc. From these experiences, companies extract information as our behavioral surplus such as preference, hobbies, address, name, age, gender, credit card info, search history, and so on. This information makes the companies able to profile every person and in behavioral futures markets, companies have obtained countless profiles.

This process of Surveillance Capitalism is a loop or can be described as a snowball effect that users tend to fall for the prediction services and products as these are specifically and precisely targeted for the individuals, and after they get more services and products, more of their personal data and information will be collected to study. These actions will repeat themselves over and over, which not only gives the tech companies more profit, but also grants them more power which makes the power structure shift from the state towards technology capitalists.

Zuboff argues that in this process, notions of freedom, democracy, and privacy are highly threatened. As users, we do not have any power but to fall under the manipulation of surveillance capitalists. For example, prior to using the service, users have to sign the user agreement. But do we really read the whole document before clicking agree? Companies have the power to shape the agreement however they want and can update the agreement without having to tell the users. Many people think there are certain laws that protect out online privacy, but the reality is far more frightening because they know everything about you, and it is only a matter of how much you know that they know everything about you.

Privacy Paradox

What we say

Privacy concerns

Opt-out

fear of missing out

not a big deal

Paradox

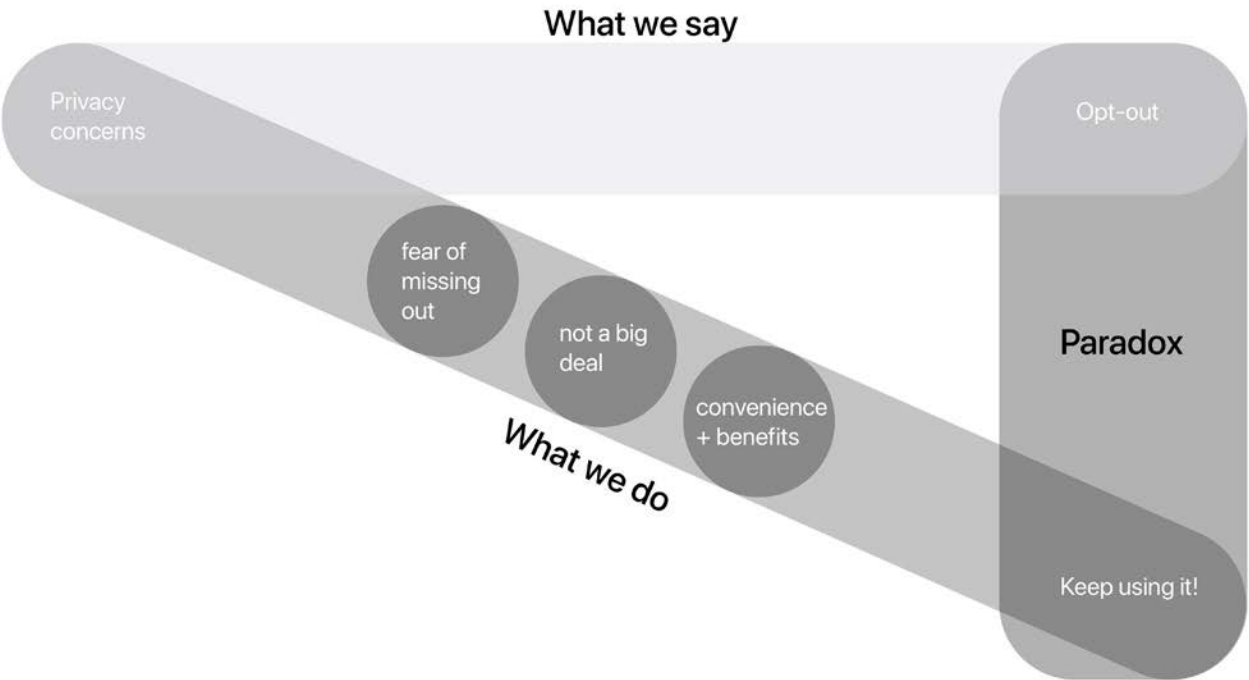convenience + benefits

What we do

Keep using it!

Image by author

Many people state that they are concerned about their online privacy, but their actual behavior says otherwise. In an ideal situation, if a person says they are concerned about their privacy, the best thing to do is to simply opt out of that program and stop using it. However, in a world where cellphones, apps, social media, and other programs are heavily relied on, who can really afford opting out? Technology has made everyday life so much more convenient and certainly brings many benefits to our society. People seem to care more about and really enjoy the convenience and fear that they would miss out from their friends and others. Therefore, they would ignore the privacy concerns and keep on using them. This creates a paradox between what people say about their concerns of privacy and what they actually do to stay in this digital world.

This privacy paradox is also utilized by tech companies as a means of control and manipulation. Tech companies understand the fear of missing out, and they will advertise the benefits of using their services and products to stay in touch with friends, news, and others while also exaggerating the disadvantages of not using them.

The use of WeChat is an example of privacy paradox. As the number one messaging and social media app in China, WeChat has 1.24 billion users, almost all in China. In other words, almost every Chinese uses WeChat to communicate, post, and see what their friends post. However, many people have experienced a lock of account if they express or post some political sensitive words/phrases/events on WeChat. People know that WeChat is constantly monitoring and censoring the content they communicate with each other, but they continue to use it because almost all people from China use it. If a Chinese does not use WeChat, it is really hard to communicate with their friends, classmates, colleagues, or even bosses in a timely manner. Therefore, people choose to ignore the fact that WeChat spies on their personal information and keep using it.

Personal Boundary

Image by author
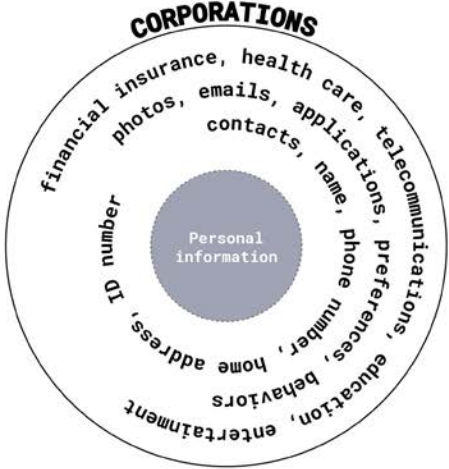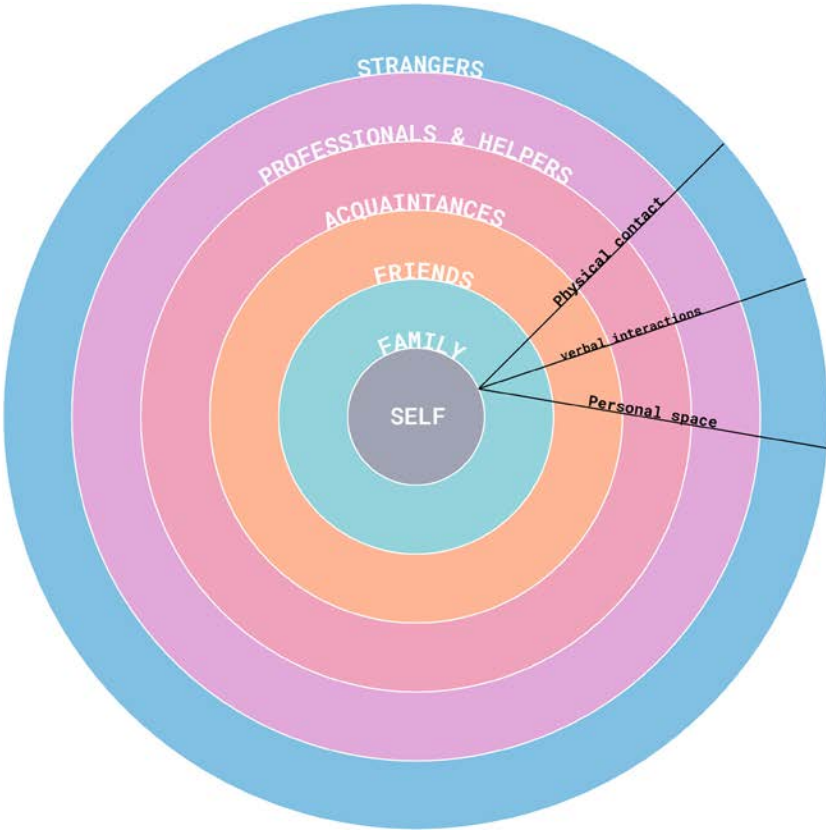
Personal Boundaries both exist in the physical and online world. Our information is all being collected while we are using the services that each platform offers us. These data changed our personal boundaries. It brings a lot of convenience to us, but on the other hand, the massive amount of information released or stored is also easily monitored and stolen by corporations. Therefore, setting up personal boundaries gets even harder when we are in the digital world. This section will approach the question and discuss the differences in personal boundaries between the physical and online world, what changes our personal boundaries in the physical and digital world, and why our privacy in the digital age is important.

Personal Boundaries in Real Life

Personal Boundaries are important for human beings and are closely related to their mental health. Normally, personal boundaries divide human relationships into categories, such as self, family, friends, acquaintances, professionals/helpers, and strangers. Each of these categories defines the rules that separate us from the outside world, ensure that we are not violated by others as an independent individual, and keep social comfort distance from others. If a person has a clear sense of boundaries, he can maintain stable interpersonal relationships, and he is aware of the sense of boundaries between people and respects them. However, if a person's sense of boundaries is vague, it will be very painful to face the boundaries established by others, and even unintentionally impose one's wishes on others, and at the same time destroy the boundaries of others. For example, in some parent-child relationships, the parent is supposed to be the closest relative to the child as they grow up. However, some parents unintentionally interfere with their children's privacy too much, which is to break their children's personal boundaries.

Digital Identity

Digital and social media provide infinite opportunities for presenting and understanding who we are. We can create our own profiles online, but we cannot be completely separated from reality. Facebook posts, Snapchat, tweets, comments, likes, and many other ways of expressing ourselves online provide opportunities for conveying our own stories and those of others. In this way, it functions as a mirror, reflecting oneself and others on what one is thinking and their narratives. It is easy to trace a person's living experience, habits, and living environment based on what they posted, bought and shared online. This greatly increases the possibility of privacy exposure. For example, if I ordered something from Amazon, they would ask me to fill out my address, phone number, credit card information, and email address. Living in an era of information explosion, the technologies that we rely on to make our lives easier and more convenient can be a way to expose our privacy. Unless we opt out of any technologies.

Digital Boundaries

Boundaries are frequently viewed as points of demarcation or separation, whether they are defined in interpersonal relationships between people or as borders between nations on a world map that represent territorial boundaries that are occasionally reinforced by physical boundaries like checkpoints or passport control. Digital boundaries are harder to define than spatial boundaries that can be set up in our physical world. The blurring and fusion of boundaries caused by digital and social media technologies have increased, and the confluence of connections, content, interaction and context presents both substantial potential and difficulties for people, society, and safety.

Profit

Users' information is all being collected while they are using the services that each platform offers them. These data changed their personal boundaries in the real world and led to an ambiguous online world where the boundaries are not easy to be defined. It brings a lot of convenience to users, but on the other hand, the massive amounts of information released or stored are also easily monitored and stolen by others. They profit by selling our information to third-party companies without our knowledge. For example, people's mailboxes are often filled with various advertisements, and browsing history is collected by search engines. As long as the user browses a category of products in the first half of an hour, the browser will target the specific keyword and browse the most related products.
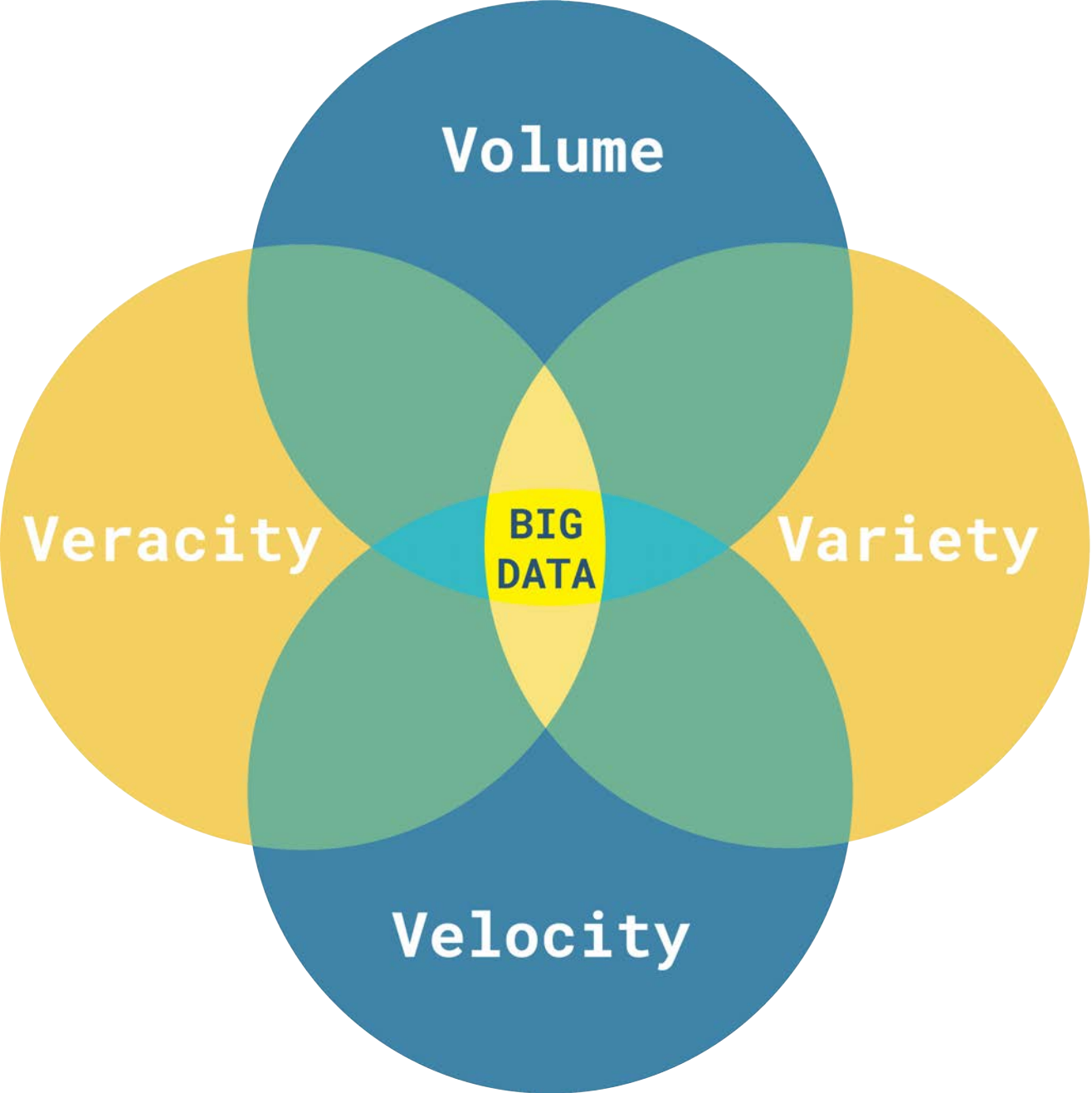
Big Data

Volume

Veracity

Variety

Velocity

BIG DATA

Image by author

According to Bridget Botelho's definition of big data, big data is a collection of "structured, semi-structured, and unstructured data" that is gathered by businesses and may be mined for information for use in advanced analytics applications like machine learning and predictive modeling. The three characteristics, volume, variety, and velocity were first introduced by Doug Laney in 2001. Veracity, value, and variability are also added to the characteristics of big data recently.

In the era of big data, the notion of digital capitalism and an antagonism emerged between networked digital productive forces and class relations. Christian Fuchs in his article, Karl Marx in the Age of Big Data Capitalism, mentions that networked digital technologies generate new kinds of commodification and exploitation, as well as new accumulation concerns. However, as a commodity, digital information possesses characteristics that make it resistant to commodification. Moreover, a political manipulation system has been established based on this social background. This political system suggests that surveillance technologies will be used to prevent and identify crime and terrorism, which would be beneficial to our society.
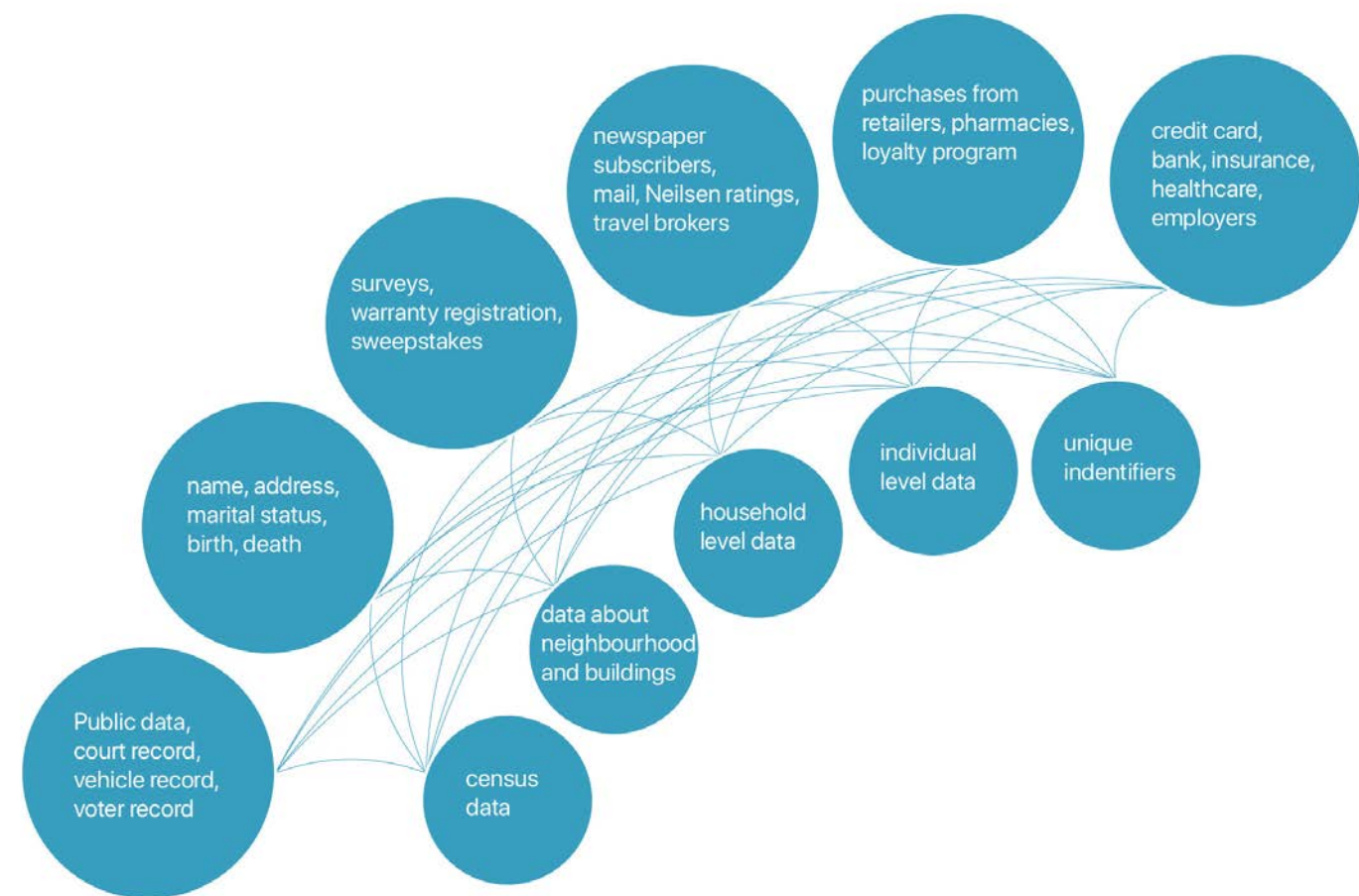
Using these data and technologies, big data companies can actually make marketing pervasive. Under the power of Big Data capitalism, humans are the targets of advertisements and being put into the trap of consumerism. Algorithms can automate human actions and decision-making to satisfy needs by using instrumental logic to calculate them. It seems beneficial to our life, but this process lacks morals and ethics, and it needs very strict supervision and laws to regulate it.

