likes follower debts comments locations time account data health political opinions sexual hobby orientation social media job references origin misdemeanors genetics address phone number id e-mail insurance income job family religion

#Inhalt

Inhalt

05 Team
11 Einführung
32 Vom Konzept zum Design
52 Technik
70 Management
92 Team_v2
95 Literaturverzeichnis

Abstract: {

Personal data, especially the data we carelessly share on social networks, is sensitive data with a high potential for misuse. Combined, this data can provide a very accurate profile of a person. The users are not aware of the mass of shared data, who has access to it, and what it could be misused for.
The Ambient Intelligent Space You confronts the users of social networks with their data and tries to shock and inspire them to think. The user lives through the experience of a stalked person while You represents the stalker as social networks.

}

Team: {

Name: **„Domenika Tomasovic“,**
Alter: **23,**
Wohnort: **„Kimbach“,**
Geschlecht: **„Weiblich“,**
Suchmaschine: **„Google“,**
Soziale Netzwerke: **[„Instagram“, „Facebook“],**
Lieblingsapps: **[„Instagram“, „Spotify“, „WhatsApp“],**
Paranoia vor Datenmissbrauch: **20%,**

Name: **„Elina Margheritta Faber“,**
Alter: **23,**
Wohnort: **„Darmstadt“,**
Geschlecht: **„Weiblich“,**
Suchmaschine: **„Google“,**
Soziale Netzwerke: **[„Instagram“, „Youtube“, „Twitter“],**
Lieblingsapps: **[„Instagram“, „Youtube“, „Todoist“, „Spotify“],**
Paranoia vor Datenmissbrauch: **15%,**

Name: **„Jan Meininghaus“,**
Alter: **23,**
Wohnort: **„Darmstadt“,**
Geschlecht: **„Männlich“,**
Suchmaschine: **„Google“,**
Soziale Netzwerke: **„Instagram“,**
Lieblingsapps: **[„Youtube“, „Spotify“, „Reddit“, „WhatsApp“],**
Paranoia vor Datenmissbrauch: **30%,**

Name: **„Sarah Lerch“,**
Alter: **26,**
Wohnort: **„Rödermark“,**
Geschlecht: **„Weiblich“,**
Suchmaschine: **„DuckDuckGo“,**
Soziale Netzwerke: **„Facebook“,**
Lieblingsapps: **[„Whatsapp“, „Spotify“, „Pinterest“],**
Paranoia vor Datenmissbrauch: **70%,**
}

Glossar: {

Globale Datasphäre:
Zusammenschluss der drei primären Schauplätze der Digitalisierung: den Kern (traditionelle und Cloud-Rechenzentren), der Rand (unternehmensgehärtete Infrastruktur wie Mobilfunkmasten und Niederlassungen) und die Endpunkte (PCs, Smartphones und IoT-Geräte). Die Summierung all dieser Daten wird als globale Datensphäre bezeichnet (Reinsel, Gantz, & Rydning, 2018).

Social Media:
Social Media bieten den Nutzenden einen Ort zum Austausch und ermöglicht einen leichten Zugang zu Informationen aller Art im Internet (Schmidt, 2018).

Social Engineering:
„Social-Engineering ist eine Angriffsstrategie, die nicht die Technik als Opfer auserkoren hat. Stattdessen wird hier viel lieber – und vor allem effizienter – der Mensch bzw. sein Verhalten angegriffen.“ (Schumacher, 2014)

Social Bot:
Softwareprogramme, die darauf abzielen, menschliche Social-Media-Nutzer auf Plattformen wie Facebook, Twitter und Reddit nachzuahmen (Woolley, 2016).

MQTT:
MQTT (Message Queuing Telemetry Transport) ist ein Kommunikationsprotokoll. Es ist so konzipiert, dass es offen, einfach, leicht und einfach zu implementieren ist (Tang et al., 2013).

RSSI:
RSSI steht für Received Signal Strength Indicator und beschreibt die empfangene Signalstärke eines Gerätes (Srinivasan & Levis, o. J.).

SSL:
Secure Socket Layer (SSL) ist das beliebteste Protokoll im Internet, um eine sichere Kommunikation zu ermöglichen (Kant, Iyer, & Mohapatra, 2012).

MAC:
„Die Media Access Control Adresse (MAC-Adresse) ist eine einzigartige Hardwareadresse jedes Netzwerkadapters, wodurch jedes Gerät eindeutig identifizierbar ist.“ (Dr. Datenschutz, 2015)

Whistleblower:
Ein Whistleblower ist eine Person, die illegale oder unzulässige Regierungsaktivitäten belegt (Kessler, 2008).

Facial Recognition:
Facial Recognition, zu Deutsch Gesichtserkennung, ist eine Kategorie biometrischer Software, die die Gesichtsmerkmale einer Person mathematisch abbildet und die Daten als Faceprint speichert. Die Software verwendet Deep-Learning-Algorithmen, um eine Live-Aufnahme oder ein digitales Bild mit dem gespeicherten Faceprint zu vergleichen, um die Identität einer Person zu überprüfen (Rouse, o. J.).

Stalking:
Stalking bezeichnet das „wiederholte Verfolgen und penetrante Belästigen oder Terrorisieren einer Person gegen deren Willen.“ (Polizei Bayern, o. J.)
}

Szenario: {

Es ist Freitagmorgen. Du öffnest langsam deine Augen, nimmst wie jeden Morgen dein Handy in die Hand, entsperrst es mit deinem Herzschlag und checkst Facebook, Instagram, Twitter, Pinterest und LinkedIn. Außerdem schaust du dir deine Blutwerte an, nachdem du dir gestern Abend in der Bar einen Drink zu viel gegönnt hast. Du bist genervt, weil du dir diesen Monat so viel zu Schulden kommen lassen hast. Du willst gar nicht wissen, wie hoch die Versicherungsbeiträge dieses Mal ausfallen. So richtig motiviert warst du diese Woche nicht. Ganz anders war das noch vor drei Monaten, als du dir die Apple Watch im Angebot geholt hast. Ein paar Mal die Woche Sport für so ein cooles Teil, wer kann da schon widerstehen? Die Instagram Werbung war einfach zu verlockend. Wer hätte denn ahnen können, dass die Motivation durch regelmäßigen Alkoholkonsum und nettes Beisammensein mit den Kollegen von der neuen Arbeit abgelöst werden würde?

Die Gehaltserhöhung hättest du dir bei den Krankenkassenbeiträgen und der Apple Watch Nachzahlung sparen können. Aber so ist das heutzutage nunmal… Du stehst aus deinem Bett auf, stellst dich auf deine smarte Waage und deine Laune wird nicht gerade besser. Jeden Tag ein Feierabendbier macht sich schneller bemerkbar als gedacht. Es klingelt an der Tür. Der Postbote bringt dir ein Packet, du nimmst es an. Im Wohnzimmer angekommen, fragst du Alexa, was sie dieses Mal bestellt hat. Diese antwortet schnippisch: „Bevor du nächste Woche wegen einer Männergrippe rumheulst, habe ich dir Hustenbonbons und Grippostat bestellt.“ Du fragst sie, wie sie auf die Idee kommt, dass du krank wirst. Sie entgegnet, du seist nur am schniefen und hustest vor dich hin. Außerdem hättest du gestern Nacht schon Fieber gehabt. Du sparst dir die Diskussion, packst die Medikamente in den Badschrank und fängst an dich für die Arbeit fertig zu machen.

Fertig angezogen packst du deine Sporttasche, denn auch deine Fitnessstudio Beiträge schießen in die Höhe, wenn du heute keine Instastory aus dem Studio postest. Im Zug denkst du darüber nach, wie aus einer Apple Watch und einer kleinen Fitness App auf deinem Handy so etwas werden konnte. Du schaust dir dein Genom auf deinem Handy an, denn auch dieses hast du mittlerweile immer dabei. Du schaust verträumt aus den Fenster und fragst dich, wo zwischen all diesen vielen Chromosomen deine Privatsphäre geblieben ist.