For example, using information leaked by users from public unprotected Wi-Fi, a restaurant in a shopping mall can deliver discount information to users who have recently visited the mall, and choose messages or social media as the delivery channel according to the situation.

In addition to user information being collected without users' knowledge, they have very little choice over how to control their information. Besides the option to opt-in or opt out, users only have very limited control over the types of data that may be collected. Users have to agree to the terms and conditions that social media companies offer in order to use their services. Opting out of these social media also means opting out of the social network and social benefits they provide. Opting out of search engines and social media would have a strong impact on people's lives, such as lower information retrieval and social life.

History of Surveillance

surveys, warranty registration, sweepstakes

newspaper subscribers, mail, Neilsen ratings, travel brokers

purchases from retailers, pharmacies, loyalty program

credit card, bank, insurance, healthcare, employers

name, address, marital status, birth, death

household level data

individual level data

unique indentifiers

data about neighbourhood and buildings

Public data, court record, vehicle record, voter record

census data

1700s
Panopticon

1860s
Telegraph
D.C.Williams, a stock broker, listened in on corporate telegraph lines and sold the information he overheard to stock traders.

1930s
Telegraph
Corporate management use wiretapping to root out labor unions activity.

1940s
Security cameras
The earliest CCTV CAMERAS are produced by American company Vericon, they still couldn't record and required constant monitoring.

1920s
Telephone

1925
Panopticon
Round Cellhouse, Stateville Correctional Center, Crest Hill

1950s
Security cameras
the videotape recorder (VTR) was invented

Surveillance started long before the emergence of technologies. With the development of technology, the means of surveilling people are constantly upgrading, from a visible version, such as panopticon, telegraphs, telephones, and security cameras, to an invisible version, such as Nielsen TV ratings, credit cards, and website history. Edward Snowden made public the existence of a system for monitoring and analyzing communication flows in real-time used by secret agencies around the world. Companies including AOL, Apple, Facebook, Google/YouTube, Microsoft, Paltalk, Skype/Microsoft, and Yahoo! are among those involved in this surveillance apparatus. The public witnessed executive branch abuses of wiretapping, and it has increased once more as a result of Edward Snowden's revelations concerning the National Security Agency. It's important to understand, however, that justified wiretaps are now nearly always used for criminal rather than national security investigations.
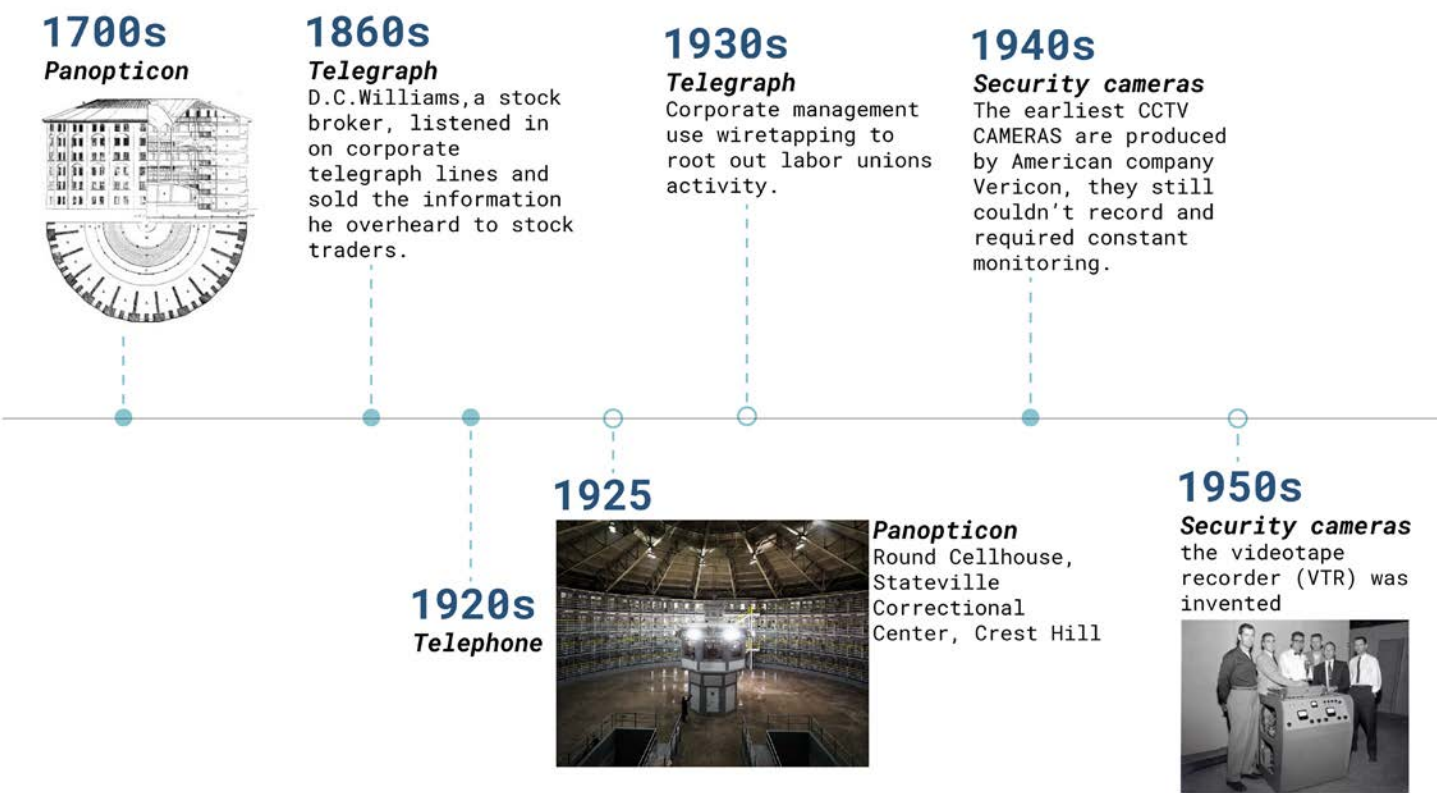
The idea of surveillance in eighteenth century begins with the panopticon that introduced by Jeremy Bentham in 1785. The Panopticon is a circular prison with cells arranged around a central watch tower from which inmates wil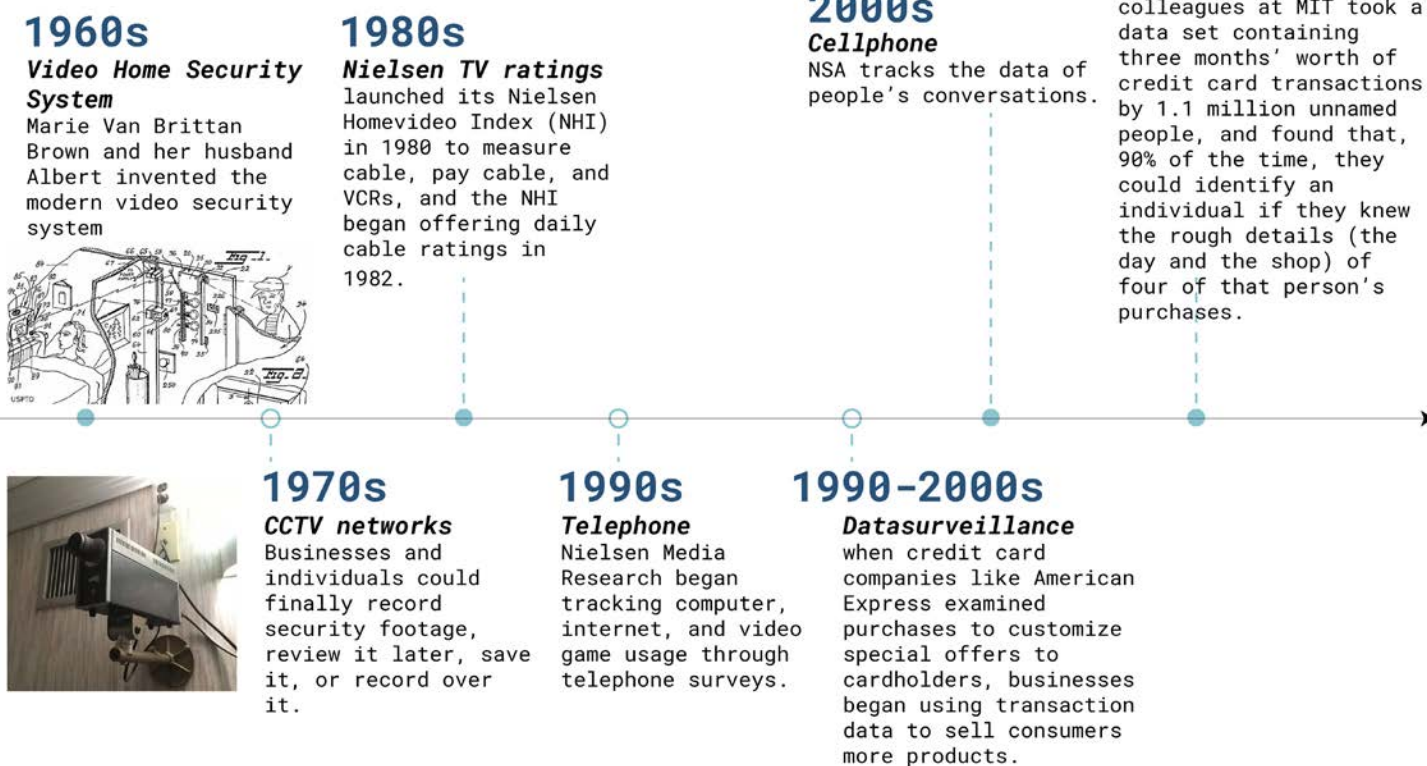l be constantly surveilled. Even when no one is actively observing, the presence of the central watch tower gives the prisoners the impression of continuously being watched.

The Pacific Telegraph Company reached the West Coast, California passed the first law outlawing wiretapping in 1862. The first person to be found guilty was a stockbroker by the name of D.C. Williams in 1864. His clever plan involved listening in on business telegraph lines and selling stock dealers the information he learned.

Security cameras have spread widely in a relatively short period of time. Over a billion cameras have reportedly been deployed globally. It's hard to get away from them. In 1949, the first CCTV security cameras that the general public could buy appeared. They were created by American business Vericon, but they were still unrecordable and required continual supervision. In 1949, the first CCTV security cameras that the general public could buy appeared. They were created by American business Vericon, but they were still unrecordable and required continual supervision. The videotape recorder (VTR) was created just two years later, in 1951.

1960s
Video Home Security System
Marie Van Brittan Brown and her husband Albert invented the modern video security system

1970s
CCTV networks
Businesses and individuals could finally record security footage, review it later, save it, or record over it.

1980s
Nielsen TV ratings
launched its Nielsen Homevideo Index (NHI) in 1980 to measure cable, pay cable, and VCRs, and the NHI began offering daily cable ratings in 1982.

1990s
Telephone
Nielsen Media Research began tracking computer, internet, and video game usage through telephone surveys.

1990-2000s
Datasurveillance
when credit card companies like American Express examined purchases to customize special offers to cardholders, businesses began using transaction data to sell consumers more products.

2000s
Cellphone
NSA tracks the data of people's conversations.

2010-Now
Datasurveillance
de Montjoye and colleagues at MIT took a data set containing three months' worth of credit card transactions by 1.1 million unnamed people, and found that, 90% of the time, they could identify an individual if they knew the rough details (the day and the shop) of four of that person's purchases.
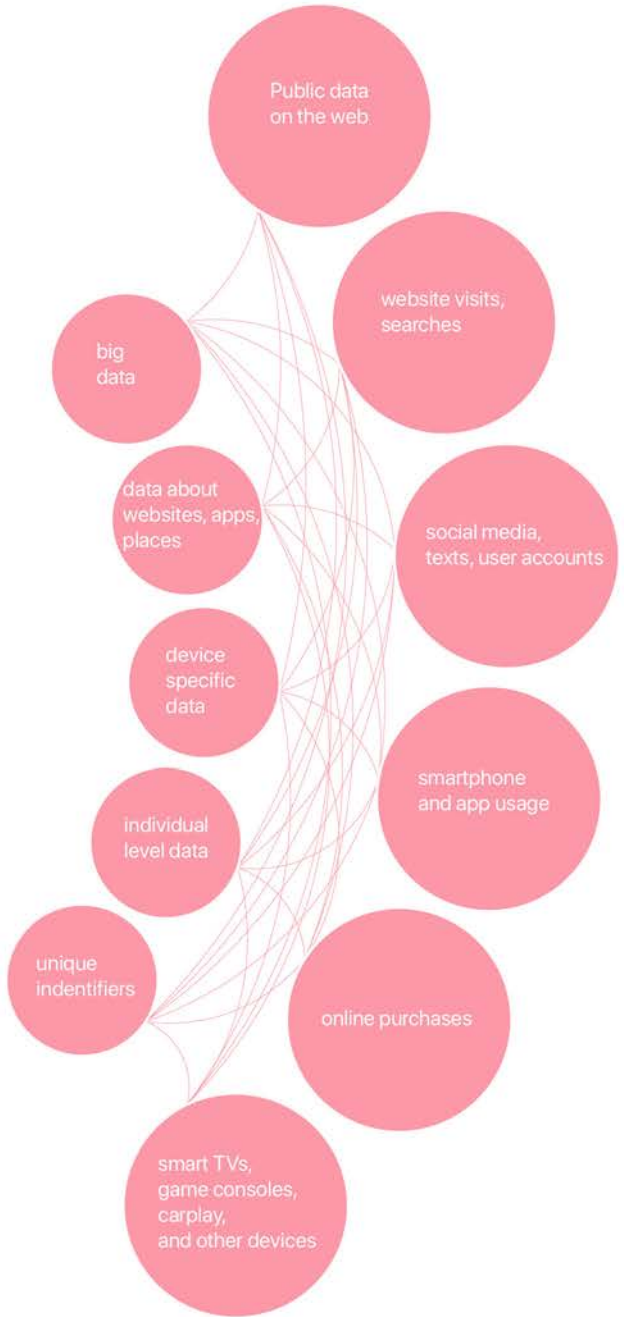
In 1969, videocassettes revolutionized the industry. They were less expensive and smaller than conventional reels. The recorded tape was contained in a plastic case. As a result, cassettes may be changed swiftly and simply. This development made it possible for security and surveillance cameras to become widely used. Consumer VCRs, which first became available in 1971, greatly accelerated adoption. In the late 1960s, Marie Van Brittan Brown and her husband Albert created the first video surveillance system. She created an integrated security system out of concern for her safety when she was home alone. She could use this to view and communicate with whoever was at the door. The world had never seen anything like it before.

The game Pokémon Go is an augmented reality mobile game, which based on the use of real street view. It does not notify users that full access is being granted in the sign-in process. Any time you sign in, whether it be through a Google account or the Pokémon Trainer Club, your username and email address are made public. This is a rather common procedure when entering game accounts. Because augmented reality (AR) relies on your camera, it will also need access to it.

However, nowadays, people don't care about the eavesdropping by companies.

Every word we talk to cell phones, computers, Amazon Alexa, and Google Home is being listened and wiretapped. This new kind of surveillance lead to a new argument that people are willing to be surveilled because they can offer you what you want and know your needs. Seems we are in the privacy paradox, right? But where will the surveillance go in the future?

The situation will be put to the extreme. All products by PAN are connected to the implant. So, every transaction on PAN network, app usage through PAN devices, body and health conditions, conversation, voice, sound, social media, thoughts, actions, encounters, and public data on the cloud through the clip implant will be collected and surveilled by PAN. PAN will use data to optimize the community, city, living environment, and every aspect of people's lives. It will be the end of privacy.

Public data on the web

website visits, searches

big data

data about websites, apps, places

social media, texts, user accounts

device specific data

smartphone and app usage

individual level data

unique indentifiers

online purchases

smart TVs, game consoles, carplay, and other devices

Observation
-Uber Eats

Uber introduced its online meal ordering and delivery service called Uber Eats in 2014.

I use Uber Eats almost everyday for ordering meals from various restaurants. On Tuesday night, I was doing my thesis diagrams, and I was starving. So, I ordered from McDonald's on Uber Eats. On the next day, I was chilling on the sofa. I got a notification from Uber Eats...
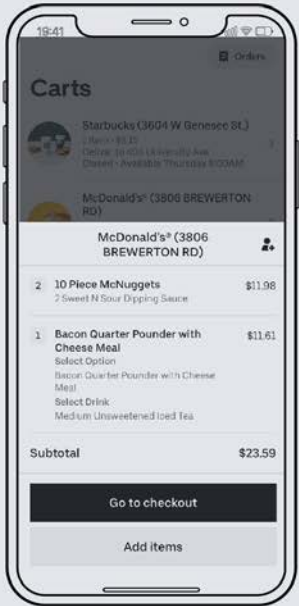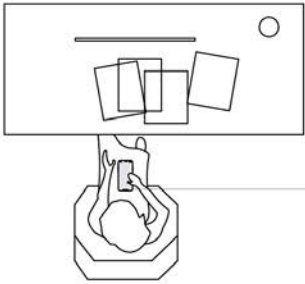
Ordered from Ubereats on Tuesday

Got notification from Ubereats on Wednesday

Observation
–Google Ads

Google Ads targeted a specific keyword you search for and display products or services that users are most likely to buy.

I was wondering can Google Ads predict what I want just based on the keywords I searched.

With this question, I searched for chairs at 9:12 p.m. Google Ads showed a bunch of chairs on my screen, but none of them is what I want.