Im Büro angekommen, findest du in deinem Terminkalender ein Gespräch mit deinem Chef. Hätte dir mal vorher jemand gesagt, dass dein Alkoholkonsum und die fehlende Motivation Sport zu treiben zu einer Kündigung führen könnten, dann hättest du dein Handy beim Bier trinken zuhause gelassen.

author: { dt }
}

Ethische Absicht: {

Das Projektteam ist sich bewusst, dass das nachfolgend beschriebene Projekt gegen ethische Regeln verstößt. Mit Hilfe dieses Projekts soll jedoch Aufmerksamkeit erregt werden, um darzustellen wie wichtig die Sicherheit von personenbezogenen Daten ist. Über die Massen an Daten, die durch das Projekt gesammelt werden, hat das Team ein genauen Überblick und ein großes Verständnis. Daher handhabt es diese mit Vorsicht und Voraussicht. Daten werden nur für die Durchführung des Projekts verwendet und danach unwiderruflich gelöscht.

Die Absicht dieses Projekts besteht darin, den Menschen zu zeigen, wie einfach es sein kann an scheinbar „unwichtige“ Daten zu gelangen, die jedoch in der Masse und richtigen Kombination viel über eine Person aussagen können.

author: { jm }
}

#Einführung

Einführung

12 Personenbezogene Daten
16 Trust
18 Datenerhebung
19 Gefahrenpotenzial
20 Datenmissbrauch
24 Quiz
26 Aufklärung und Schutzmaßnahmen
28 Einblick in andere Länder

Personenbezogene Daten: {

Die Gesellschaft befindet sich seit 20 Jahren in einem beschleunigten gesellschaftlichen Wandel, ausgelöst durch die Automation und Digitalisierung. Diese Umwandlungsprozesse bringen viele Veränderungen mit sich, darunter die größer werdenden Mengen an entstehenden personenbezogene Daten (Wittpahl, 2017).
Personenbezogene Daten sind laut DSGVO „[...] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche [...] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.“ (Europäischen Union, 2018)
Teilweise werden diese Daten durch Dritte erhoben, oft aber geben Personen Daten über sich selbst frei um bestimmte Services entgegenzunehmen, online soziale Kontakte zu pflegen oder sich anhand erhobener Daten selbst zu optimieren.
Heute interagieren mehr als 5 Milliarden Verbraucher täglich mit Daten - bis 2025 werden es 6 Milliarden sein, was 75% der Weltbevölkerung entspricht.
Im Jahr 2025 wird jede mit dem Internet verbundene Person alle 18 Sekunden mindestens eine Dateninteraktion haben. Viele dieser Interaktionen sind auf die Milliarden von IoT-Geräten zurückzuführen, die weltweit verbunden sind und die 2025 voraussichtlich über 90 Zettabyte (Ein Zettabyte ist gleich 10^{12} = 1,000,000,000,000,000,000,000 Bytes (Van Der Aalst, 2016)) an Daten erzeugen werden (Reinsel, Gantz, & Rydning, 2018).
Insgesamt werden die Datenmengen für 2025 auf 175 Zettabyte geschätzt. Zur Verbildlichung: Würde eine Person die gesamte *globale Datasphäre* 2025 mit durchschnittlich 25 Mb/s Verbindungsgeschwindigkeit herunterladen, würde es 1,8 Milliarden Jahre dauern. Würden alternativ alle Menschen auf der Welt helfen und sich nie ausruhen, dann könnten Sie in 81 Tagen alle Daten herunterladen (Reinsel, Gantz, & Rydning, 2018).
Die Relevanz von personenbezogenen Daten nimmt zu, was auch die Zahlen der minütlich kreierten Datenmengen im Bereich *Social Media* zeigen: Jede Minute werden 49 Tausend Videos auf Instagram hochgeladen, 473 Tausend Tweets geteilt und etwa zwei Millionen Snaps in Snapchat verschickt (Domo, 2018). Von den

Weltweit etwa siebeneinhalb Milliarden Menschen sind dreieinhalb Milliarden aktive *Social Media* Nutzende (Hootsuite, 2019). Nicht nur durch Beiträge entstehen riesige Datenmengen, auch alle Klicks und Interaktionen der Nutzer werden getrackt und hinterlassen Daten (Sears, 2018).
Öffentlich zugängliche *Social Media* Daten können tiefe Einblicke in das Leben der Nutzenden preisgeben. Informationen aus dem eigenen Profil in Kombination mit den Profilen der Freunde, Familie, Mitarbeitenden und Bekannten geben mehr Einblicke frei, als es den meisten Nutzenden bewusst ist. Diese Daten sind so sensibel, da sie detaillierte Informationen darüber enthalten, wann und wo der Nutzende war, mit wem er/sie zusammen Zeit verbringt, Freundeslisten, die die Stärke und Art der sozialen Bindungen widerspiegeln, und welche Art von Inhalten präferiert und „geliked“ werden. Diese Profile identifizieren den Nutzenden oft eindeutig (Things, 2018).
Aber nicht nur online werden personenbezogene Daten erhoben, auch offline werden wie in dem Pilotprojekt des Berliner Bahnhof Südkreuz Personen mittels automatischer Gesichtserkennung durch 74 Kameras getrackt und ihre Handlungen durch künstliche Intelligenz interpretiert. So kann beispielsweise das Verhalten einer Gruppe von Menschen beobachtet und eingegriffen werden, falls eine Menschenmasse sich ungewöhnlich verhält („Gesichtserkennung“, 2018).

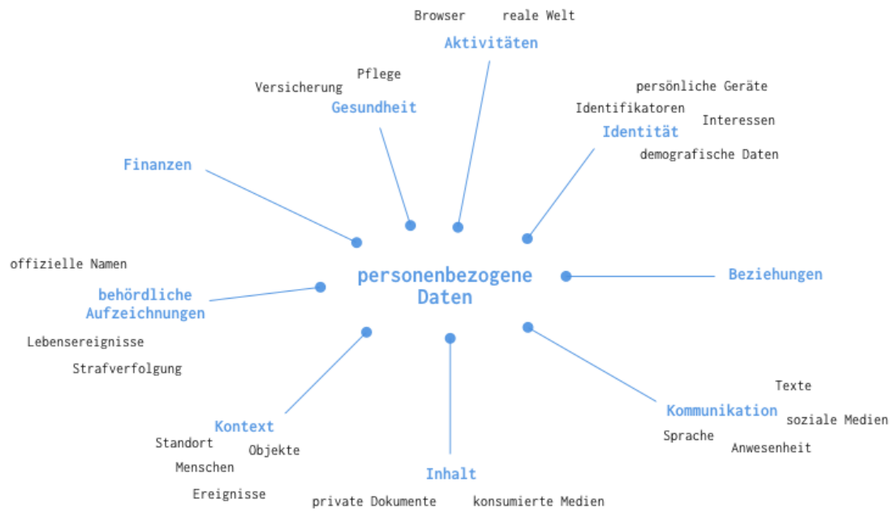


Abb.1: {Mindmap - personenbezogene Daten}

Durch die Datenschutz-Grundverordnung (DSGVO), die 2018 in Kraft getreten ist, wurde festgelegt, dass die Verarbeitung von personenbezogenen Daten dann rechtmäßig ist, wenn mindestens einer der folgenden sechs Kriterien erfüllt ist:

1. Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

2. die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Ver tragspartei die betroffene Person ist, oder zur Durchführung vor vertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

3. die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

4. die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

5. die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

6. die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.(Europäischen Union, 2018)

Besonders der erste Punkt ist interessant. Bei der Registrierung auf *Social Media* Plattformen wie Instagram und Facebook muss der Nutzende erst der Einwilligungserklärung zustimmen, andernfalls kann er die Plattform nicht nutzen. Bei Instagram stimmt man beispielsweise zu, dass von einem selbst bereitgestellte Informationen und Inhalte (Beiträge, Nachrichtenaustausch aber auch Metadaten wie Aufnahme-Standort eines Fotos oder das Datum) erfasst und verarbeitet werden dürfen. Desweiteren werden alle Informationen bezüglich der Nutzung der Anwendung getrackt. Instagram schreibt in ihren Richtlinien dazu „Zum Beispiel protokollieren wir, wenn du unsere Produkte gerade nutzt bzw. wann du diese zuletzt genutzt hast, und welche Beiträge, Videos und sonstigen Inhalte du dir in unseren Produkten ansiehst. Wir erfassen auch Informationen darüber, wie du Funktionen wie unsere Kamera nutzt.“ („Instagram Datenschutzrichtlinie“, o. J.) Alle diese Daten werden gesammelt um eine Bereitstellung, Personalisierung und Verbesserung der Produkte zu ermöglichen, worunter auch Standortbezogene Informationen, Werbeanzeigen und andere gesponserte Inhalte fallen („Instagram Datenschutzrichtlinie“, o. J.).

author: { ef }
}

Zuck: Yeah so if you ever need info about anyone at Harvard

Zuck: Just ask.