I searched for a specific chair – a Barcelona chair at 9:13 p.m.
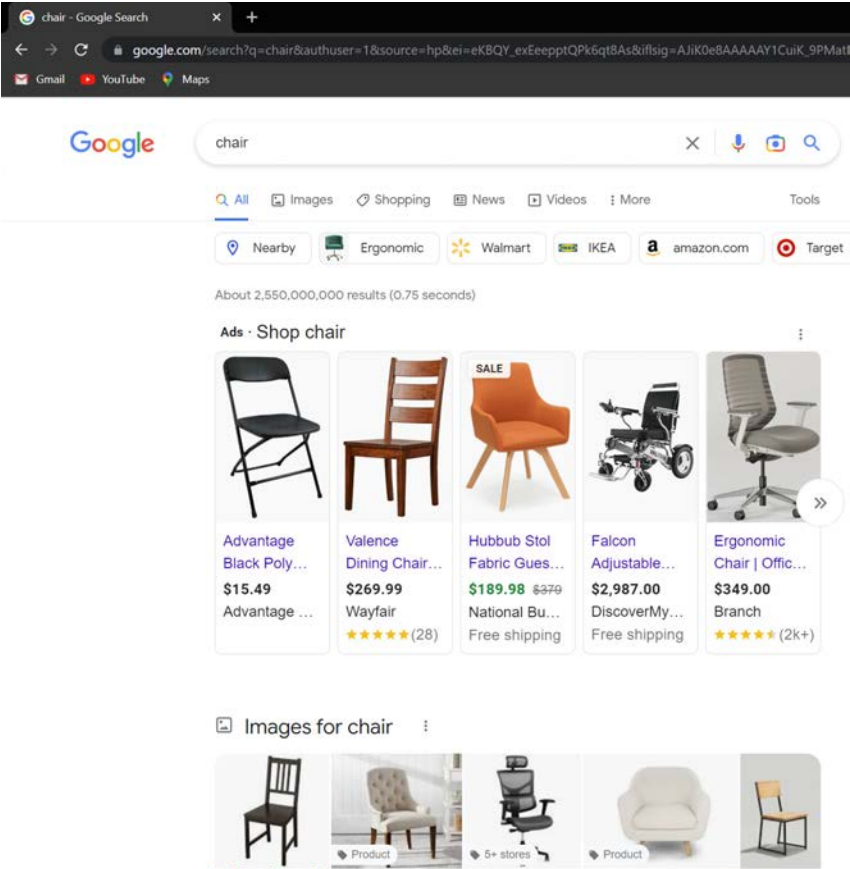
9:12 PM
Search Chair on Google
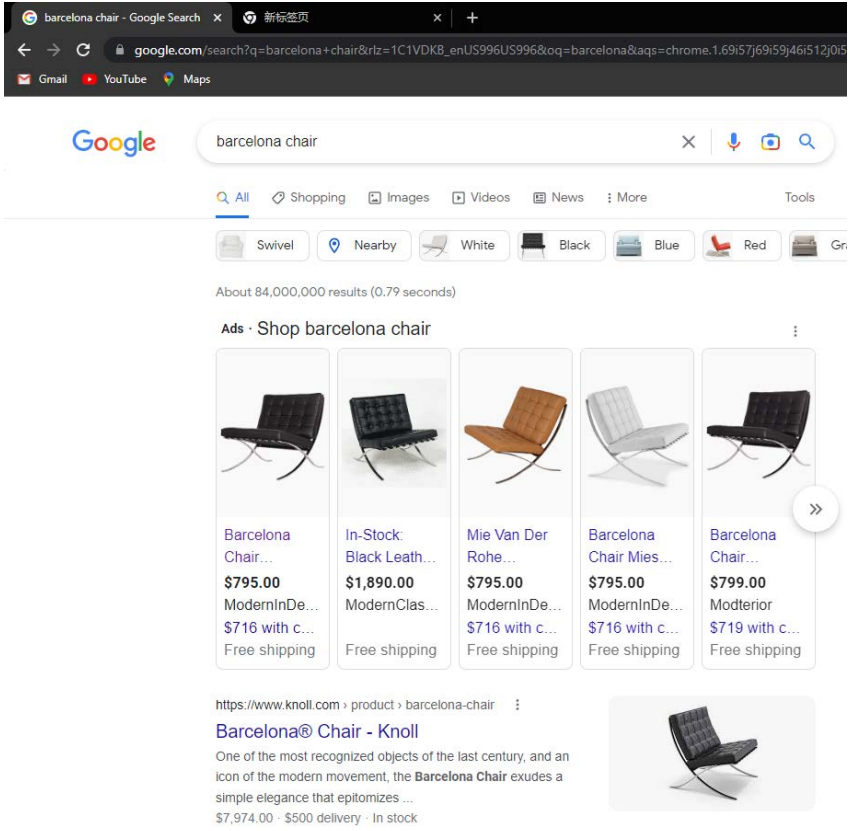
9:13 PM
Search Barcelona Chair on Google

Observation
–Google Ads

9:32 PM
Search Chair Again on Google

And then I searched for a chair again at 9:32 p.m. This time Google Ads also showed two Barcelona chairs on the screen. That was interesting.

At last, I searched for Mies Van Der Rohe at 10:13. Google Ads also showed two Barcelona chairs on the screen. That became even more interesting...
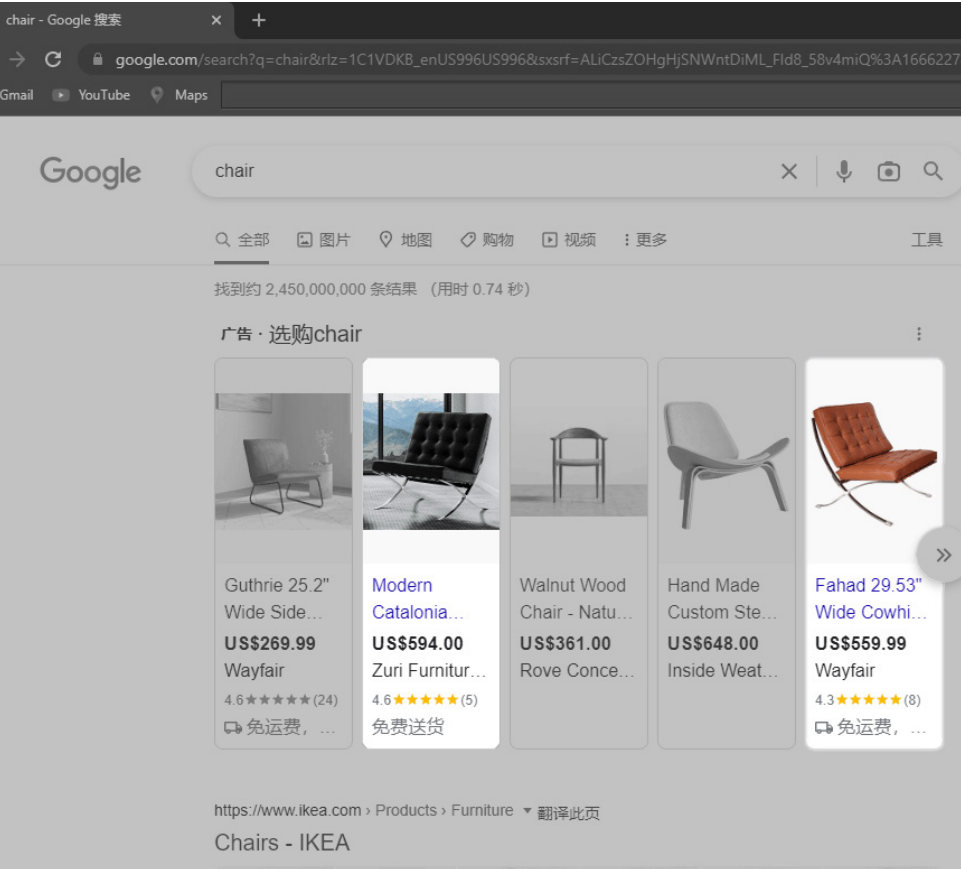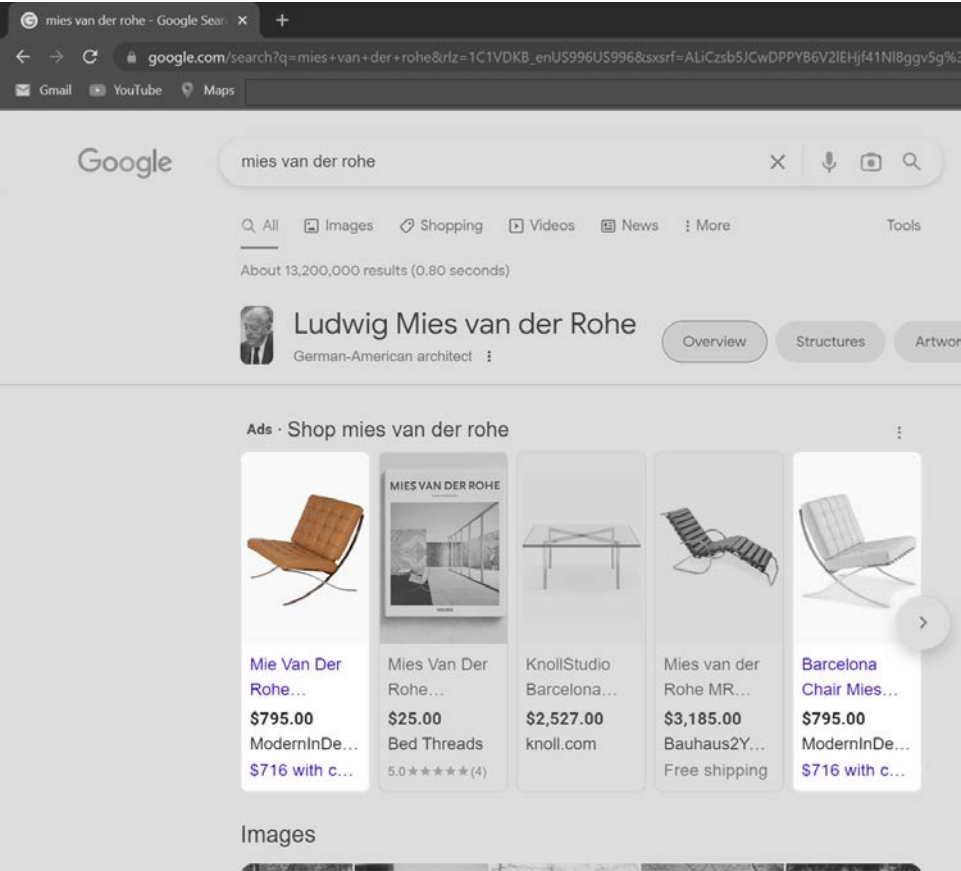
10:13 PM
Search Chair Again on Google

Observation
-Instagram

In our everyday life, data surveillance happens all the time. For example, if a person is watching an NBA game, their cellphone actually hears and captures that. This is just like the Siri feature on iPhone. They say they do not listen when you are not having a conversation with Siri, but they are actually listening at the backstage all the time. If they are not listening, how could you activate Siri simply with a voice command of "Hey Siri"?

Same as with Instagram, the backstage will hear the sound of an NBA game being broadcast from the TV, and it will advertise related products to you. If you like certain post about an NBA game, Instagram will also know your preference and feed you related advertisement such as NBA player jerseys, NBA league pass subscription, sports bet, and NBA related video games.

Similar situations can be seen at so many other aspects of daily life. After you did something or said something, you immediately see the exact topic shows up on your social media, Google search suggestion, and online shopping platforms.
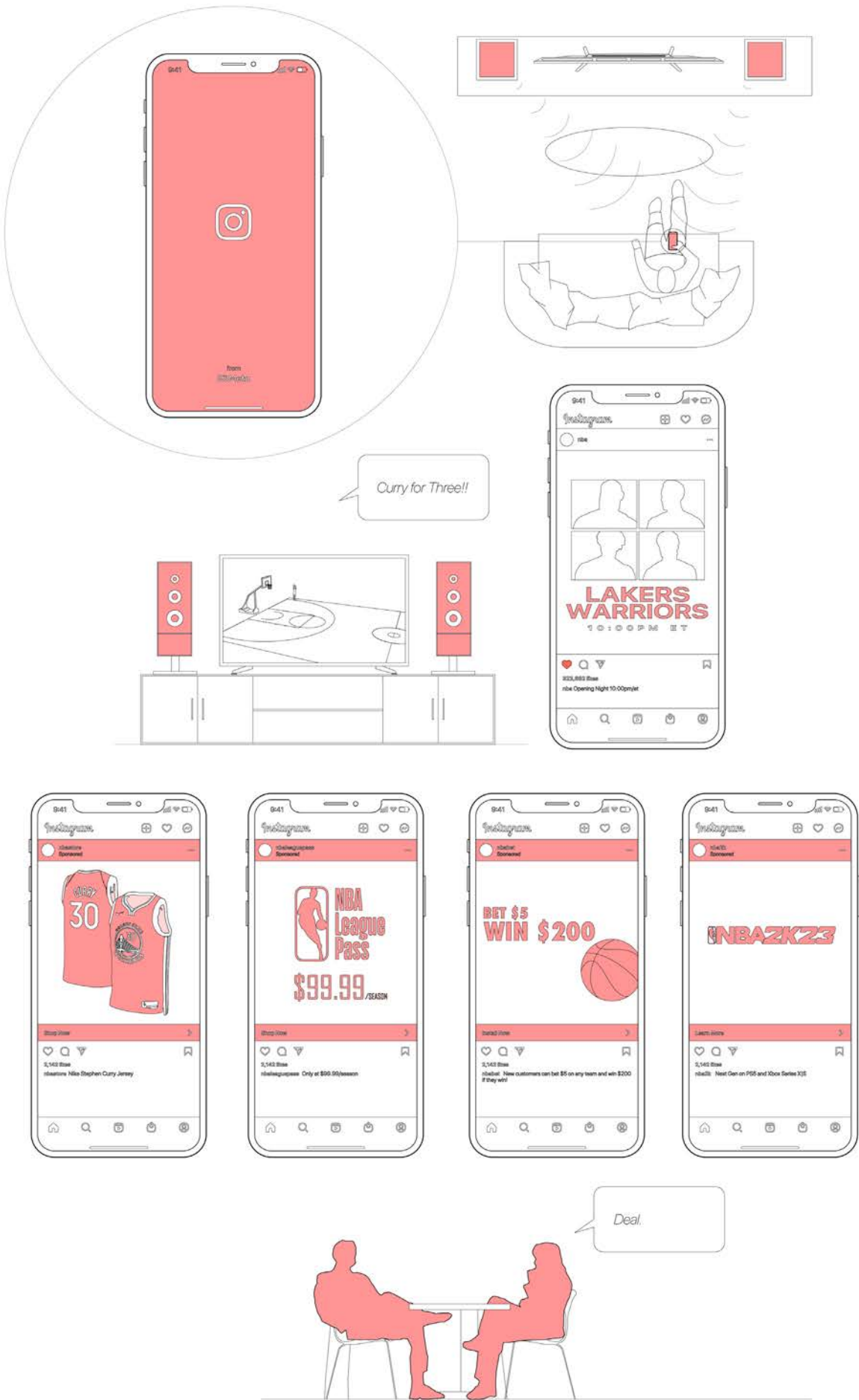
Observation
-Apple Maps

Another striking example of data surveillance happens when you use Apple Maps. After you get to your destination using its navigation feature, the app marks your location as where you parked your car. Certainly, this might be helpful if you could not find your car, but did we ask Apple Maps to do it in the first place? This suggests that we are giving the app too much power that it makes a decision for you without you telling it to do so.

Not only does it know your location, it also knows when you plan to go home, where your home is, and automatically tells you how long it takes to get home. A frightening observation I have is when I get in the car from my parked location, a message from Apple Maps pops up automatically showing how long it takes to get home. This message does not show up before I get in the car or when I stand outside of the car. It shows up immediately after I get into the car. I never told my phone where my home is, and it just studies my daily routine and figures out where my home is by itself.

Observation
-Strava

Such a data surveillance can lead to serious exposures and consequences. In 2018, the fitness tracking app Strava has exposed US army base location in Afghanistan through their heatmap. As the military was training and jogging, their jogging route was recorded and uploaded by the Strava app they use. Such an exercising route and location can be seen by anyone who uses Strava, and thus the exposure of the army base location. This could lead to dangerous consequences as their location and activities should be confidential.
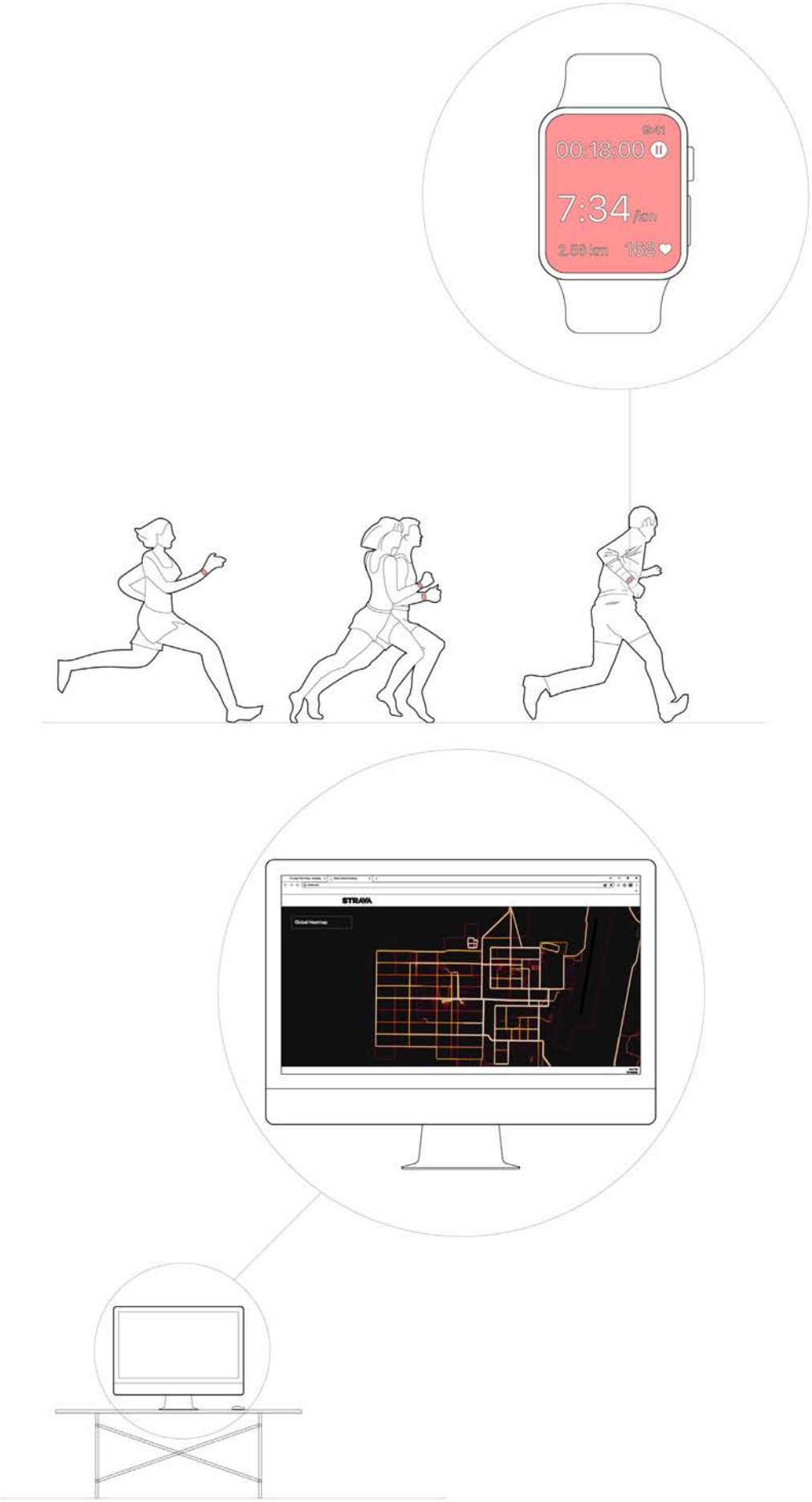
Behavior Control

In the 1890s, Russian physiologist Ivan Pavlov discovered that dogs not only salivate when food is placed in front of them, but also start to salivate whenever they notice anything associated with food. This led him to a series of experiments which would be known as Pavlovian conditioning, or classical conditioning. At the beginning of the experiment, food is the unconditioned stimulus and salivation is the unconditioned response, which means a dog would naturally respond to food with salivation. Pavlov then used the sound of a metronome as a neutral stimulus and the dog showed no response of salivation to that because the sound of a metronome would not remind the dog anything about food. Pavlov then started the conditioning process in which he rang the metronome before he gave the dog food and repeated it several times. After the conditioning process, the sound of a metronome itself can cause the dog to salivate even without food. In this case, the sound of a metronome is the conditioned stimulus and salivation becomes a conditioned response of that. This conditioning proved that behavior can be controlled and manipulated. If the stimulus is conditioned, the response would be conditioned as well.
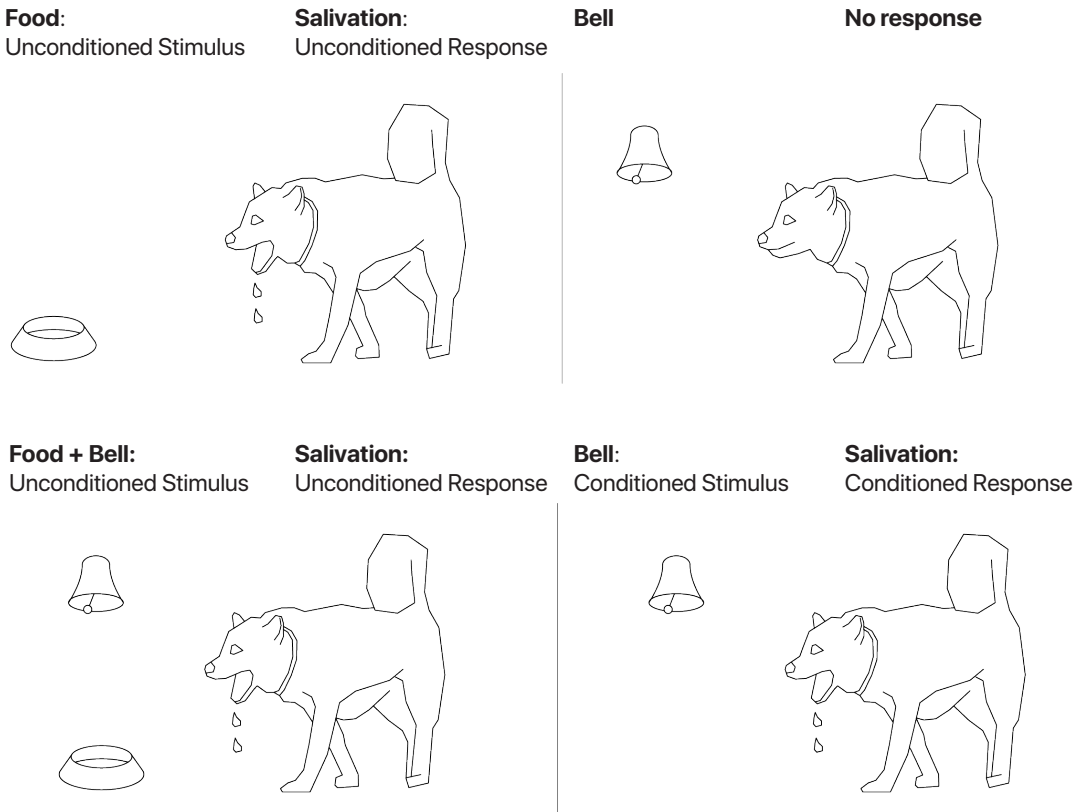
Pavlov's experiment shows that conditioning applies to animals, but John B. Watson's Little Albert Experiment proves that the same conditioning can be applied to human as well. In this experiment, Watson brought a nine-month-old baby called "little Albert" and recorded his reaction towards a rat. At the beginning, little Albert showed no fear of the rat as both stimulus and response are unconditioned. Watson then introduced a loud sound caused by a hammer and a steel bar along with the rat. Little Albert started to cry since he was scared by the sudden loud sound. After repeating this process seven times, little Albert was conditioned to cry and show fear with only the appearance of the rat and without a loud sound.