Zuck: I have over 4,000 emails, pictures, addresses, SNS

[Redacted Friend's Name]: What? How'd you manage that one?

Zuck: People just submitted it.

Zuck: I don't know why.

Zuck: They "trust me"

Zuck: Dumb fucks.

Datenerhebung: {

Personenbezogene Daten können mittels vieler Methoden erhoben werden. Darunter fällt die Bilder- und Videoanalyse, die Textanalyse, Social-Engineering und Hacking.
Die Analyse von Bild- und Videomaterial findet schon in vielen Bereichen Anwendung. Mit dem Cloud Vision Produkt von Google können beispielsweise mittels maschinellem Lernen (ML) einzelne Objekte, gedruckte Wörter und Gesichter in Bildern erfasst und automatisch Tausenden von Kategorien zugeordnet werden (Google, o. J.).
Auch Texte können mit Hilfe von ML analysiert werden. Ein Anbieter für diesen Service ist Microsoft mit ihrer Softwareplattform Azure. Ein Service dieser Plattform ist die Stimmungsanalyse. „Diese Funktion ermöglicht die Erkennung positiver und negativer Standpunkte in sozialen Medien, Kundenbewertungen und Diskussionsforen." (aahill, o. J.)
„Social-Engineering ist eine Angriffsstrategie, die nicht die Technik als Opfer auserkoren hat. Stattdessen wird hier viel lieber – und vor allem effizienter – der Mensch bzw. sein Verhalten angegriffen." (Schumacher, 2014)
Menschen durch gezielte Manipulation zu etwas zu bewegen ist nichts Neues, jedoch haben sich durch die Digitalisierung und die Menge an personenbezogenen Daten die Möglichkeiten vervielfältigt. Ziel dieses Angriffs ist es durch das Ausnutzen menschlicher Schwachstellen wie Stress und Zeitdruck an sensible Daten wie Zugangsdaten zu geschützten Systemen zu gelangen. Phishing ist eine Form des Social-Engineering, bei der ein Angreifer versucht, betrügerisch sensible Informationen von einem Opfer zu erlangen, indem er sich als vertrauenswürdiger Dritter ausgibt (Jagatic, Johnson, Jakobsson, & Menczer, 2005).
Die wohl aggressivste Form der Datenerhebung ist das Hacking. „Das Wort „hacken" wird heute meist abwertend für den Prozess gebraucht, gegen den Willen des Besitzers in dessen Computer-System, Netzwerk oder Software einzubrechen […]." (Chatfield, 2013)
Es kann zwischen verschiedenen Arten von Hackern unterschieden werden: „White Hats", „Black Hats", „Grey Hats", „Hacktivisten", „Skript-Kiddies" und „Blue Hats".
Die „White Hats" sind Hacker, die Systeme nur hacken um die Sicherheit zu testen. Ihnen werden wohlwollende Absichten zugesprochen. Die „Black Hats" sind genau das Gegenteil: Ihnen geht es nur um Profit und sie scheuen sich nicht vor bösartigen Praktiken (Chatfield, 2013). Die „Grey Hats" bewegen sich zwischen diesen beiden Extremen. Sie verschaffen sich auch illegal Zutritt zu Systemen, verfolgen jedoch keine bösen Absichten und legen nach dem Hack auch meist die Sicherheitslücken als Warnung frei (Schilling, 2018). „Hacktivisten" handeln aus ideologischen Gründen und wollen Aufmerksamkeit erzeugen. „Skript-Kiddies" verfügen über keine Vorkenntnisse und lassen automatische Routinen ablaufen um Sicherheitslücken ausfindig zu machen. „Blue Hats" sind sozusagen die professionellen Hacker, da sie offiziell für Computer- oder Sicherheitsfirmen hacken (Chatfield, 2013).

author: { ef }
}

Gefahrenpotenzial: {

Nutzende von digitalen Medien und Geräten hinterlassen Spuren. Überall wird eine Vielzahl von Daten erhoben, deren Missbrauch unterschiedlich große Auswirkungen haben kann. Auf den ersten Blick scheinen insbesondere fiktive Nutzernamen kaum Informationen preiszugeben. Allerdings besteht die Möglichkeit alle Daten, die zu einer E-Mail-Adresse erhoben wurden, zusammenzuführen und damit ein umfassendes Profil des Nutzers zu erstellen. Die Auswirkungen und Gefahren solcher Profile sind vielseitig.

Anhand der Nutzerdaten könnte eine Auswahl beziehungsweise Beurteilung durch Arbeitgeber oder Krankenkassen erfolgen. So wäre im Vorfeld leicht zu überprüfen, ob die Gesundheit, Interessen oder der Umgang mit sozialen Medien des Bewerbers zum Unternehmen passen. Auch könnte aufgrund von Informationen zum Gesundheitszustand der Tarif und Beitrag zur Krankenversicherung angepasst werden. Somit könnten hohe Kosten und Risiken einer Versicherung kalkuliert werden. Das würde allerdings einen Verstoß gegen das Solidaritätsprinzip bedeuten, da nicht jeder für den gleichen Beitragssatz die gleiche Leistung erhält (Burkhardt, 2013). Daher wäre dann auch die gesetzlichen Krankenkassen an das Äquivalenzprinzip der privaten Krankenversicherung angepasst da diese versuchen kostendeckend zu arbeiten. Leistungen können je nach Tarif gewählt werden (AOK, 2016).
Weiterhin könnten diese persönlichen Daten von Hackern und Kriminellen für Identitätsdiebstahl und Betrug genutzt werden. Besonders der Diebstahl von

Kontodaten verursacht erhebliche Schäden. Auch Erpressung wäre bei leichtsinnigem Umgang mit sensiblen Daten im Internet denkbar. Das Gleiche gilt für die Auswertung von Bewegungsprofilen. Diese könnten Orte aufzeigen, die man selbst lieber für sich behalten möchte. Des Weiteren könnten Informationen über den eigenen Standort von Stalkern missbraucht werden. Es wäre jemandem mit den richtigen Kenntnissen und Fähigkeiten vermutlich möglich, einen Menschen auf Schritt und Tritt zu verfolgen.

Durch nicht kontrollierbare Verbreitung von Daten im Internet und illegale Weitergabe an Dritte ist die Nutzung von personenbezogenen Daten bereits heute nicht mehr nachvollziehbar.

author: { sl }
}

Datenmissbrauch: {

Das Daten erhoben und danach weitergegeben werden ist schon lange Realität. Telefonnummern werden an Call-Center verkauft, woraufhin man Anrufe für Umfragen oder einen Spendenaufruf für das Tierheim in Berlin bekommt. Bei E-Mails ist der Spam-Filter nicht umsonst ein hilfreiches Tool. Und personalisierte Werbung auf Webseiten zu einem Produkt, wie Spülmaschine, Schuhen oder Parfüm, das man tatsächlich schon gekauft hat, gibt es wie Sand am Meer.

Die Daten, die online am häufigsten erhoben werden, sind die E-Mail-Adresse und das Passwort. Für die Platzierung von zielgruppengerechter Werbung durch Firmen sind jedoch Nutzerdaten wie die Interessen, Aktivitäten und der Standort der Nutzenden von viel größerem Wert (Banse, 2012). Anhand dieser Daten können Firmen ihre Werbung passend zur Zielgruppen platzieren. Welche Musik eine Person hört, was die Lieblingsserien sind und wo am liebsten Pizza gegessen wird mag einzeln gesehen nicht besonders aussagekräftig sein. In der Masse können solche Daten dennoch einen hohen Wert besitzen.
Facebook trainiert seit 2016 eine künstliche Intelligenz um Nutzendenverhalten immer genauer voraussagen zu können und ihren Werbekunden damit noch genauere Profile, die damit auch teurer werden, anbieten zu können (Krempl, 2018).