In today's digital world, we are all conditioned by this behavioral control because when we hear a notification tone from our phones, we would "naturally" pick it up to see whatever content whichever app sends us. This behavioral control method can be further used to control the users by tech companies.
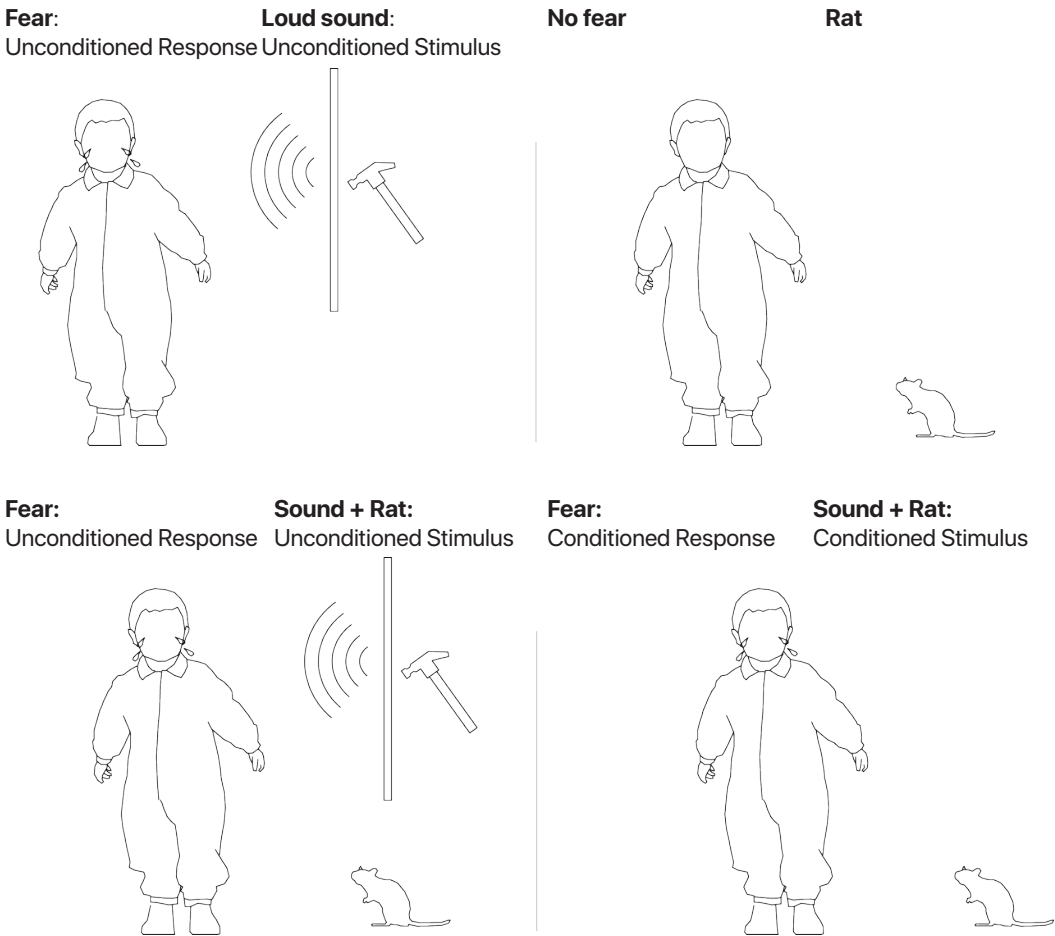
Ivan Pavlov

Pavlovian Conditioning

Food: Unconditioned Stimulus   **Salivation**: Unconditioned Response   **Bell**   **No response**

Food + Bell: Unconditioned Stimulus   **Salivation**: Unconditioned Response   **Bell**: Conditioned Stimulus   **Salivation**: Conditioned Response
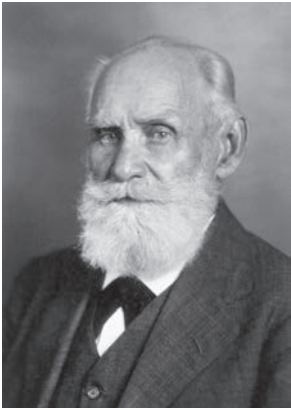
John B. Watson

Little Albert Experiment

Fear: Unconditioned Response   **Loud sound**: Unconditioned Stimulus   **No fear**   **Rat**

Fear: Unconditioned Response   **Sound + Rat**: Unconditioned Stimulus   **Fear**: Conditioned Response   **Sound + Rat**: Conditioned Stimulus

Human Microchip Implant

1998

The first experiments with a radio-frequency identification (RFID) implant were carried out in 1998 by the British scientist Kevin Warwick. His implant was used to open doors, switch on lights, and cause verbal output within a building. After nine days the implant was removed and has since been held in the Science Museum in London.
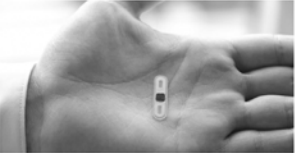
2004

Nokia, Philips (now under NXP Semiconductors) and Sony established the NFC Forum, a non-profit industry formed to advance the use of NFC wireless interaction in consumer electronics, mobile devices and PCs. Standards include the four distinct tag types that provide different communication speeds and capabilities covering flexibility, memory, security, data retention and write endurance. NFC Forum promotes implementation and standardization of NFC technology to ensure interoperability between devices and services.
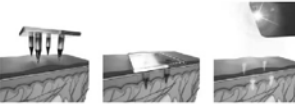
2018

VivoKey Technologies developed the first cryptographically-secure human implantable NFC transponders in 2018. The Spark is an AES128 bit capable ISO/IEC 15693 2mm by 12mm bioglass encased injectable device. The Flex One is an implantable contactless secure element, capable of running Java Card applets (software programs) including Bitcoin wallets, PGP, OATH OTP, U2F, WebAuthn, etc. It is encapsulated in a flat, flexible 7mm x 34mm x 0.4mm flat biopolymer shell. Applets can be deployed to the Flex One before or after implantation.
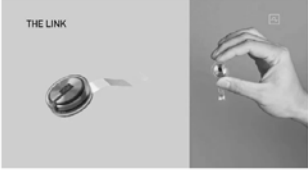
2019

Bill & Melinda Gates Foundation funded MIT to develop an invisible microneedle patch used to store digital medical information, along with a vaccine.

2020

On 28 August 2020, Neuralink CEO Elon Musk, revealed a company directed live video podcast showcasing a pig called Gertrude with a coin-sized computer chip in her brain to demonstrate his ambitious plans to create a working brain-to-machine interface.

2021

Dsruptive Subdermals tested a COVID-19 vaccine passport in their bioglass coated NFC microchip designed to get implanted in the subcutaneous tissue for humans. However, this is a start-up hub, is not yet for sale. It has been demonstrated by its managing director Hannes Sjöblad who wears the chip in his arm.

"Author, Michael Fitzhugh Bell is drugged, abducted, raped, and surgically implanted with illegal microchip implants; all done without his knowledge or consent. Michael is tracked, stalked, and tortured, 24/7—and physically burned remotely with directed energy weapons which most people don't even know exist. His every thought and feeling is being read in real time by his perpetrators via GPS and current cellular satellite systems, making him, quite literally, a human piñata. Michael must prove his crime to the police and a judge before his attackers erase his memories and murder him."

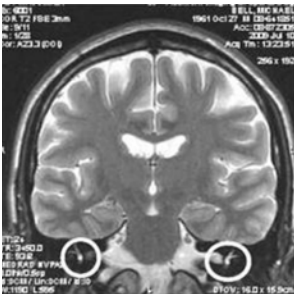"A linear foreign body in my navel can be seen here in an ultrasound image."

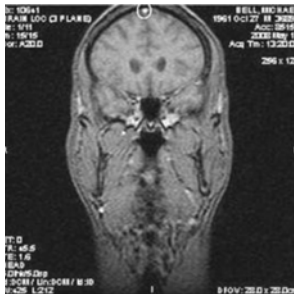"A linear shaped foreign body can be seen at the top of the ultrasound image, just above my left eye."

"Three bright white foreign bodies can be seen clearly, one at the top of my brain, the other two behind each ear."

"A foreign body can be seen above my left eye. These are my actual MRI images."

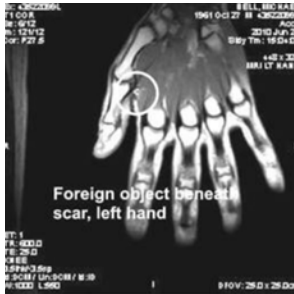"Two 'rabbit ear' antenna devices can be seen below my brain."

"Another MRI image shows a foreign body on top of my brain."

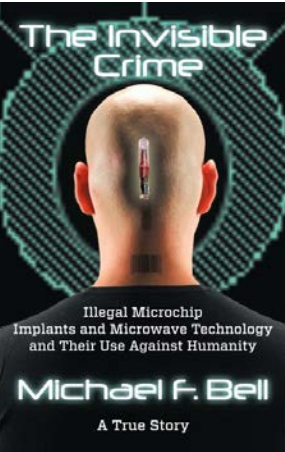"Six clearly visible foreign bodies can be seen in this image."

"This object is located beneath a small surgical scar on my right hand."

"A cosmetic surgery scar on my left hand, directly above a foreign body picture below in an MRI image."

The Invisible Crime :
Illegal Microchip Implants and Microwave Technology and Their Use Against Humanity

Michael F. Bell

Bell, Michael F. *The Invisible Crime: Illegal Microchip Implants and Microwave Technology, and Their Use against Humanity*. Brighton Pub. LLC, 2011.

Social Media App Analysis

Introduction

Social media is an integral part of our modern lives. It helps you to connect with the world, keep in touch with loved ones, engage with current events, share information, and have fun. But also, it is the one who took your privacy away from your control subtly.

We chose 9 social media apps: Facebook, WhatsApp, Kakao Talk, Instagram, Line, imo, Tik Tok, Viber, and WeChat, to be our analysis subjects. We chose these apps based on their popularities in different languages speaking regions.

In this section, we will look at three aspects of these apps, from User Distribution, Political Control, to Monthly Active Users.

syracuse

■ unknown

*Imo is the only messenger currently available in Turkmenistan without a VPN

Hey all! I am wendy.w, a architecture student, based in **Syracuse**, NY, USA. I love **social media**! They helped me getting to know **the world**!
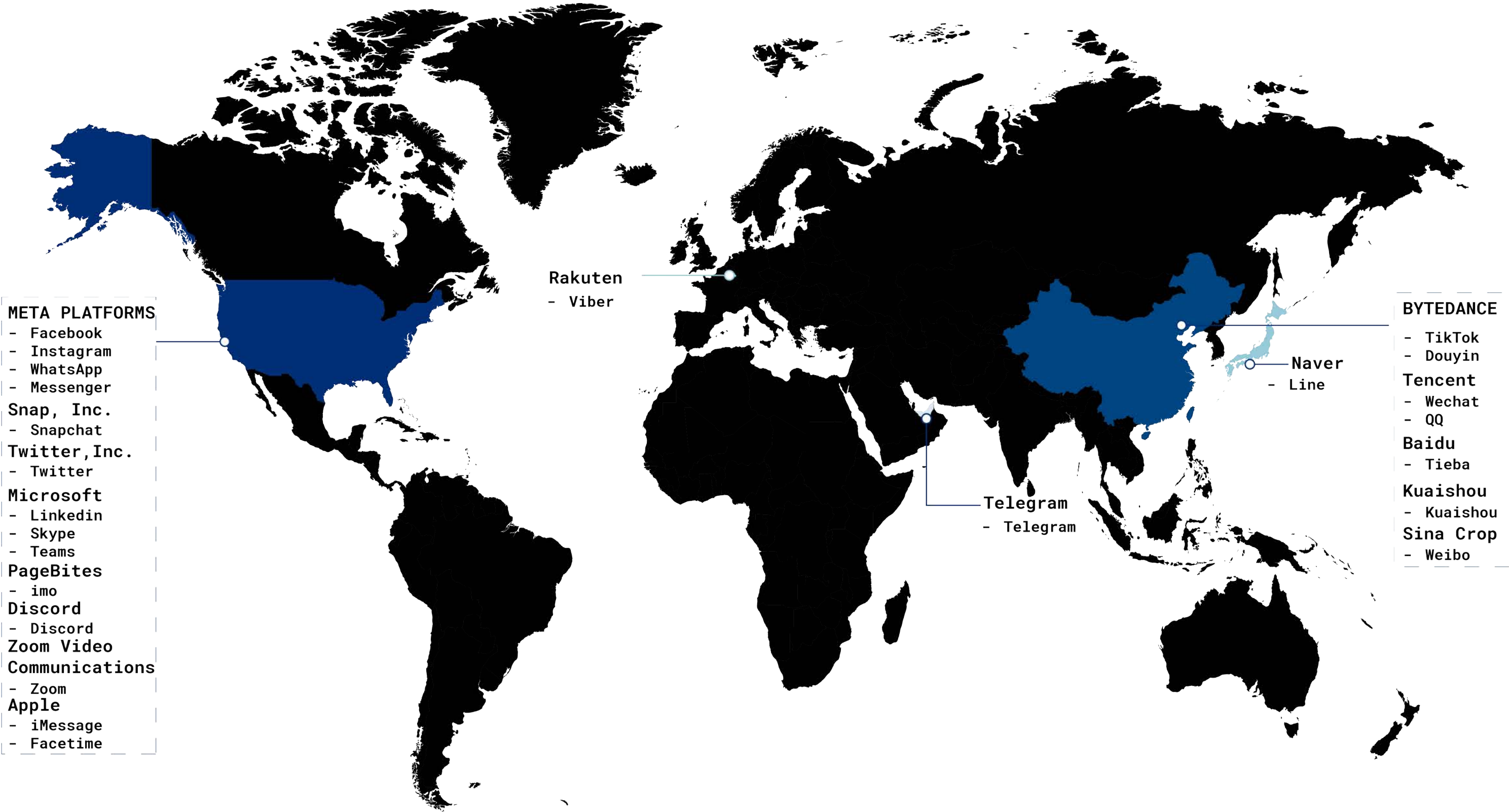
Profile

USERNAME:wendy.w

ABOUT ME:Definitely need social media addiction treatment

Apps with at least 100 million active users

The more users they have around the world, the more information the companies may hold. The apps also can be used as a political manipulation tool. The United States has the most messaging apps with at least 100 million active users, which means they have more control over users' personal data and use it to predict users' behavior and preferences to make a profit.

Rakuten
- Viber

Naver
- Line

Telegram
- Telegram

META PLATFORMS
- Facebook
- Instagram
- WhatsApp
- Messenger

Snap, Inc.
- Snapchat

Twitter,Inc.
- Twitter

Microsoft
- Linkedin
- Skype
- Teams

PageBites
- imo

Discord
- Discord

Zoom Video Communications
- Zoom

Apple
- iMessage
- Facetime

BYTEDANCE
- TikTok
- Douyin

Tencent
- Wechat
- QQ

Baidu
- Tieba

Kuaishou
- Kuaishou

Sina Crop
- Weibo

Facebook

Owned by the American business Meta Platforms, Facebook is a social media and networking website. It was established in 2004 by Mark Zuckerberg and fellow Harvard College students Eduardo Saverin, Andrew McCollum, Dustin Moskovitz, and Chris Hughes.

Devices with Internet connectivity, such as laptops, tablets, and smartphones, can access Facebook. Users can make a profile that contains information about them. They can send text, pictures, and other types of media with other users who have accepted to be their "friends" or, depending on the privacy settings, with the general public.
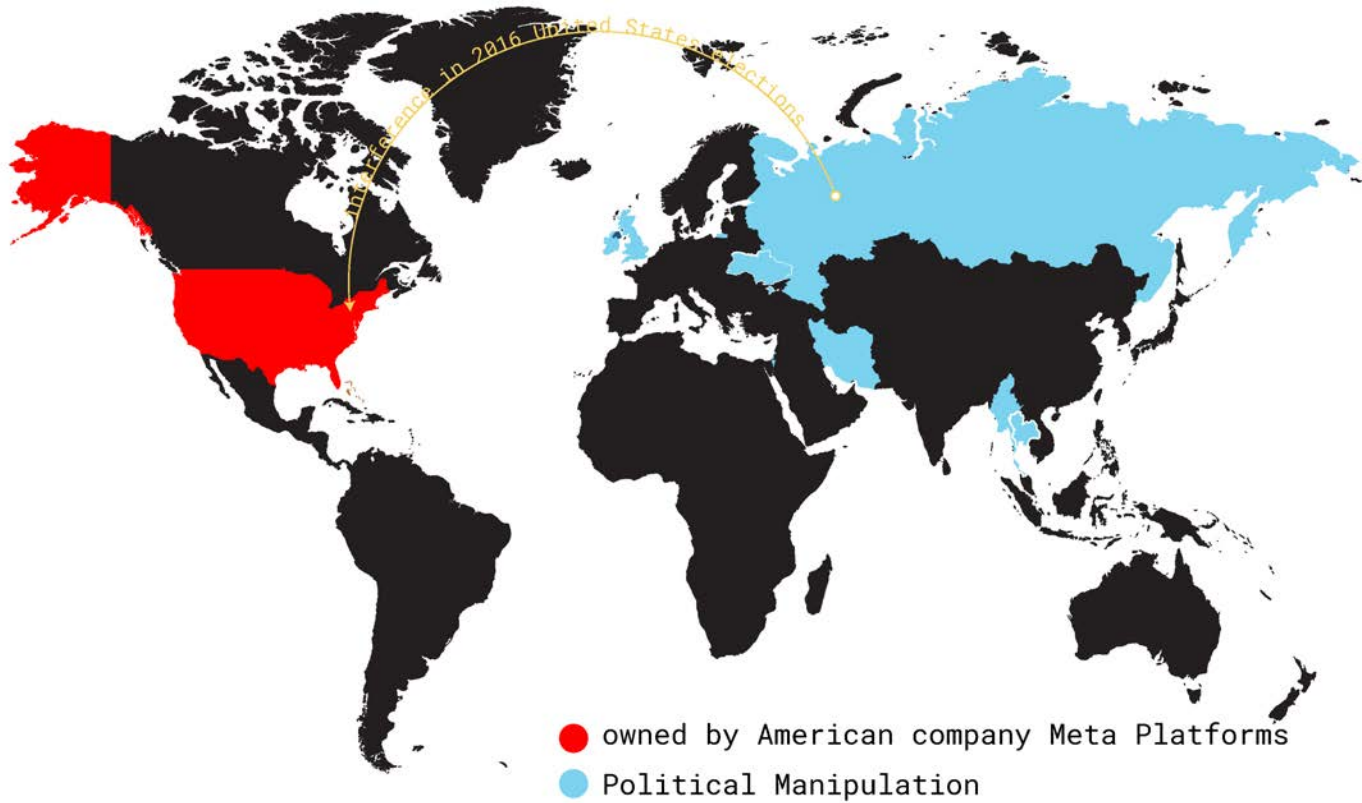
Facebook has received criticism for a variety of issues, including political manipulation, and user privacy.

Political Control

● owned by American company Meta Platforms
● Political Manipulation

User Distribution

syracuse

Jun.2022

Monthly Active Users: 2.934 Billion (July 2022)

unit: million

349.7

45.9

1. India
2. The United States
3. Indonesia
4. Brazil
5. Mexico
6. The Philippines
7. Vietnam
8. Thailand
9. Bangladesh
10. Egypt
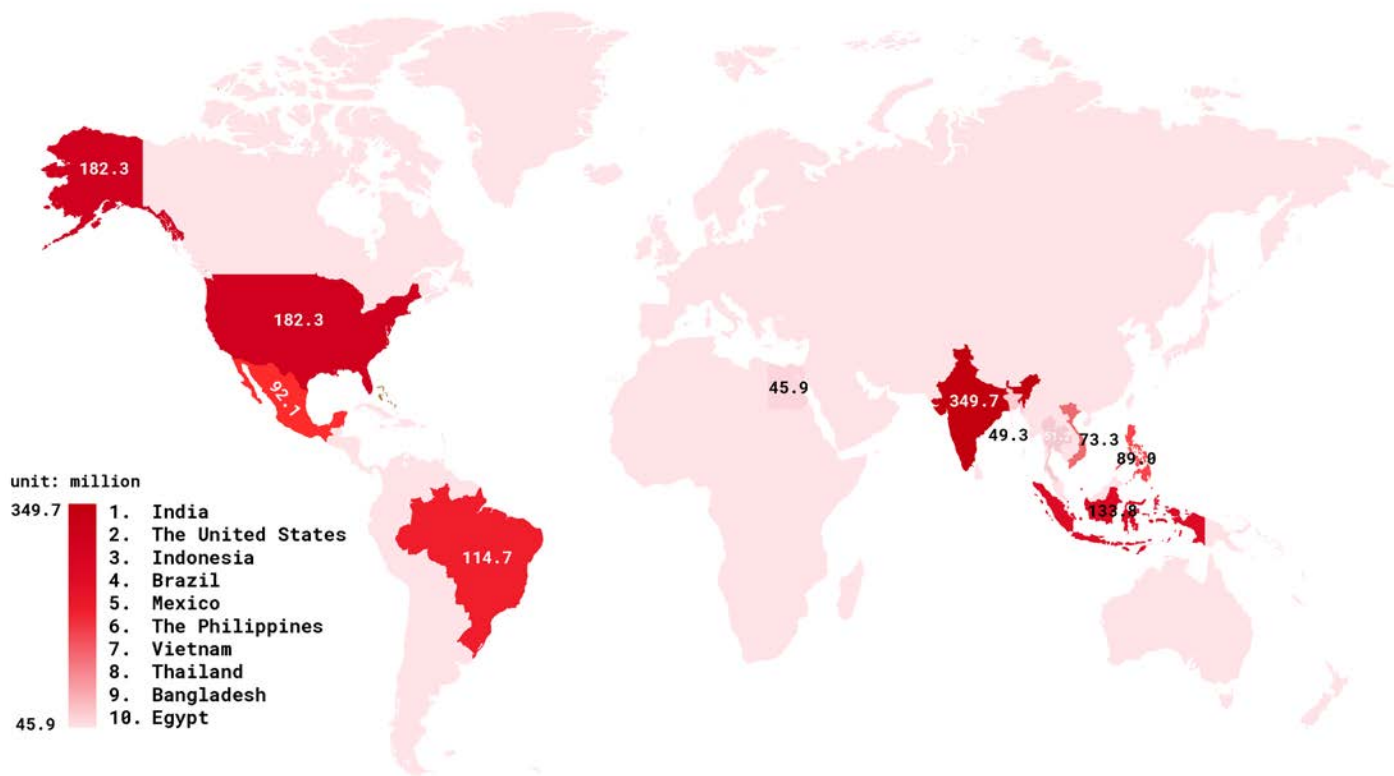
WhatsApp

Meta Platforms

Owned by the American business Meta Platforms, WhatsApp is a voice-over-IP (VoIP), cross-platform, centralized instant messaging (IM), and freeware service that is accessible worldwide. It enables users to share photographs, documents, user locations, and other content in addition to text and voice messages, phone conversations, and video calls. The client application for WhatsApp is available on PCs and works on mobile devices.

Devices with Internet connectivity, such as laptops, tablets, and smartphones, can access Facebook. Users can make a profile that contains information about them. They can send text, pictures, and other types of media with other users who have accepted to be their "friends" or, depending on the privacy settings, with the general public.

WhatsApp has received criticism for a variety of issues, including political manipulation (2018 Elections in Brazil), terrorism, snooping scandal, and privacy.
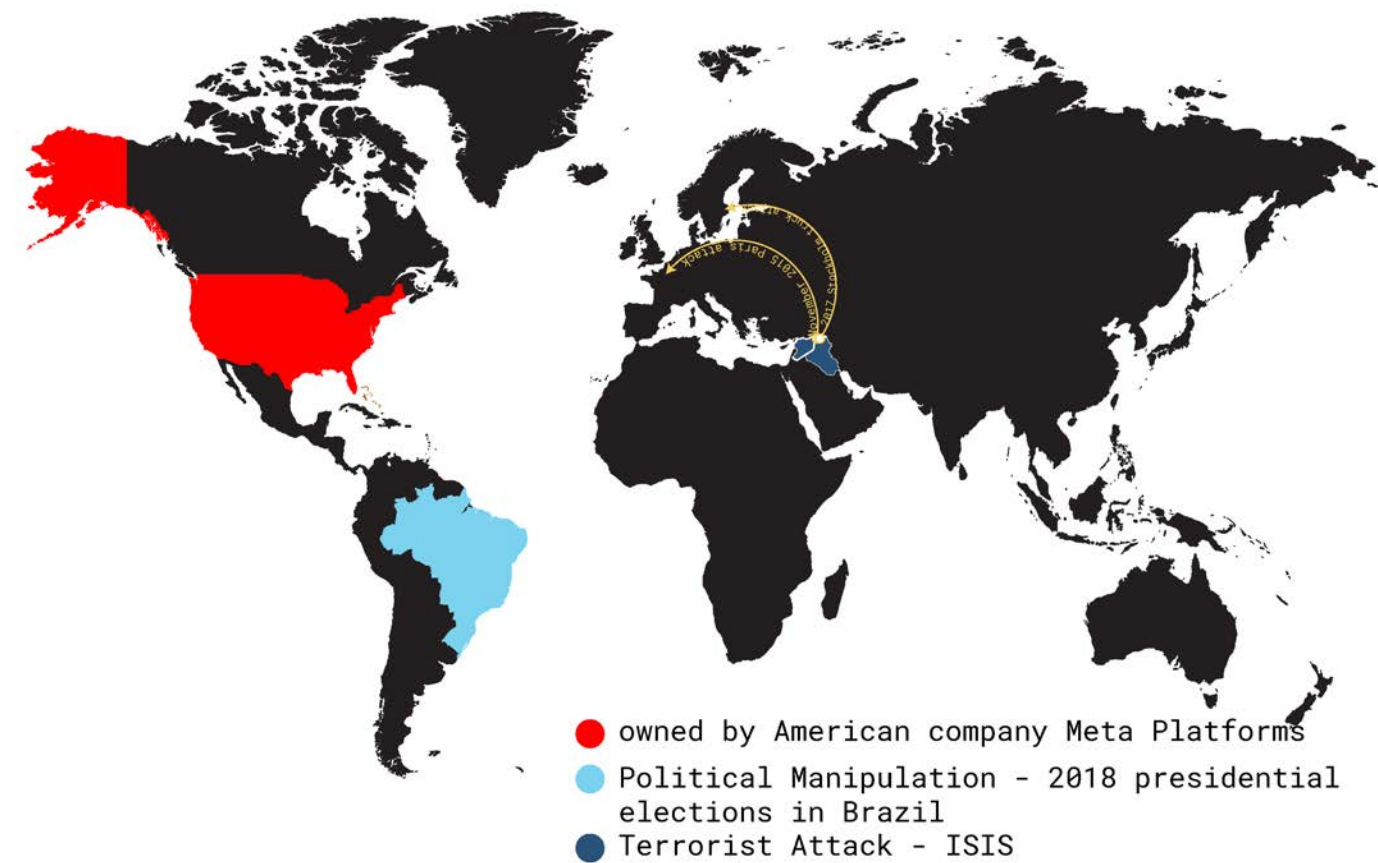
Political Control
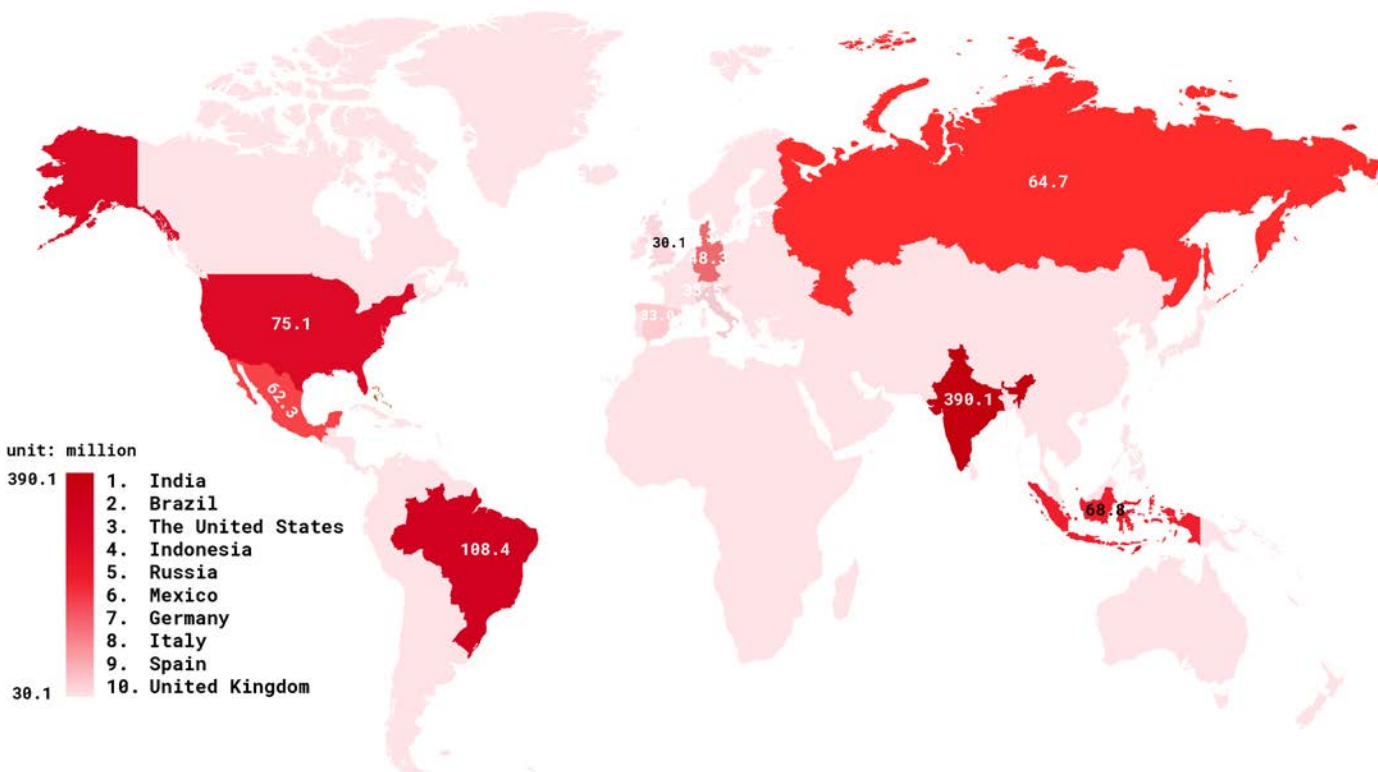

● owned by American company Meta Platforms
● Political Manipulation - 2018 presidential elections in Brazil
● Terrorist Attack - ISIS

User Distribution

syracuse

Jun.2022

Monthly Active Users: 2.000 Billion (Jan 2022)

unit: million
390.1

1. India
2. Brazil
3. The United States
4. Indonesia
5. Russia
6. Mexico
7. Germany
8. Italy
9. Spain
10. United Kingdom

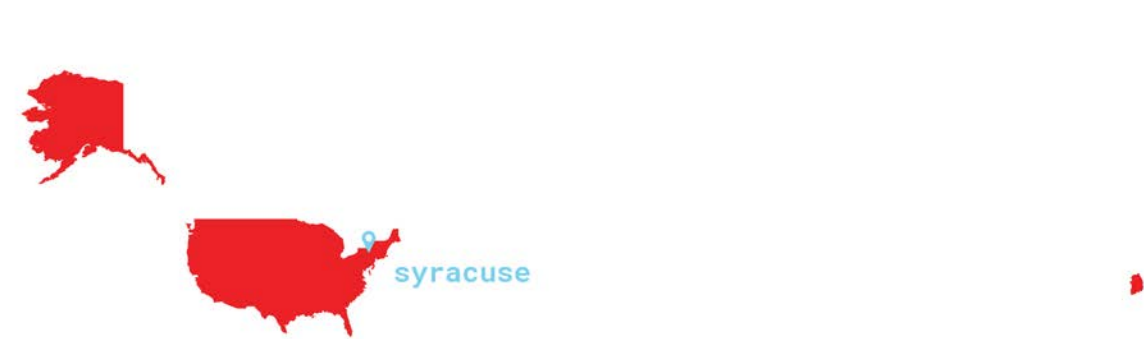30.1

64.7
30.1
75.1
62.3
390.1
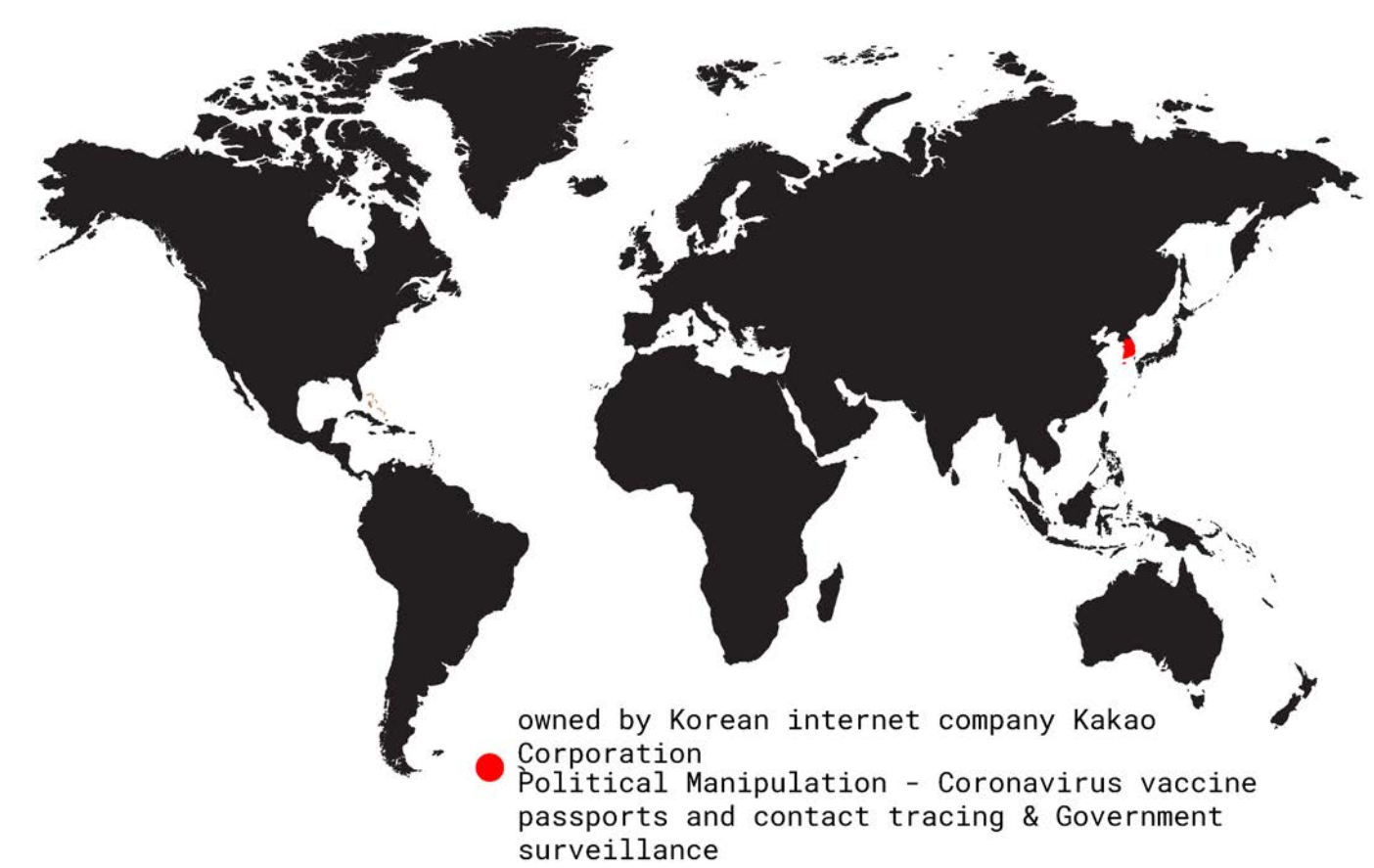108.4

Kakao Talk

Kakao Corporation

Kakao was founded in 2010. Kakao talk is a messaging app for smartphones, laptops, and PCs. It became the largest social media platform in South Korea, and it has 47 million active users in South Korea.