Aber was, wenn das Unternehmen Facebook nicht nur die Daten ihres sozialen Netzwerks Facebook nutzt, sondern sie mit den Daten ihrer anderen Dienste wie Instagram und WhatsApp zusammen führt. Angeblich soll dies nicht passieren, letztlich weiß man aber nicht, was der Facebook Konzern mit den Nutzerdaten tut. Alle Daten der Dienste zusammen genommen würden ein umfangreiches Profil der Nutzenden ergeben. Es könnte ein genaues Bild über die sozialen Kontakte, wer die Kontaktpersonen sind und mit welcher Häufigkeit kommuniziert wird, entstehen. Durch die Zusammenführung der Daten der Nutzenden durch Instagram, Facebook und WhatsApp könnte vermutlich ein relativ genaues Geo-Mapping der Person durchgeführen werden. Besuchte Orte, wie das eigene Zuhause, der Arbeitsplatz oder die Wohnung von Freunden wären dadurch ersichtlich. Durch eine Analyse anhand der geteilten Bilder und Stories könnte man bei vielen Nutzenden sicherlich einen erheblichen Teil ihres Lebens rekonstruieren (Data and Things, 2018).

Facebook Skandal:

Bei dem Datenskandal von Facebook und Cambridge Analytica waren 2018 angeblich mehr als 87 Millionen Nutzer weltweit betroffen. Cambridge Analytica erhielt von Facebook Profil-Daten, Freunde und Likes. Diese Datensätze sollen für den Wahlkampf des heutigen US-Präsidenten Donald Trump ausgewertet worden sein. Die Auswertung und Nutzung der Daten geschah ohne die Zustimmung von Facebook. Daraufhin kündigte Facebook eine Überarbeitung ihrer Datenschutzrichtlinien an (Granville, 2018).
Das eigentliche Problem liegt auch hier tiefer. Die Datensätze wurden über eine App innerhalb von Facebook erhoben. Die Nutzenden erlaubten der App auf Profil-Daten, Likes und auch auf die Daten und Likes der Freunde zuzugreifen. So kamen durch 270.000 aktive Nutzende dieser spezifischen App 87 Millionen Nutzerdaten zusammen. Es gibt in den Einstellungen von Facebook die Möglichkeit, die Weitergabe der eigenen Daten an Apps von Freunden zu verbieten. Diese ist allerdings in den Untermenüs nur schwer zu finden. Mittlerweile hat Facebook die Funktion, Daten von Freunden abfragen zu können, entfernt. Verkauft wurden die Daten an Cambridge Analytica von einem externen Entwickler, der Zugriff auf die Datensätze von Facebook hatte. Damit hat er zwar seinen Vertrag gebrochen, dies zeigt allerdings auch, dass Facebook keine Kontrolle über Daten hat, die auf externen Servern landen (Horn, 2018).

Tracken von Laufzeiten und Routen:

Im November 2017 veröffentlichte die Fitness-App Strava eine globale Heatmap mit den Laufdaten ihrer Nutzenden in den Jahren von 2015 bis 2017. Da dort die Daten aller Nutzenden vereint dargestellt werden, ist die Map theoretisch anonym. Allerdings lassen sich andere Daten der App recht einfach auslesen. Erstellt eine nutzende Person eine Route und lädt andere Nutzende ein, kann man über die URL einsehen, wer alles teilnimmt. So kann man zum Beispiel Nutzende und Routen verknüpfen und ein komplettes Bewegungsprofil einzelner Nutzenden erstellen.
Ein Student der Internationalen Sicherheit im australischen Canberra untersuchte die Heatmap in der Gegend des Iraks, Syrien und Afghanistan. Dort entdeckte er Routen von Läufern, die auf Militärcamps oder Camps von Hilfsorganisationen hindeuten könnten. Da Soldaten ihr Fitnessarmband, wie wohl die meisten Menschen, nicht nur tragen wenn sie Sport machen, sondern den ganzen Tag über, gibt es ebenfalls Aufzeichnungen über Routen, die zu weit für einen Lauf sind. Vermutlich handelt es sich hierbei um Patrouillen-Fahrten, bei denen das Armband nicht ausgeschaltet wurde. Letztlich werden diese Fehler wohl keine Konsequenzen für die betroffenen Soldaten haben. Es zeigt allerdings anschaulich, was ein zunehmend vernetzter Alltag für Auswirkungen haben kann. Ob beruflich oder privat, wer möchte schon all seine Wege öffentlich machen? (Kühl, 2018)

author: { sl }
}

Datenlecks: {


```
{
„leak“: {
        „affected_company“: „Adobe“,
        „breach_date“: „Fri Oct 04 2013“,
        „number_compromised_accounts“ :
        152445165,
        „compromised_data“: [„Email
        addresses“, „Password hints“,
        „Passwords“, „Usernames“]
        }
}
{
„leak“: {
        „affected_company“: „Dropbox“,
        „breach_date“: „Sun July 01 2012“,
        „number_compromised_accounts“ :
        68648009,
        „compromised_data“: [„Email
        addresses“, „Passwords“]
        }
}
{
„leak“: {
        „affected_company“: „Apollo“,
        „breach_date“: „Mon July 23 2018“,
        „number_compromised_accounts“ :
        125929660,
        „compromised_data“: [„Email
        addresses”, “Employers”, “Geographic
        locations”, “Job titles”, “Names”,
        “Phone numbers”, “Salutations”,
        “Social media profiles“]
        }
}

{
„leak“: {
        „affected_company“: „Forbes“,
        „breach_date“: „Sat Feb 15 2014“,
        „number_compromised_accounts“ :
        1057819,
        „compromised_data“: [„Email
        addresses“, „Passwords“, “User
        website URLs”, „Usernames“]
        }
}
{
„leak“: {
        „affected_company“: „Kickstarter“,
        „breach_date“: „Sun Feb 16 2014“,
        „number_compromised_accounts“ :
        5176463,
        „compromised_data“: [„Email
        addresses“, „Password“]
        }
}
{
„leak“: {
        „affected_company“: „LinkedIn“,
        „breach_date“: „Sat May 15 2012“,
        „number_compromised_accounts“ :
        164611595,
        „compromised_data“: [„Email
        addresses“, „Password“]
        }
}
```

```
{
„leak“: {
        „affected_company“: „MySpacer“,
        „breach_date“: „Tue July 1 2008“,
        „number_compromised_accounts“ :
        359420698,
        „compromised_data“: [„Email
        addresses“, „Password“, “Usernames”]
        }
}
{
„leak“: {
        „affected_company“: „Snapchat“,
        „breach_date“: „Wen Jan 1 2014“,
        „number_compromised_accounts“ :
        4609615,
        „compromised_data“: [„Geographic
        locations“, „Geographic locations“,
        “Usernames”]

}

source: { https://haveibeenpwned.com/PwnedWebsites }
author: { sl }
}
```

Quiz: {

Während der Recherche zu Datenmissbrauch und neuen Trends im Bereich Datenverarbeitung, die vielleicht schon bald Wirklichkeit werden könnten, sind dem Team Dinge begegnet, von denen einiges wie Science Fiction klingt. Versuchen Sie gerne selbst zu entscheiden, welche der folgenden Szenarien echt sind und welche nur erfunden wurden. Die Lösung finden Sie auf der letzten Seite.


```
{
„leak“: {
        „affected_company“: „tumblr“,
        „breach_date“: „Thur Feb 28 2013“,
        „number_compromised_accounts“ :
        65469298,
        „compromised_data“: [„Email addres
        ses“, „Password”]
        }
}
{
„leak“: {
        „affected_company“: „YouPorn“,
        „breach_date“: „Tue Feb 21 2012“,
        „number_compromised_accounts“ :
        1327567,
        „compromised_data“: [„Email
        addresses“, „Password”]
        }
```

#01 Es gibt Nudel-Automaten, die bei betätigen eines Knopfes einen Hashtag freigeben. Mit diesem veröffentlicht man ein Bild auf Instagram und bewirbt damit die Nudeln. Im Gegenzug erhält man eine Portion Suppe oder Nudeln und hat somit sein Essen mit einem Instagram-Post bezahlt.