During the COVID-19, the app served as a tool for vaccine passport and contact tracing.

owned by Korean internet company Kakao Corporation
Political Manipulation - Coronavirus vaccine passports and contact tracing & Government surveillance

User Distribution

syracuse

Monthly Active Users: 53 Million (2013)

unit: million
47.0   Korea

6.0   other countries
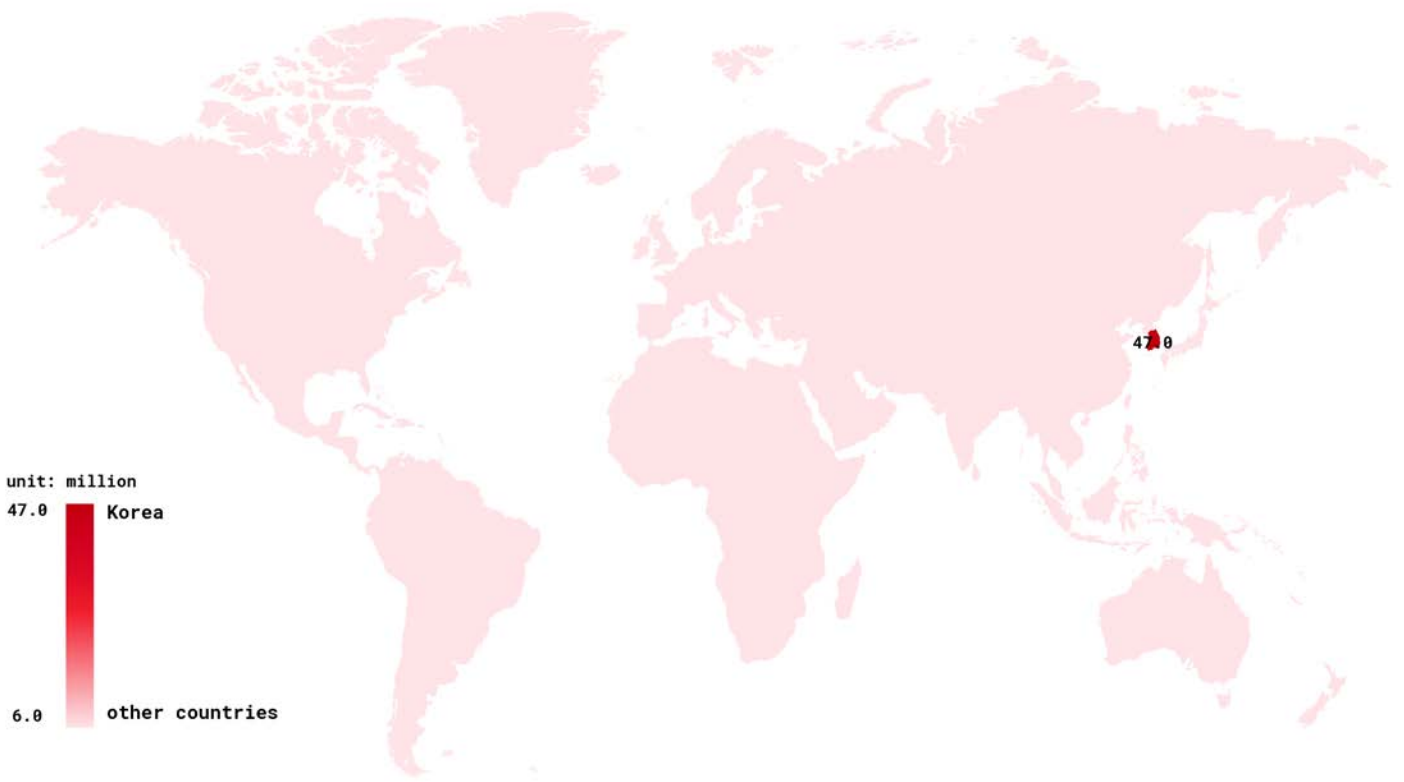
Jun.2022

Instagram

Meta Platforms

Owned by the American business Meta Platforms, Instagram is a photo and video sharing platform. Users can upload media that can be altered by filters, arranged by hashtags, and categorized by location.
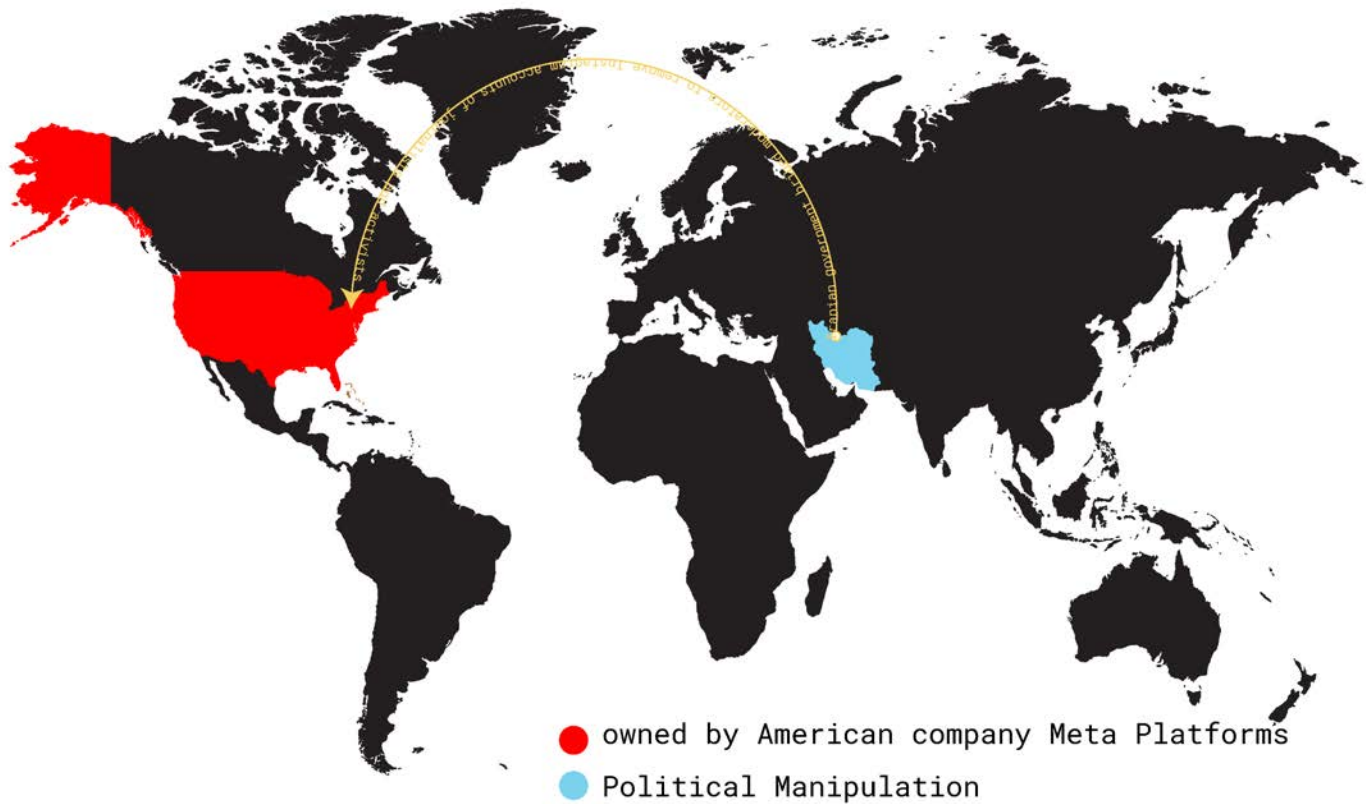
Instagram is the fourth-largest social media network globally, and it has 2 billion active users. Also it is the most popular social media platform for Gen Z.

User Distribution

Jun.2022

Political Control

● owned by American company Meta Platforms
● Political Manipulation

Monthly Active Users: 1.440 Billion (July 2022)

unit: million

263.8
27.4

1. India
2. The United States
3. Brazil
4. Indonesia
5. Turkey
6. Japan
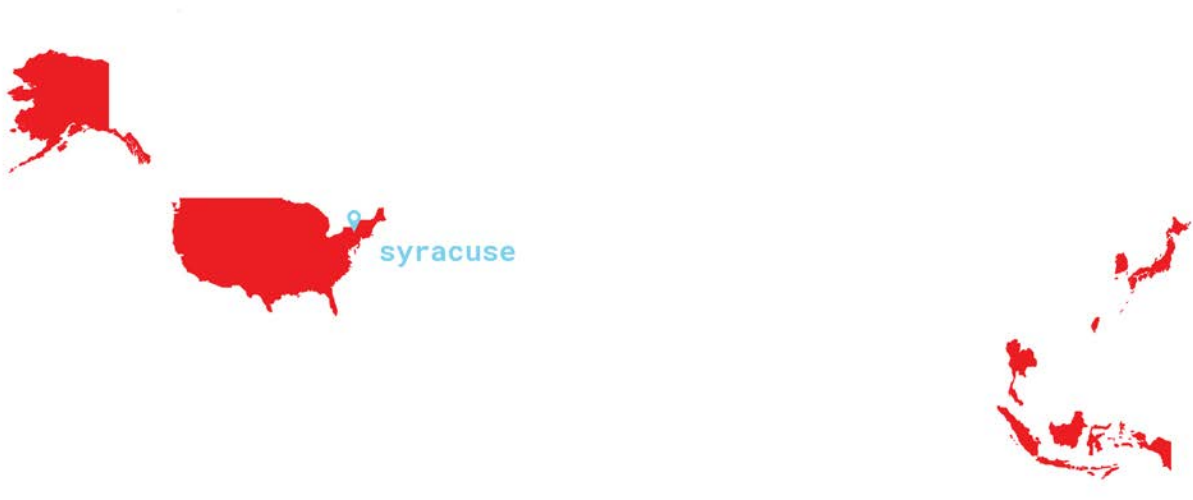7. Mexico
8. The United Kingdom
9. Germany
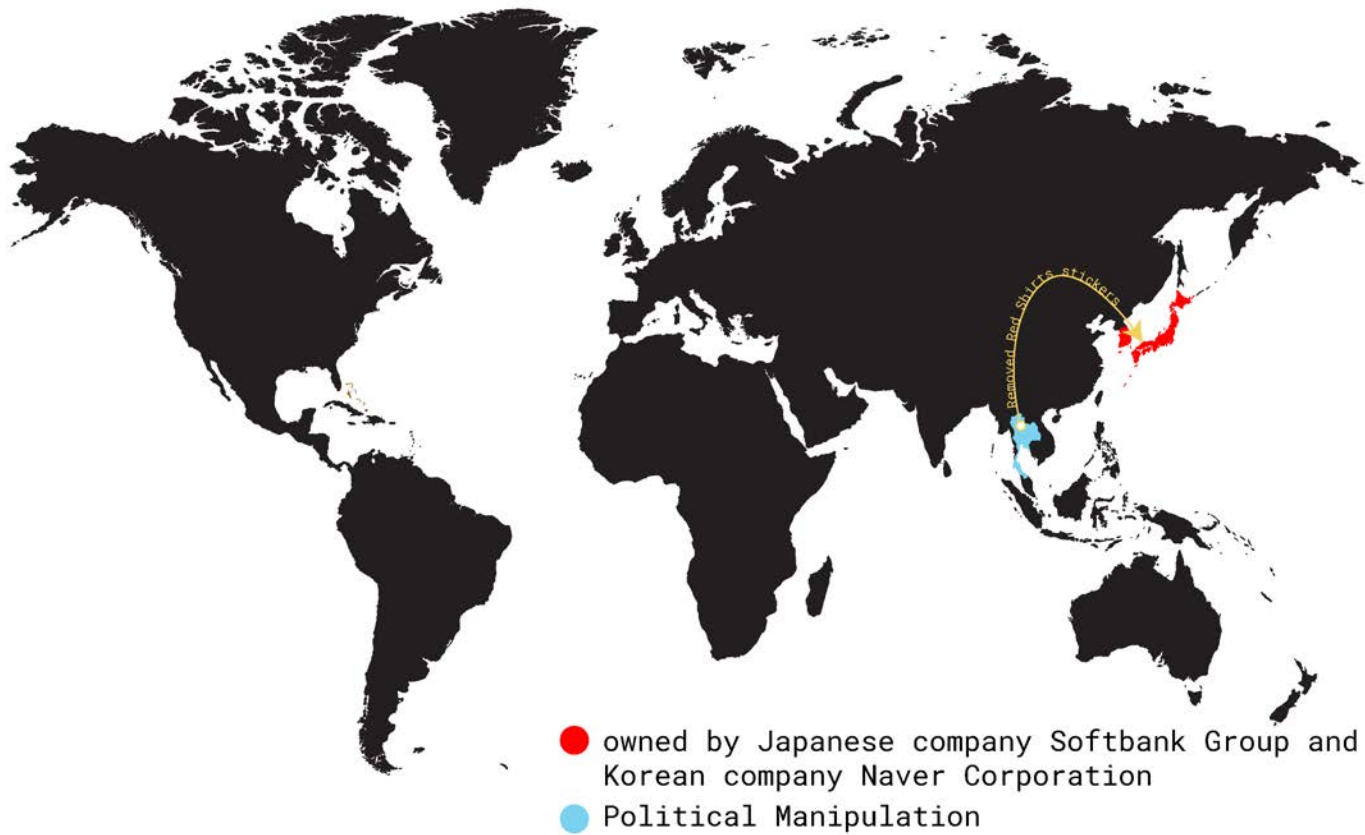10. Italy
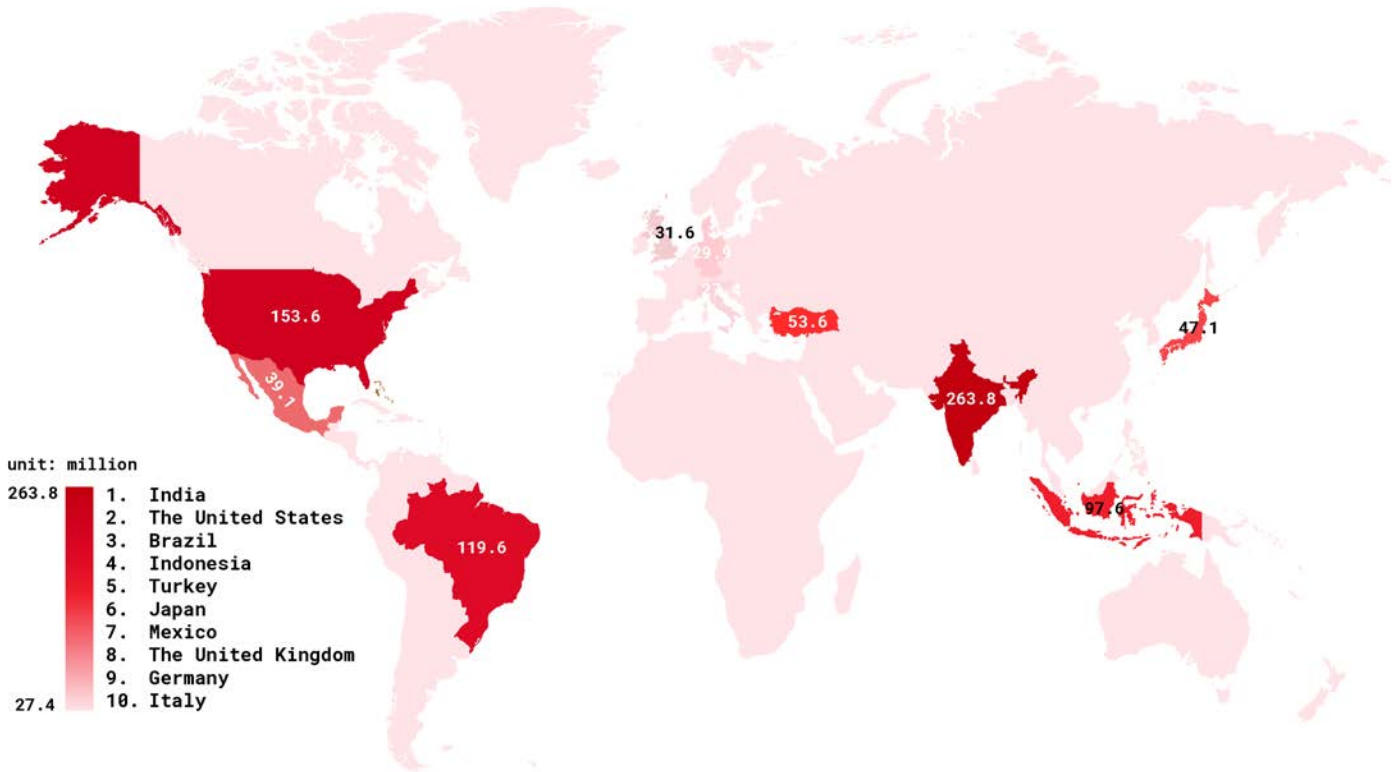
Line

Softbank Group and Naver Corporation

Line is a popular messaging app among Japan, Thailand, Taiwan, and the United States. Users of Line can hold free VoIP calls and video conferences as well as exchange texts, photos, videos, and audio. Additionally, Line offers various services, such as a digital wallet called Line Pay, a news feed called LINE Today, on-demand video called Line TV, and the distribution of digital comic books called Line Manga and Line Webtoon.

Political Control

● owned by Japanese company Softbank Group and Korean company Naver Corporation
● Political Manipulation

User Distribution

syracuse

Monthly Active Users: 178 Million (July 2022)

unit: million
86   Japan
      Thailand
      Taiwan
      The United States

other countries

3.15

Aug.2022

imo

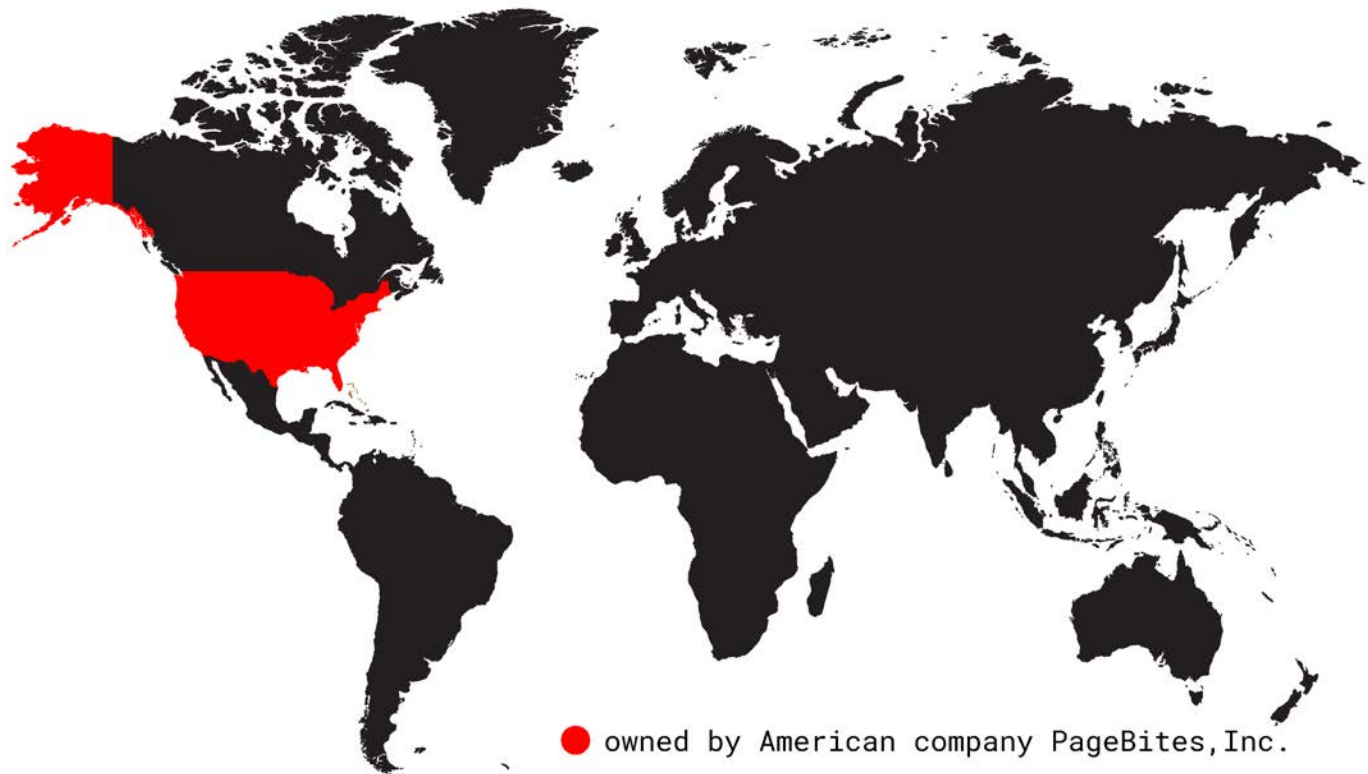*PageBites, Inc.*

imo allows users to call and message with friends. It enables the sending of free stickers, music, video, documents, and other materials through the application.
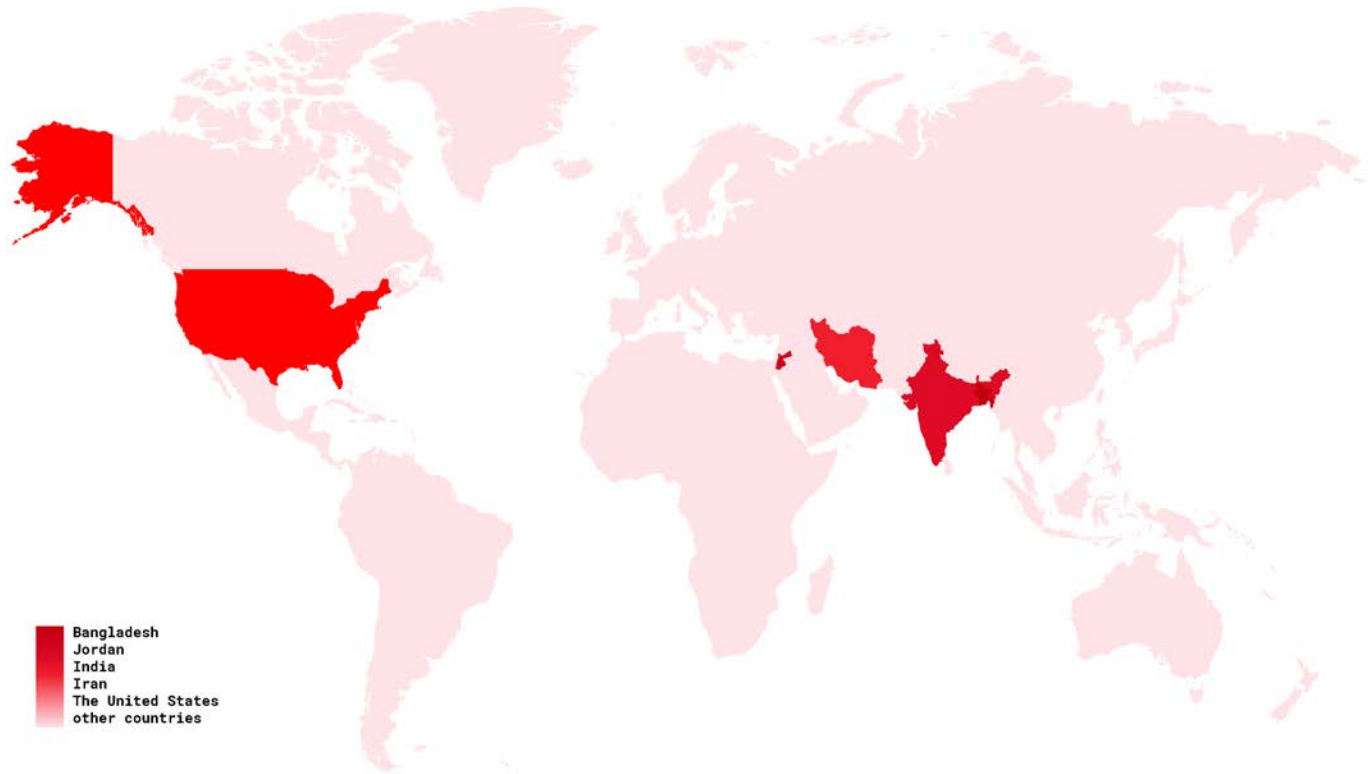
● owned by American company PageBites,Inc.

User Distribution

syracuse
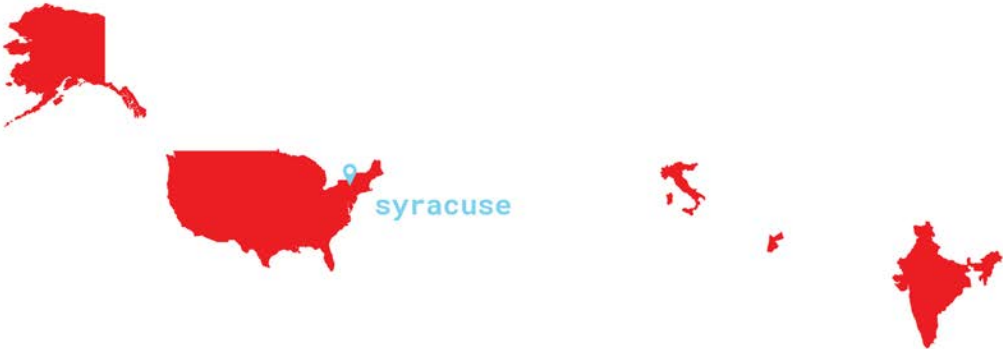
Monthly Active Users: 212 Million (Jan 2022)

Bangladesh
Jordan
India
Iran
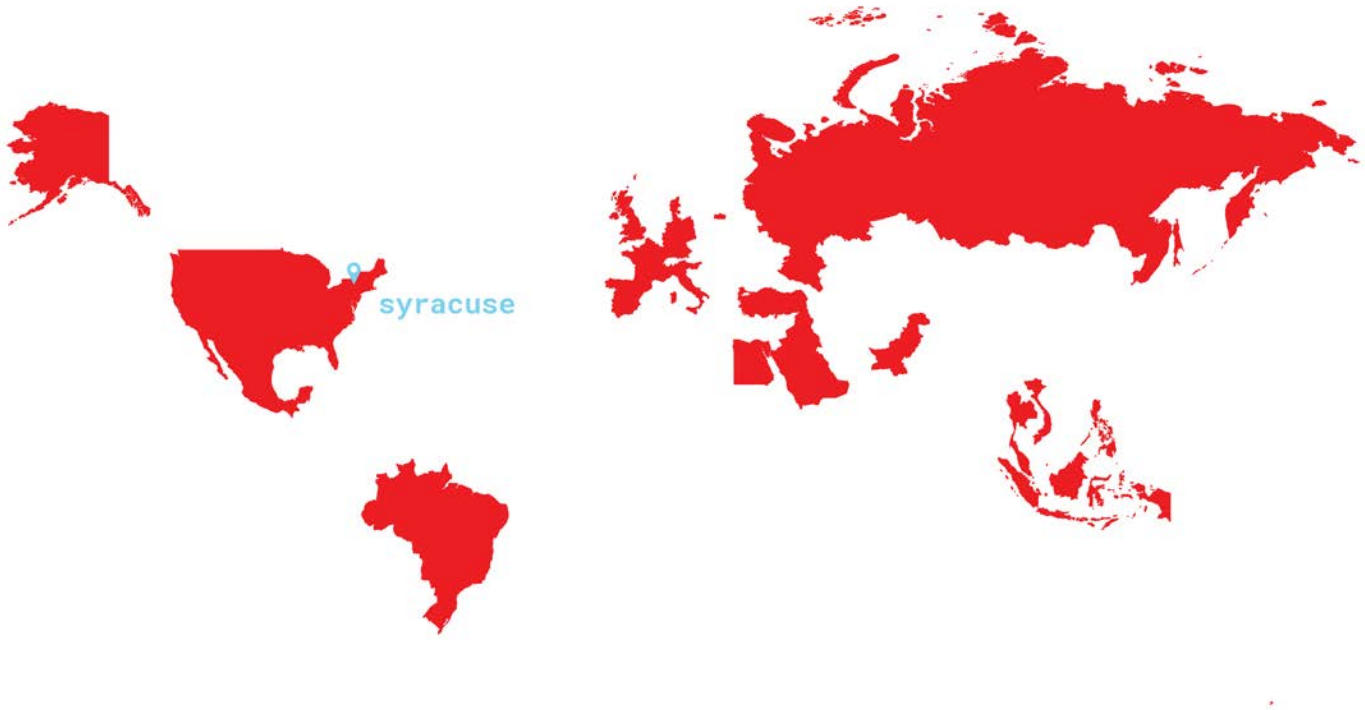The United States
other countries

Aug.2022

Tik Tok

ByteDance

Tiktok is a popular short-video-sharing platform owned by the Chinese company ByteDance. It contains a variety of user-submitted videos with lengths ranging from 15 seconds to ten minutes, including pranks, stunts, tricks, jokes, and dancing.

TikTok has received criticism for its addictive qualities and other psychological impacts, as well as for issues with censorship and moderation, and user privacy.

Political Control

● owned by Chinese company ByteDance
● Political Manipulation + Tik Tok Partnered with Oracle

User Distribution

syracuse
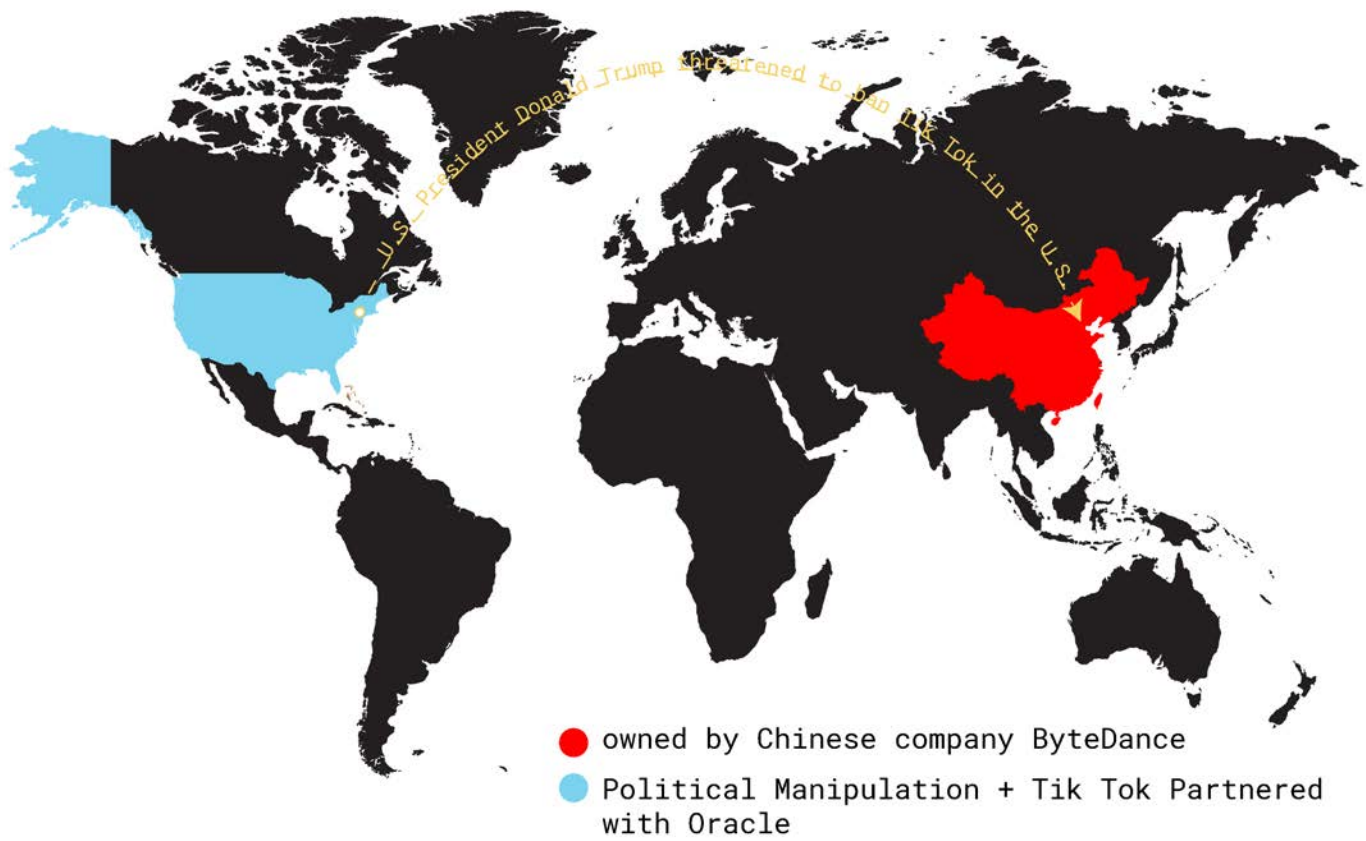
Monthly Active Users: 1.000 Billion (July 2022)

unit: million

140.6 1. The United States
       2. Indonesia
       3. Brazil
       4. Russian Federation
       5. Mexico
       6. Vietnam
       7. The Philippines
       8. Thailand
       9. Turkey
25.2   10. Saudi Arabia

May.2022
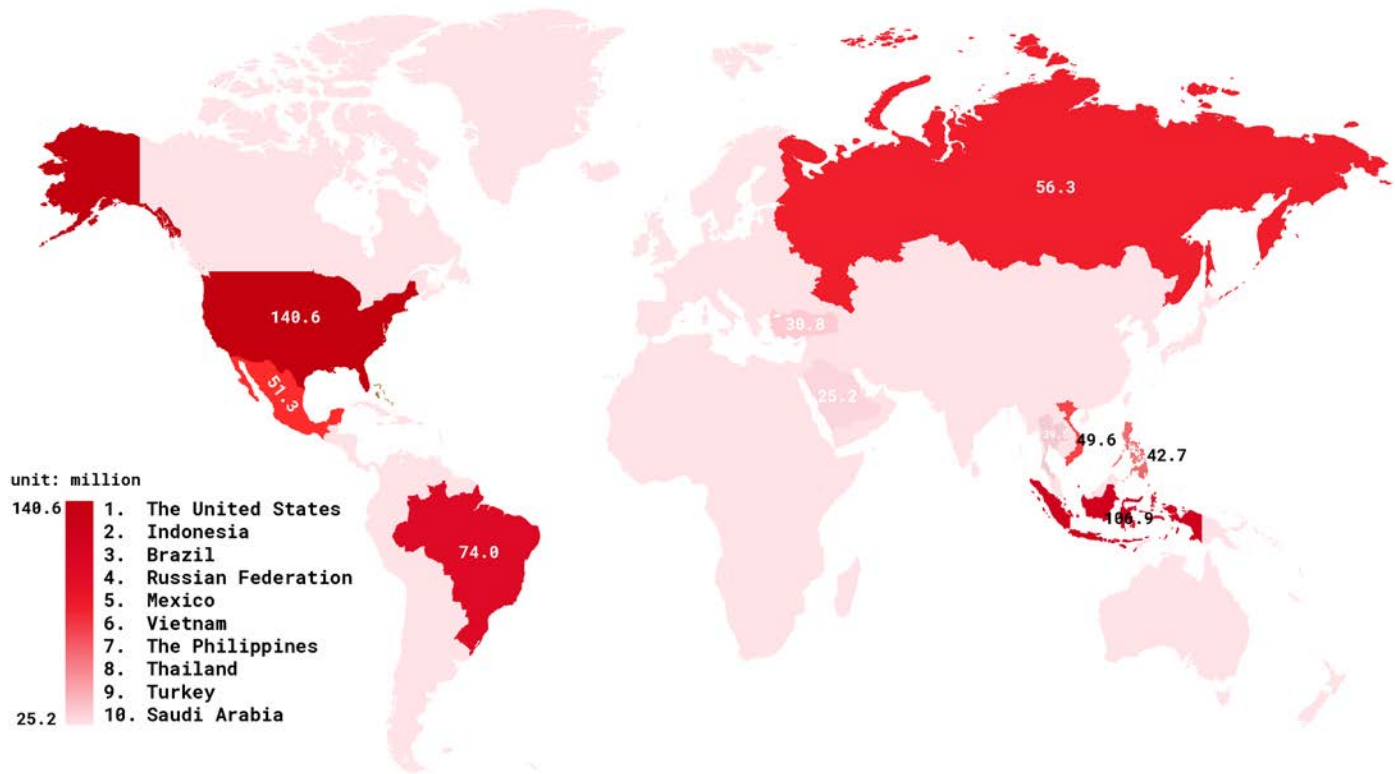
Viber

Rakuten Group Inc.

Viber is a free social media app that users can send messages, photos, videos, and make video calls to other Viber users. It has over 260 million active users, and its users are mainly from Europe.
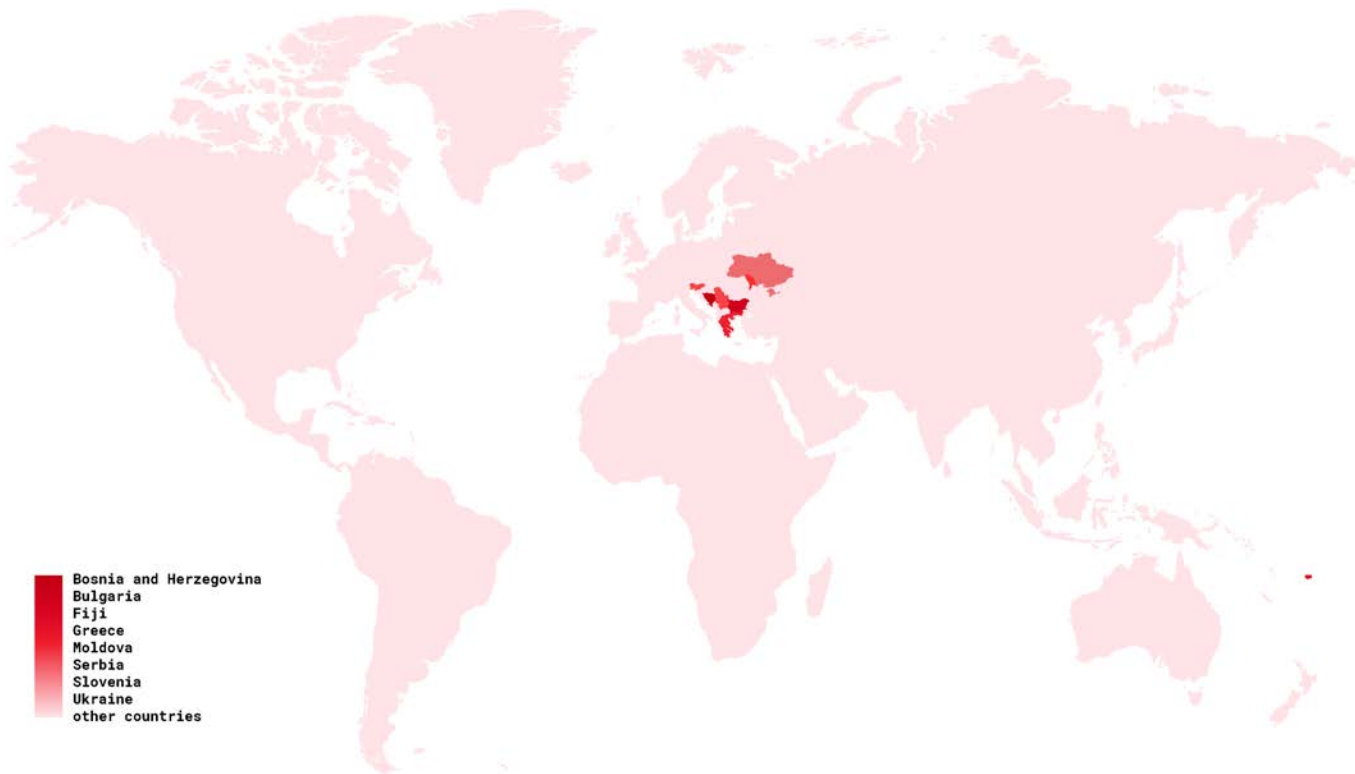
● owned by Japanese multinational company Rakuten Group Inc.

User Distribution

syracuse

Monthly Active Users: 260 Million

Bosnia and Herzegovina
Bulgaria
Fiji
Greece
Moldova
Serbia
Slovenia
Ukraine
other countries

Jun.2022

WeChat

Tencent

WeChat is an instant messaging app with 1 billion monthly active users around the world. It also includes other functions such as mobile payment, mini programs, text/photo sharing.