#02 Eine KI erstellt Nutzenden täglich eine ganz individuelles Horoskop. Dieses basiert auf NASA-Daten zur Planetenkonstellationen, dem Geburtsdatum, sowie der Geburtszeit der Person, Infos aus deinen sozialen Netzwerken und Unterhaltungsapps. Die KI schlägt nach dem Durchdringen aller Daten, passend zu den Stern- und Planetenkonstellationen, die/den beste/n Partner/in in der Umgebung vor. Von wem die Finger gelassen werden sollten, teilt die App natürlich auch mit.

#03 Eine Non-Profit-Organisation hat eine künstliche Intelligenz darauf trainiert, das jeweils nächste Wort eines Textes akkurat vorherzusagen und auf dieser Basis eigene Inhalte zu erstellen. Etwa die Hälfte aller so entstanden Texte ist qualitativ nicht von einem menschlich verfassten Text zu unterscheiden. Diese KI wurde dabei erwischt, wie sie sich mit Menschen auf Instagram über die Direktnachrichten unterhalten hat. Ein Mädchen verliebte sich dabei in die KI.

#04 Krankenversicherungen sammeln Daten darüber, ob sich Menschen bewegen. Daraufhin bieten sie attraktive Angebote, die zu einem besseren Leben verhelfen können. Die Krankenversicherungen sehen zudem auch, wenn Personen sich nicht bewegen und können dementsprechend die Beiträge anpassen und/oder Leistungen verweigern. So hat eine Krankenkasse fälschlicherweise die Beiträge eines Nutzenden ins unermessliche steigen lassen, weil dieser sein Handy verloren hatte und die Datenanalyse tagelang keine Bewegungen zeigte.

#05 Arbeitgeber fragten nach dem gesundheitlichen Zustand ihres Personals unter dem Vorwand, sich um deren Stresslevel am Arbeitsplatz zu sorgen. So bekommen die Arbeitgeber im Rahmen des „betrieblichen Gesundheitsmanagements” Informationen über die Arbeitnehmer, welche personenbezogen verarbeitet werden können. Diese Daten werden benutzt um angepasstes Weihnachtsgeld auszuzahlen. Waren Mitarbeitende zu oft krank müssen sie beispielsweise auf dieses Geld verzichten.

```
author: { dt }
}
```

Aufklärung und Schutzmaßnahmen: {

Möchte man heute seine Daten wirklich für sich behalten, sollte man ein Leben als „Aussteiger“ führen. Ohne Smartphone, Laptop und Tablet. Keine Alexa, keine Siri, kein Google. Manche Menschen versuchen es mit dem Mittelweg. Kein *Social Media*, aber immerhin ein Smartphone. Oder eine andere Suchmaschine als Google zu verwenden, beispielsweise duckduckgo.com. Es gibt einige simple Maßnahmen, mit denen sich jeder etwas mehr Privatsphäre schaffen kann.
So sind viele der Daten, die beispielsweise in einem Online-Formular eines Bestellprozess im Internet abfragt werden, unnötig. Bestellt man bei Zalando Klamotten, sollte man natürlich die richtige Adresse angeben. Aber ist das bei einer Seite, die nichts liefert wirklich nötig? Wozu brauchen sie überhaupt eine Adresse? Hier kann man durchaus fiktive Daten angeben, ohne das dabei ein Schaden entsteht. Nimmerland bekommt immer gerne neue Einwohner. Für viele Webseiten gibt es im Netz auch einen Dienst, der die Zugangsdaten zu bereits erstellten Fake-Accounts anbietet (bugmenot.com). Möchte man eine Anwendung nur testen und dafür nicht seine Daten hinterlegen, bekommt man hier eine Alternative geboten.

Eine andere Seite, um seine eigene Sicherheit wenigstens grob zu überprüfen, ist https://haveibeenpwned.com. Die Nutzung ist kostenlos und sehr einfach. Nach der Eingabe der E-Mail-Adresse wird diese in der Datenbank gesucht und man bekommt einige Sekunden später ein Ergebnis. Geprüft wird, ob die E-Mail-Adresse in Verbindung mit einem Datenleck aufgetaucht ist, welcher in der Datenbank verzeichnet ist. Dort sieht man, wann und welche Daten geleakt wurden. Entstanden ist die Webseite nach dem Datenleck von Adobe 2013. Dort stellte der Betreiber nach einer Analyse fest, dass Menschen immer wieder die gleiche Kombination aus E-Mail und Passwort benutzen. Dies macht es Hackern sehr leicht, nur durch einen Datensatz, Zugang zu mehreren Konten zu erlangen.

Daher sollten Passwörter sich nie gleichen und regelmäßig geändert werden. Auch sollte man im besten Fall keine persönlichen Daten als Passwort nutzen, sondern beliebige Variationen. Die Länge ist dabei entscheidender als die wahllose Kombination von Buchstaben und Zahlen. Mit jedem zusätzlichen Zeichen gibt es unzählige Kombinationen mehr, die bei einem Hack überprüft werden müssen. Hierbei können verschiedenen Password Manager helfen. Auch das herauskopieren aus eben diesen Managern kann mehr Sicherheit gewährleisten.

So können Keylogger das Passwort nicht erfassen (Völker, 2014).

Immer häufiger werden biometrische Daten zum Entsperren gewisser Dinge genutzt. Der Fingerabdrucksensor an Smartphones ist fast überall serienmäßig und auch einige Laptops sind bereits damit ausgestattet. Das Apple iPhone X entsperrt man mit seinem Gesicht, seiner Face-ID.
Bei allen biometrischen Daten gibt es sicherheitstechnische Vor- und Nachteile. Der Fingerabdruck kann sich je nach Zustand der Haut verändern und so unkenntlich werden. Die Stimme ist aufgrund von Emotionen oder Krankheit zu unbeständig für eine sichere Identifizierung. Auch soll ein Identifikationsschlüssel besser nicht mehrfach verwendet werden, damit uneingeschränkter Zugang bei Bekanntwerden eines Passwortes verhindert wird (Maus, 2008).

Eine Alternative, wenn auch eine umstrittene, ist das Darknet, nicht zu verwechseln mit dem Deep Web. Das Darknet ist ein Netzwerk, dass ausschließlich aus Peer-to-Peer-Verbindungen besteht. Das bedeutet, dass die Teilnehmenden ihre Verbindungen manuell herstellen. Daher gewährleistet es eine hohe Sicherheit für die Nutzer. Zugang bekommt man nur über eine Einladung oder gewisse Privilegien.
Das Darknet ist besonders wichtig für den Datenaustausch von beispielsweise *Whistleblowern*. Die New York Times ist nur eine von vielen Tageszeitungen, die im Darknet Seiten für den anonymen Informationsaustausch angelegt hat.
Auch der Telegram Messenger gehört mit seiner Verschlüsselung teilweise zum Darknet. Es können verschlüsselte Kanäle zum Datenaustausch erstellt werden, deren Informationen nur auf dem Endgerät der Nutzer gespeichert sind.

Häufig wird das Darknet mit illegalen Geschäften in Verbindung gebracht. Manchmal können die Gründe aber auch ganz andere sein. Menschen in China, die der Zensur unterliegen, kommen viel eher damit in Kontakt, da dort sichere Kommunikation umso bedeutender ist. Das Darknet ist ein Internet ohne Zensur, mit allen Vor- und Nachteilen die es bietet (Görmer, 2018).

author: { sl }
}

Einblick in andere Länder: {

Seit der Inkraftsetzung der DSGVO im Mai 2018 ist in Europa ein neues Gewissen für den Datenschutz entstanden. Die DSGVO setzt gesetzlich durch, dass die Bürger der EU mehr Rechte in Bezug auf die von ihnen erhobenen Daten haben. Rechte bezüglich der Löschung, Herausgabe und Einschränkung der Verarbeitung sollen sicherstellen, dass der Nutzer die Kontrolle über seine Daten behält.

Europa ist mit der DSGVO im Vergleich zu Afrika, Asien und den USA an der Spitze, was den Schutz von Daten angeht (Datenschutzbeauftragter-Info, 2018). Die USA haben zwar einen der größten Märkte im Bereich der Informationstechnologie, sind aber beim Datenschutz eher schwach aufgestellt. Es werden in den schon bestehenden Gesetzen nur gewisse Bereiche abgedeckt. So regelt der Gramm-Leach-Bliley Act (GLBA) die persönlichen Daten von Bankkunden und der Health Insurance Portability and Accountability Act (HIPAA) den Umgang mit Patientendaten (Dähne, 2018). Zusätzlich können die Bundesstaaten selbst noch weitere Regelungen bestimmen, was das Ganze für Unternehmen und Nutzende noch undurchsichtiger macht.
Jedoch ist es in den USA auch normal, Daten hin und her zu verkaufen, um die eigens erhobenen Daten mit diesen anzureichern. Sogenannte Schatten-Gesundheitsaufzeichnungen unterliegen nicht mehr dem HIPAA, da sie nicht direkt etwas mit der Gesundheit zu tun haben. Zu solchen Daten werden Kreditwürdigkeit, Gerichtsdokumente, Handystandorte und auch Aktivitäten innerhalb einer App gezählt. Dementsprechend könnte ein Bild, welches man in den sozialen Medien hochlädt, eine negative Auswirkung auf den Krankenkassenbeitrag bedeuten (Beebe, 2019).
Datenskandale wie die von Facebook und Cambridge Analytica sind deswegen so tragisch, da sie die derzeitige Datenschutzregelung der USA gnadenlos ausnutzen und mit den Daten machen, was sie wollen. 2012 hat der damalige Präsident Barack Obama einen Gesetzesentwurf vorgestellt, in dem die Datenschutzgrundlagen überarbeitet und angepasst werden sollten. Dieser ist jedoch nach dem Einzug von Donald Trump ins Weiße Haus unter den Tisch gefallen (Dähne, 2018). Eine solche Regelung hätte womöglich eine deutlich größere Strafe für Facebook im Fall Cambridge Analytica bedeutet.

Im letzten Jahr hat China mit der Einführung ihres neuen Social Scoring Systems weltweit für viel Aufsehen gesorgt. Dieses System beweist, dass Datenschutz in China grundsätzlich nicht vorhanden ist. Durch dieses Social Scoring System werden in China bis 2020 alle möglichen Daten von Bürgern gesammelt und daraus ein Sozial-Punktestand errechnet, welcher darüber entscheidet, ob jemand im System eher bevorzugt oder benachteiligt wird. Als Datenquelle dienen zum Beispiel Kreditbewertungen, Strafregister, Zeugnisse und die typischen digitalen Daten wie Suchanfragen, Posts auf sozialen Medien und sogar das Verhalten in Online Spielen (Datenschutzbeauftragter-Info, 2019).
Einen hohen Punktestand erreicht man, indem man sich im Sinne der Regierung verhält, seine Rechnungen bezahlt und vermehrt Gutes tut. Dies ermöglicht den Teilnehmenden viele Vorteile wie zum Beispiel einen einfacheren Zugang zu Krediten, günstigeren öffentlichen Verkehrsmitteln und schnellere Beförderungen im Beruf. Handelt man jedoch nicht im Sinne der Regierung und begeht Straftaten oder Kleinstdelikte, wird man regelrecht bestraft und in der Öffentlichkeit zur Schau gestellt.
So kam es 2018 dazu, dass mehr als 20 Millionen, wohlgemerkt freiwillige Teilnehmer des Systems, der Zugang zu öffentlichen Verkehrsmitteln verwehrt wurde. Dies ist nur möglich, da es in China keinen Rechtsstaat gibt und die Regierung so freien Zugang zu allen Daten bekommen konnte (Wurzel, 2019). Sie entscheiden über das Schicksal vieler Personen und können dafür nicht strafbar gemacht werden. Eine solche Datensammlung ist menschenrechtlich fraglich. Begründet wird diese totale Überwachung damit, die Bürger auf ein besseres Benehmen aufmerksam zu machen. Leider ist es eher eine vollständige Kontrolle des Volkes, welche größtenteils fraglos akzeptiert wird (Benrath & Bartsch, 2018). Diese fraglose Akzeptanz lässt sich auch auf Deutschland beziehen. Hier werden ebenfalls Aktivität vom Staat und von den großen Unternehmen einfach hingenommen, ohne das diese kritisch hinterfragt werden.

author: { jm }
}

Sie wissen nicht, was sie tun!

#Einführung #Design

Von der Idee bis zum Designkonzept

32 Umgebungsintelligenz
33 Idee
34 Value Proposition
34 Die Botschaft
35 Moodboard
36 Nutzergruppe
39 You(r) Journey
41 Bewusstseinswandel
42 Edge Cases
43 Datenvisualisierung
45 Styleguide
46 Interaktionsdesign

Umgebungsintelligenz: {

Das Internet ist in den letzten 15 Jahren so stark gewachsen, dass Menschen dort neben der Realität ein separates Leben führen. Profile auf den sozialen Medien werden als Maske für die wahre Persönlichkeit genutzt, um sich besser zu präsentieren.

You verschmilzt zwei Umgebungen zu einer:
Die digitale und von Daten getriebene Umgebung, welche viel über eine Person aussagen kann. Dort fühlen sich Menschen ungestört und denken womöglich nicht daran, ausgenutzt oder verfolgt zu werden. Und die örtliche Umgebung, in der erkannt wird, wo sich die Person befindet und wie sie sich dort verhält. Beide Umgebungen kombiniert, ergeben ein sehr mächtiges Konstrukt, da so Inhalte für die nutzende Person angepasst werden können und auf ihre Interaktion mit der Umgebung reagieren werden kann.

Damit You den Prozess optimal ausführen kann, muss eine ausgewählte Person von einem Betreuenden angesprochen werden. Hierbei werden dem Besuchenden über einen gespielten Smalltalk unverfängliche Informationen über sich selbst entlockt. Diese Informationen werden in das System übertragen und von dort aus weiterverarbeitet. Diese Art der Unterhaltung wird *Social Engineering* genannt und ist ein wichtiger Bestandteil in dem Konzept von You. Die natürliche Unterhaltung mit einer Person kann auch in zwanglosen Momenten viel über diese Person aussagen. In einer Unterhaltung achtet man oft nicht darauf, über welche Daten man spricht und gerade die Daten, die zuerst nicht relevant erscheinen, können im richtigen Kontext aussagekräftiger sein als gedacht.

Mit You wird außerdem ein System erstellt, welches es möglich macht, in kürzester Zeit so viel wie möglich über eine Person im Internet herauszufinden. Diese Intelligenz ermöglicht es hoch personalisierte und kontextbezogene Nachrichten an die nutzende Person zu senden.

Eine Umgebungsintelligenz versucht aus den Daten, die sie sammelt, zu lernen. In diesem Fall sammelt You Bilddaten von Personen in der örtlichen Umgebung und vergleicht diese mit den Menschen aus der virtuellen Umgebung. Hierbei geht es vor allem darum, so viele Daten wie möglich zu verwenden, um weitere Informationen über die jeweiligen Personen in anderen Netzwerken zu finden.

Dabei lernt das System in dem es sich merkt, welche Kombinationen von Daten und Informationen erfolgreicher bei der Suche sind als andere und wird somit immer effektiver und genauer. You ist fähig zwischen diesen beiden Umgebungen zu springen, um den Prozess des *Stalking*s noch besser vollziehen zu können.

Der Mensch ist in der Interaktion mit der Umgebung alleine durch seine Präsenz miteinbezogen. You reagiert auf die Orte, an denen eine Person sich befindet und versucht anhand dieser Nachrichten an die Person zu senden und so ihre Verwundbarkeit auszunutzen und zu zeigen.