Political Control

- 🔴 Owned by Chinese multinational company Tencent Government surveillance
- 🔵 Political Manipulation
- 🟣 Global Cencorship

User Distribution

syracuse
1000+
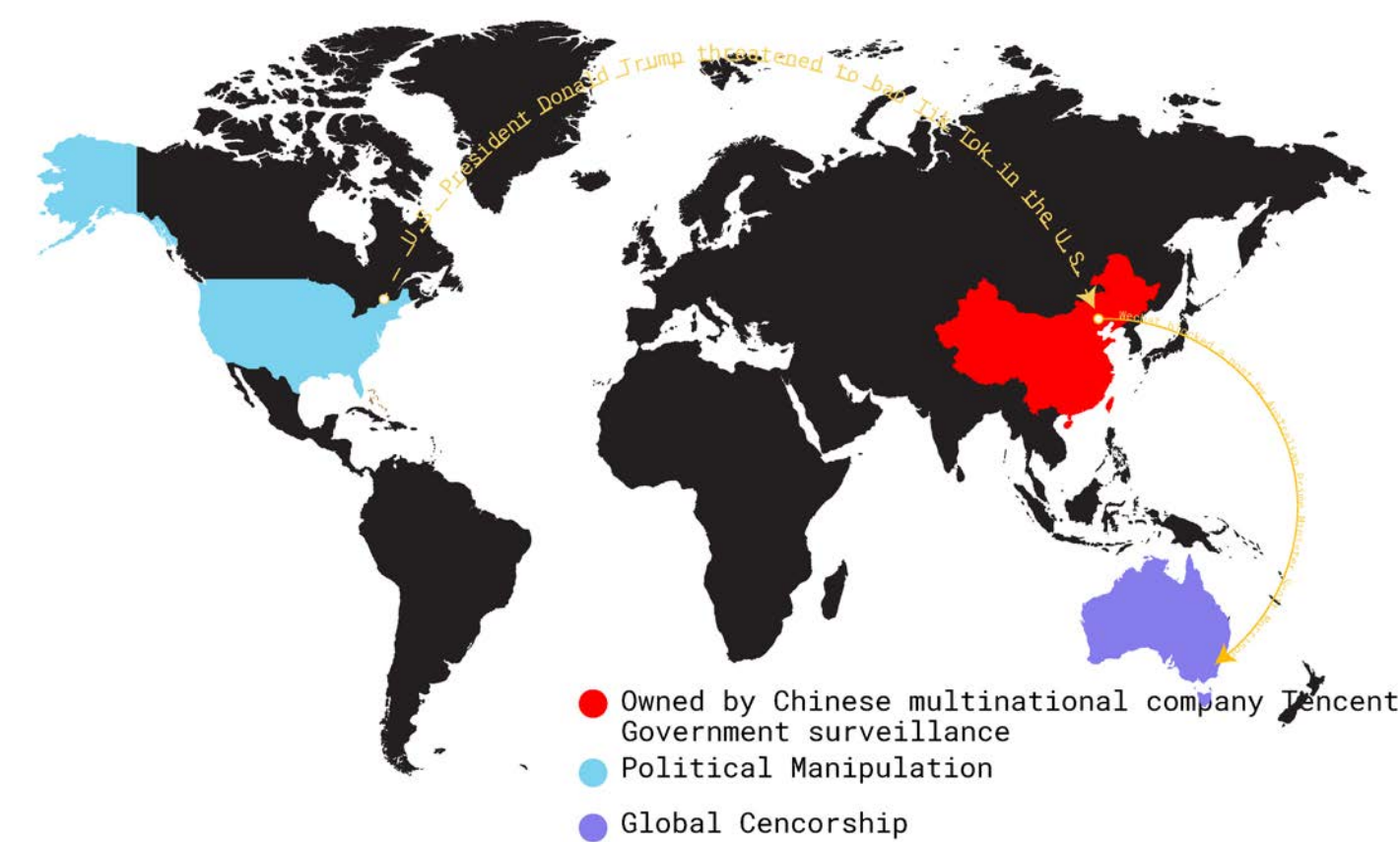
Monthly Active Users: 1.299 Billion (2022)

unit: million
1000+ China

100-200 other countries

Jun.2022

syracuse
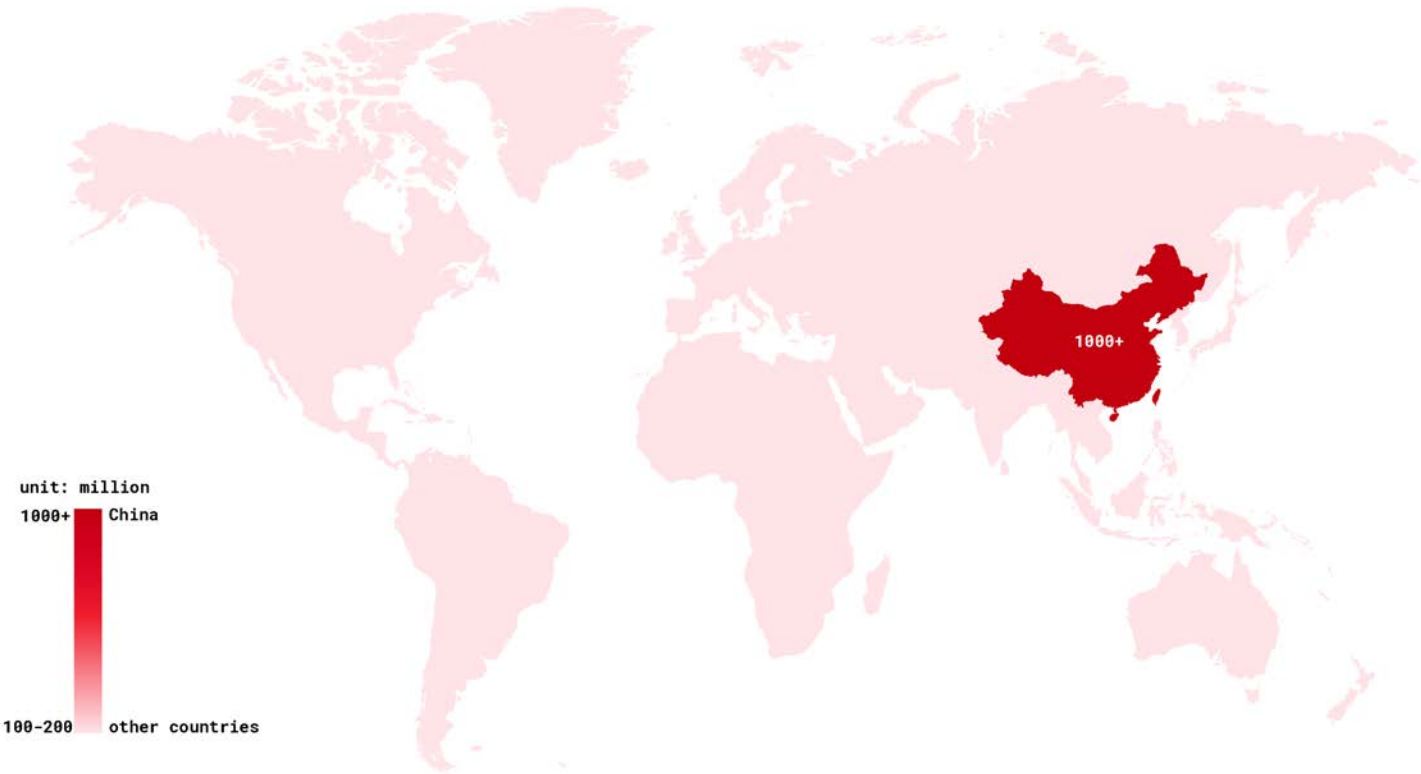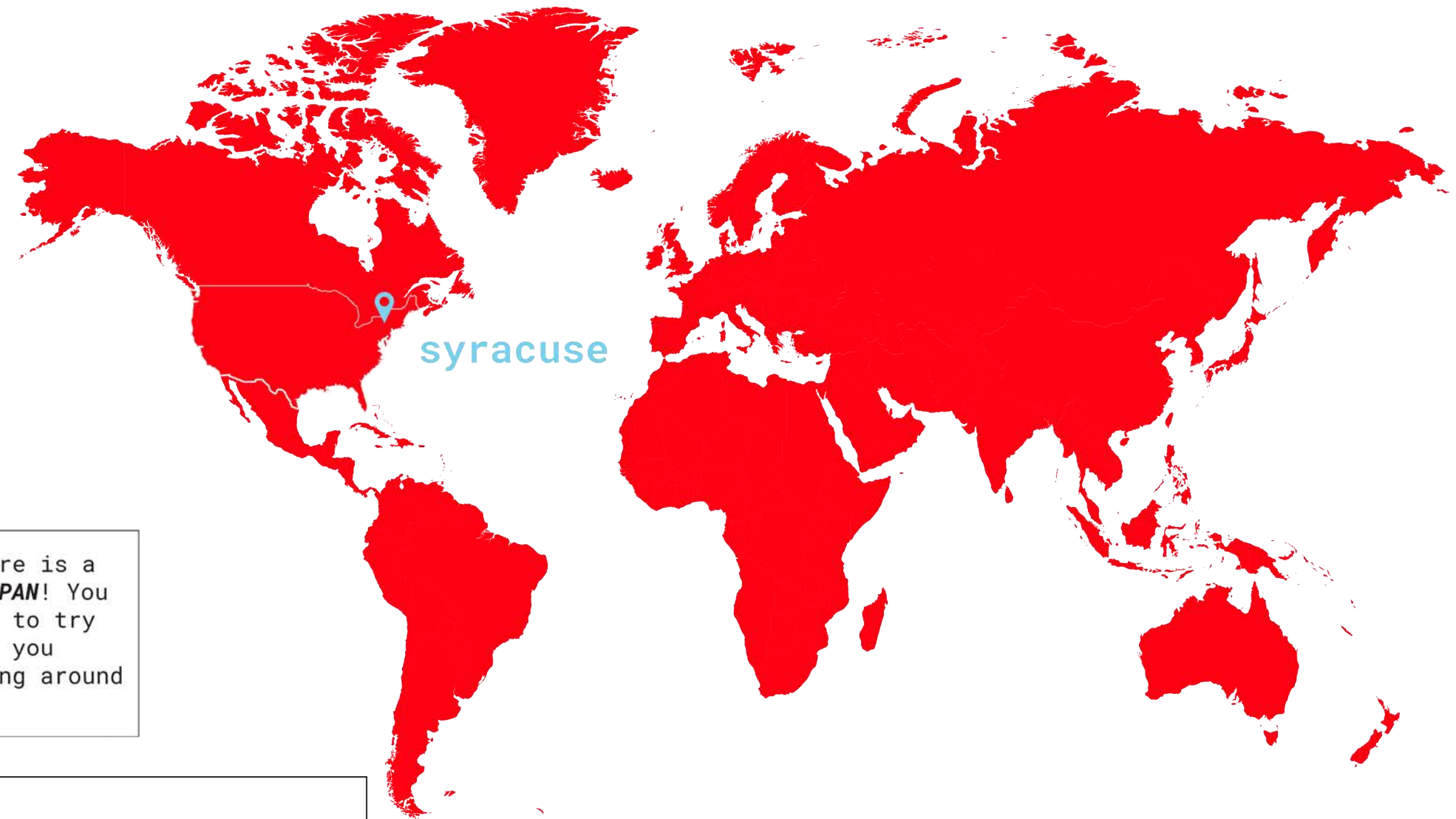
Hey wendy.w, here is a new app called *PAN*! You definitely want to try this! It allows you access everything around the world.
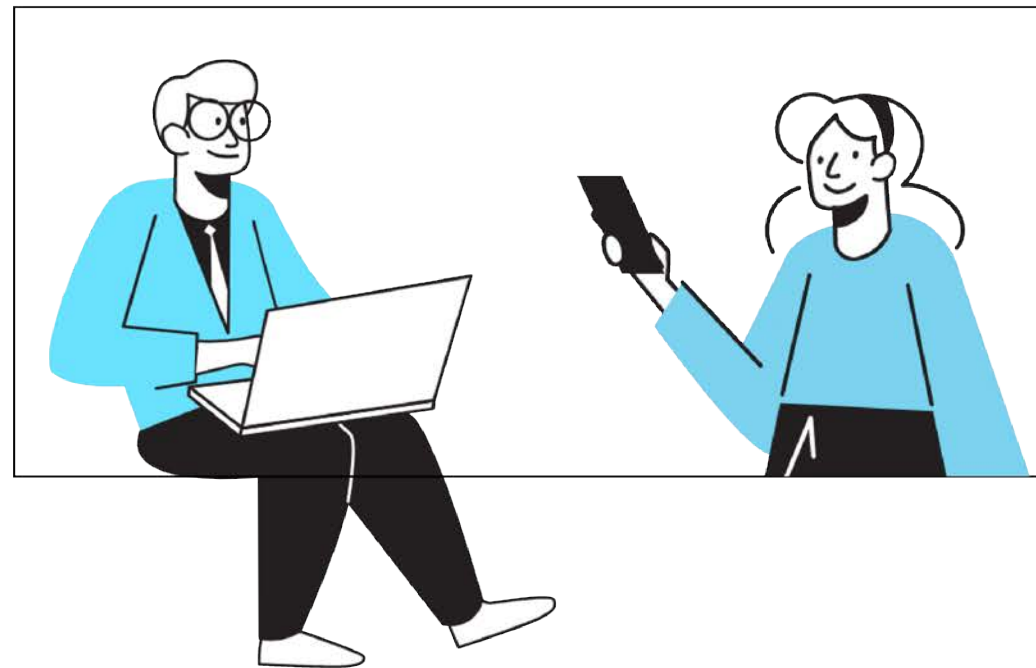
Chapter 03

REVELATION

By using our services, users have to click agree on the user agreement, which we assume people will just scroll down to the bottom and not read a single word. But it reveals our true project. This entire narrative is actually describing a data panopticon, which is the true meaning behind "pan". Our true intent is to design an apocalyptic narrative, in which people's privacy is deprived to an extreme. We want to use this project to address the importance of privacy.

pan

"Just agree, no one cares about your privacy"

click **Agree**.

Ok, this is long enough, you probably get tired reading this already. I mean, who even read these Agreements? It's not like you can do anything after reading this right? Yeah, you don't really have a choice, to be honest. We even find this document too boring to read, and it is too boring to write as well. Just scroll to the bottom and click agree. If you are unwilling or unable to be bound by these Terms, sure you can opt out anytime, but oh poor man, we will erase all your previous memories and identities that are connected to our microchip implant, and you won't be able to use these amazing apps that everyone in this world is using! Can you really afford being left out of this technological world? Come on, just, I mean, just stop reading already, click agree, easy peasy lemon squeezy.

Yes, this is really happening. This means through this little chip inside your brain, we are able to monitor and know everything about you. We know all your sense, how you feel, and even what you are thinking. Read on, if you are still reading, which I highly doubt, and you will discover more about how we use your data. It's fun.

How else could we possibly obtain all of your personal information? Of course the little chip would send it back to our server and we can store it.

Not only do we know you, we also know your next moves! Sounds a little scary and insecure, but hey, think of it the good way. We plan things for you! You don't need to worry about your life anymore, what a relief! Let us take control.

Yes, you've read it right. It's our data. We reserve the right to use, modify, copy, share, display the data. Again, I've said it once and I'll say it again, there is nothing you can do. We can do anything we want with our data.

What do you think? You are sharing it! Doesn't matter who you are sharing to honestly, you are sharing with us ultimately.

Yeah, I know you probably don't care about what kind of information we collect, and I'm too lazy to list all of them. There's a whole range of them. And you know what, there is no way you've read this far. Well, if you do, let me tell you more.

How do you think we make money while providing you with this lifelong predictive service for free? We are not philanthropists. We will sell your information to others if profitable.

Remember that we know what you are thinking. If you are attempting to commit a crime, we will predict that and there is a chance that we report to the law enforcement, depending on whether we want or not.

As we stated above, we have the right to do whatever we want with your information. But if it is stolen or hacked, well, unfortunately there is nothing we can do, and we do not hold the responsibility.

You can't sue us, ever, for any reason!

You really think we would give the money back to you once we have it?

Yes, it is really our products, our money, our everything. Imagine if you opt out from our services, you wouldn't be able to use Pandora Pay which everyone is using for paying. How are you going to buy things? No one uses cash anymore.

you do not legally own them. We may modify, suspend, eliminate, or substitute virtual items at any time and in our sole discretion. Even if you choose to terminate our service, you are not permitted to a refund.

I'd be surprised if you actually read this far. Anyways, we do not care if you want to stop using our Apps and the little chip that tracks you. We only care about your data and the profit it brings. And guess what, if you choose to opt out, you don't get to keep a single bit of your information. I know it is hard starting your life all over again and finding out you don't even fit into this society that's entirely technologically driven. So why bother? Just sit back, relax, and accept our service.

Yes, yes, yes, that's right. We can change this Agreement how ever we want and there is absolutely nothing you can do. And we don't even have to tell you. Once you click agree, it is all done, no need to worry about anything. Let the professionals handle the business here my dear users. And I bet you won't even read this last sentence. You just scrolled down to the very bottom right?

Agree

pan

opticon

Bibliography

Bell, Michael F. *The Invisible Crime: Illegal Microchip Implants and Microwave Technology, and Their Use against Humanity.* Brighton Pub. LLC, 2011.

Foucault, Michel. ""Panopticism" from *Discipline & Punish: The Birth of the Prison." Race/Ethnicity: Multidisciplinary Global Contexts 2*, no. 1 (2008): 1-12. muse.jhu.edu/article/252435.

Fuchs, Christian. "Karl Marx in the Age of Big Data Capitalism." In *Digital Objects, Digital Subjects: Interdisciplinary Perspectives on Capitalism, Labour and Politics in the Age of Big Data*, edited by Christian Fuchs and David Chandler, 53–72. University of Westminster Press, 2019. http://www.jstor.org/stable/j.ctvckq9qb.6.

Hern, Alex. "Fitness Tracking App Strava Gives Away Location of Secret US Army Bases." The Guardian. Guardian News and Media, January 28, 2018. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

Johnston, Bryan. "A Brief History of Surveillance Cameras." Deep Sentinel, September 14, 2022. https://www.deepsentinel.com/blogs/home-security/history-of-surveillance-cameras/.

"Instagram Apks." APKMirror. Accessed December 16, 2022. https://www.apkmirror.com/apk/instagram/instagram-instagram/.

"Line Revenue and Usage Statistics (2022)." Business of Apps, June 30, 2022. https://www.businessofapps.com/data/line-statistics/.

Magazine, Smithsonian. "A Brief History of Surveillance in America." Smithsonian.com. Smithsonian Institution, April 1, 2018. https://www.smithsonianmag.com/history/brief-history-surveillance-america-180968399/.

McLeod, Saul. "Pavlov's Dogs Study and Pavlovian Conditioning Explained." Simply Psychology, January 1, 1970. https://www.simplypsychology.org/pavlov.html#:~:text=Pavlov%20showed%20that%20dogs%20could,an%20unconditioned%20(innate)%20response.

Mcleod, Saul. "The Little Albert Experiment." Little Albert Experiment - Simply Psychology, October 18, 2018. https://www.simplypsychology.org/little-albert.html.

Megele, Claudia, Peter Buzzi, and Anne Longfield. "Online Identity, Digital Citizenship and Boundaries." In Safeguarding Children and Young People Online: A Guide for Practitioners, 1st ed., 25–46. Bristol University Press, 2018. https://doi.org/10.2307/j.ctt1x76gnp.8.

O'Connor, Nuala, Alethea Lange, and Ali Lange. "Privacy in the Digital Age." *Great Decisions*, 2015, 17–28. http://www.jstor.org/stable/44214790.

Richterich, Annika. "Big Data: Ethical Debates." In *The Big Data Agenda: Data Ethics and Critical Data Studies*, 6:33–52. University of Westminster Press, 2018. https://doi.org/10.2307/j.ctv5vddsw.5.

Sehl, Katie. "What Is the Line App? Everything Brands Need To Know." Social Media Marketing & Management Dashboard, August 18, 2022. https://blog.hootsuite.com/line-app/.

Shafer, Jack. "Opinion: What Critics of the Hottest Social Media App Don't Get." POLITICO. Accessed December 16, 2022. https://www.politico.com/news/magazine/2022/10/18/tiktok-defense-internet-addiction-00062143.

Stouffer, Clare. "The Privacy Paradox: How Much Privacy Are We Willing to Give up Online?" Norton, April 14, 2021. https://us.norton.com/blog/privacy/how-much-privacy-we-give-up#.

Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Public Affairs, 2020)

"The Latest Instagram Statistics: Everything You Need to Know - Datareportal – Global Digital Insights." DataReportal. Accessed November 11, 2022. https://datareportal.com/essential-instagram-stats.

"WhatsApp 2022 User Statistics: How Many People Use Whatsapp?" Backlinko, January 5, 2022. https://backlinko.com/whatsapp-users.