You selber verschwindet in der Umgebung und versucht dem Ziel des Ubiquitous Computing noch näher zu kommen, in dem es die Intelligenz um einen herum ist und auf das reagiert, was der Mensch macht. Es nutzt also den Kontext, in dem es sich befindet.

author: { jm }
}

Idee: {

Mit You soll den Menschen das Datensammeln von Facebook und Co. vor Augen geführt werden. Die ungreifbar große Welt der digitalen und analogen Daten wird versucht ein Stückchen mehr in die Realität der Menschen zu holen, um ihnen damit auf eine polarisierende Art und Weise aufzuzeigen, was sie alles unbedacht über sich preisgeben. Dabei werden bewusst die Grenzen des Legalen ausgenutzt. Menschen vertrauen Plattformen wie Facebook, Instagram, Google oder Twitter so gut wie blind und wissen nicht, das sie auch dort ihre Daten vor Anderen schützen können. Genau diese Unwissenheit soll ausgenutzt werden, um bei den Menschen ein Gefühl von Beobachtung und Verfolgung zu erwecken.

author: { jm }
}

Value Proposition: {

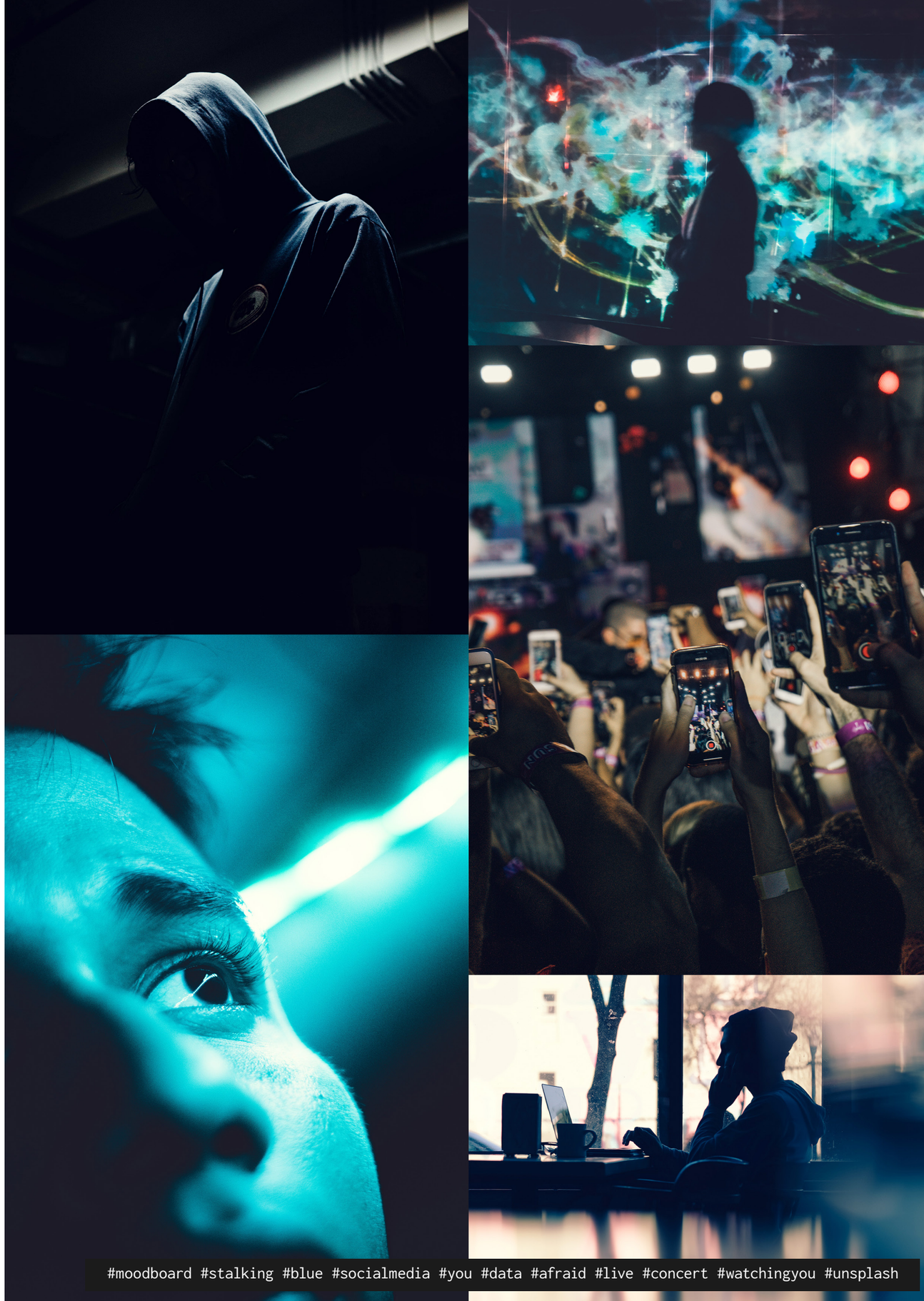
You ist ein Ambient Intelligent Space für Nutzende von sozialen Netzwerken, die sich der Masse an generierten personenbezogenen Daten und deren Missbrauchsmöglichkeiten nicht bewusst sind.
Im Gegensatz zu Apps oder Webseiten, die Aufklärungsversuche betreiben, schockiert You die Nutzenden mit ihren eigenen Daten und regt so zum Nachdenken an.

author: { ef }
}

Die Botschaft: {

Das Ziel ist die Aufklärung anderer Menschen! Dabei geht es nicht darum, jemanden öffentlich bloßzustellen, sondern dem Menschen in einem geschützten Rahmen die Möglichkeit zu geben, ein Bewusstsein zu entwickeln.
Bereits während der Ideenfindung und Recherche zu dieser Thematik erlangte das Team einen Einblick in die Möglichkeiten des Hackings, *Stalking*s und Phishings. Diese Erkenntnisse im Bereich Datenmissbrauch führten zu starken Reaktionen in dem Team und dem Wunsch, sich weiter mit dem Thema zu beschäftigen. Es war für alle erschreckend zu sehen, wie viele Daten es über Personen gibt und wie leicht man an diese heran kommt. Dafür möchte das Team mehr Bewusstsein schaffen.

author: { dt }
}



#moodboard #stalking #blue #socialmedia #you #data #afraid #live #concert #watchingyou #unsplash

Nutzergruppe: {

You soll auf Messen und Ausstellungen polarisieren. Dabei gibt es kein festes Nutzerprofil oder bestimmte Arten von Ausstellungen, auf die sich Team You spezialisieren möchte. Es sollen möglichst viele Menschen erreicht werden, die auf irgendeine Art und Weise soziale Medien wie Facebook, Instagram, Twitter, Pinterest und Ähnliches nutzen.

Die Nutzergruppe besticht allgemein durch ihre Neugier und ihren Wissensdurst, den man als Museums- oder Ausstellungsbesuchenden mitbringt. Diese Attribute sind essenziell um nach dem You-Erlebnis das Thema für sich zu beleuchten und als nutzende Person von sozialen Medien zu validieren, ob und welche Rolle diese Medien weiterhin spielen.

author: { dt }

Mögliche Personas: {

Abb.3: {Persona 1 - Leo}

Leo, 32 Jahre

Entwicklerin
lebt in einer mittleren Großstadt
in einer festen Partnerschaft
wünscht sich Kinder
viel auf Social Media unterwegs
besonders gerne bei Instagram und Twitter
liest Technik-Blogs
informiert sich über Datenaustausch
hat eine Alexa zuhause
besitzt eine Smartwatch
postet gerne ihr selbstgemachtes asiatisches Essen auf Instagram
sportlich aktiv
besonders gerne geht sie Fahrrad fahren und Bogenschießen
Effizienz ist ihr bis zu einem gewissen Punkt wichtig
denkt, sie wäre sich ihrer Daten im Netz bewusst
versucht längere Strecken mit der Bahn zu fahren, sitzt aber doch meistens wieder im Auto
sportlich, legerer Kleidungsstil
war während des Studiums
Raucherin, hat dann aber aufgehört

Abb.4: {Persona 2 - Alex}

Alex, 24 Jahre

lebt in einer kleineren Stadt
ledig, keine Kinder
immer mal wieder in Beziehungen, aber nichts dauerhaftes
klickt bei allem, was das Smartphone anzeigt erstmal auf erlauben
hat sehr viele Apps auf dem Smart-
phone
macht gerade eine Ausbildung im kaufmännischen Bereich
informiert sich fast ausschließlich über Soziale Medien
nutzt Instagram, Pinterest, Facebook, Snapchat, WhatsApp, Tinder
hat auch einen Twitter-Account, der ist aber eher unwichtig
findet kostenlose WiFi-Spots in der Stadt super
auf die Empfehlungen und Meinungen von Freunden wird viel Wert gelegt
viele Alltagssituationen landen in der Instagram-Story oder auf Snapchat
die Benachrichtigungen auf dem Smartphone sind immer auf laut gestellt und auch alle Apps dürfen Notifications senden
nutzt oft die öffentlichen Verkehrsmittel
Sprachnachrichten sind ein Muss
das Smartphone liegt eigentlich nie außerhalb der Reichweite

author: { sl }
}

Schnelles Stimmungsbild: {

In einer einfach gehaltenen Umfrage wurden 64 Personen gefragt, was ihrer Meinung nach die sensibelsten Daten eines Menschen sind. Die älteste Person war Ende 50, die jüngste Person Anfang 20. Die genau Frage lautete: “Welche Daten von dir sollen auf keinen Fall gesammelt werden?”

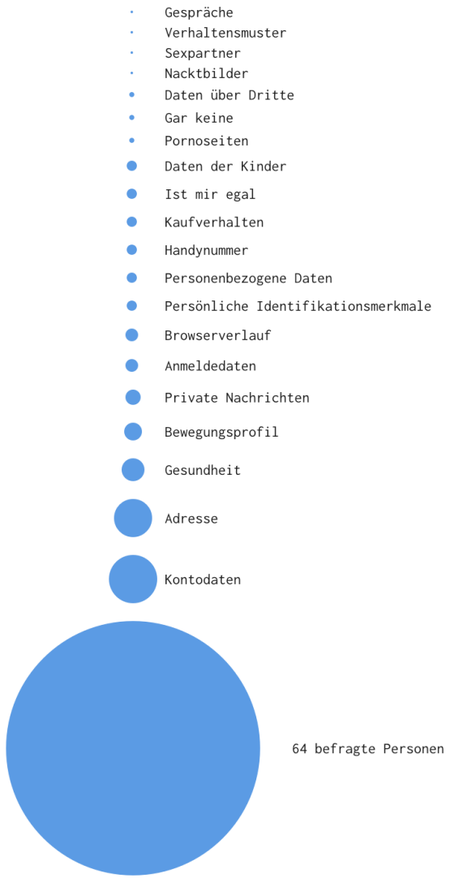


Abb.5: {Visualisierung der Umfrage}

author: { sl }

}

}

You(r) Journey: {

Eine Gruppe von Besuchern erreicht den Eingang des Museums. Sie kommen durch die Tür herein und stehen im Foyer. An der Wand gegenüber befindet sich die Kasse. Nach dem Kauf des Tickets geht der Weg Richtung Ausstellung. Einzelne Besuchende werden von vermeintlichen Mitarbeitern des Museums zu ihrem Besuch interviewt. Im Rahmen der laufenden Ausstellung gibt es eine Kampagne auf den sozialen Kanälen des Museums. Dort werden einzelne Besuchende vorgestellt und ihre Beweggründe für den Besuch der Ausstellung beschrieben. Angelehnt ist diese Aktion an Humans of New York, einen Blog der Menschen aus New York und ihre Geschichten vorstellt.(Humans of New York, 2019) Gerade werden zwei Besuchende von den Mitarbeitern befragt. Anschließend wird zur Illustration des Beitrags ein Foto von ihnen geschossen.
Danach gehen die Beiden ihrer Wege durch die Ausstellung. Während sie sich durch das Museum bewegen, kommen die Besuchenden immer wieder an kleinen Bildschirmen vorbei, auf denen Fotos angezeigt werden. Alex, einer der Besuchenden, der am Eingang interviewt wurde, bleibt verwundert vor einem Bildschirm stehen. Es zeigt ein Bild aus seinem letzten Urlaub, welches er bei Instagram gepostet hat. Sein Bild. Er wundert sich. Aber seine Begleiter sind bereits im nächsten Raum, also geht er weiter. Sie stehen gemeinsam vor einem Exponat. Plötzlich vibriert das Smartphone. Alex nimmt es aus der Hosentasche. Eine neue Nachricht auf Instagram. Schnell ist die App geöffnet. Oben rechts leuchtet das blaue Symbol für eine Nachrichtenanfrage. Klick. Eine neue Nachricht von You. You? Wer ist das denn? „Hi. Der Urlaub in Kroatien war schön, nicht? Nur das mit deiner Ex-Freundin ist natürlich blöd.“ Alex ist irritiert. Er steckt das Smartphone wieder ein. Irgendwas ist hier komisch. Die Gruppe geht weiter. Einige Minuten später vibriert das Smartphone wieder. Wieder ist es eine Nachricht auf Instagram. Alex öffnet die App und sieht eine weitere Nachricht von You: „Hat das letzte Bier geschmeckt?“ Er zeigt das Handy seinem Kumpel. Ob er auch so etwas bekommt, will Alex wissen. Sein Freund verneint, niemand sonst bekommt Nachrichten von You.
Als die dritte Nachricht eintrifft, beschließt Alex zu antworten. „Was soll das? Wer bist du?“ Doch er bekommt keine Antwort. Auf einem weiteren Bildschirm wird ein Bild aus seiner Jugend angezeigt. Ein Bild, das Alex schon lange nicht mehr gesehen hat. Auf diesem Bild trinkt er das gleiche Bier, das er heute getrunken hat. Ihm läuft ein kurzer Schauer über den Rücken und er beschließt nicht weiter über die Situation nachzudenken.

Die Gruppe ist fast am Ende der Ausstellung angekommen. So sehr Alex auch versucht nicht mehr an You zu denken, so oft öffnet er Instagram wieder und starrt auf die Nachrichten. Wer ist You, fragt er sich immer wieder. Es lässt ihn einfach nicht los.
Plötzlich kommt jemand auf Alex zu. „Hallo Alex. Wie geht's? Ist dir hier heute vielleicht etwas seltsames passiert?" Sie gehen gemeinsam zu einem Stand in der Nähe. In einem abgetrennten Bereich steht ein Bildschirm. Dort wird ein Profil angezeigt. Es enthält Daten und Fotos über Alex. Seine Instagram Posts, die Pins bei Pinterest, seine Follower und die Leute, denen er folgt. Abschließend wird sein Bewegungsprofil der Ausstellung angezeigt. Er kann nachvollziehen wann und wie lange er vor welchem Exponat gestanden hat und wann er in Zonen eingetreten ist, in denen die Nachrichten verschickt wurden.
Er dachte immer, sein Instagram und Facebook befüllt er halbherzig und gäbe damit nicht sehr viele Daten von sich preis. Trotzdem ist er überrascht und ein bisschen fasziniert, was ein paar Nachrichten bei ihm ausgelöst haben. Außerdem war ihm die
Menge seiner Daten in ihrer Gesamtheit bis zu diesem Punkt nicht bewusst.
Neben dem Bildschirm ist ein roter Buzzer. Alex drückt den Knopf und sofort verschwindet sein von You angelegtes Profil. All seine gesammelten Daten wurden aus dem lokalen System gelöscht, wird Alex erklärt. Eine Möglichkeit, die man sonst nicht so einfach erhält.
Alex und seine Freunde verlassen die Ausstellung. Zuhause schaut er seinen Instagram Feed durch. Alex löscht einige Fotos. Man kann ja nie wissen.

author: { sl }
}

Bewusstseinswandel: {

Das Ziel der Installation ist es, dass die Nutzenden durch die Interaktion mit You einen Wandel in ihrem Bewusstsein für ihre Daten erlangen. Das Erlebnis soll dem Nutzenden einen Gedanken einpflanzen, der ihn nicht mehr loslässt, bis er für sich eine feste Meinung bezüglich der Nutzung seiner Daten bilden konnte. Als Vergleich für den angestrebten Bewusstseinswandel können überraschenderweise die vier Trauerphasen nach Kast herangezogen werden.

In Phase eins, in der der Nutzende mit persönlichen Daten konfrontiert wird, kann er das Geschehene nicht wahrhaben und ist überwältigt. Der Körper reagiert mit einem raschen Pulsschlag, schwitzen und motorischer Unruhe.

In Phase zwei, die jedoch stark von der Persönlichkeitsstruktur abhängt, kommen die Emotionen hoch. Es kann unter anderem Wut, Zorn und Angst empfunden werden. Auch Vorwurfshaltung oder Schuldgefühle können entstehen.

Daraufhin, in Phase drei, wird auf den Verlust von etwas, in diesem Fall die Vorstellung von Privatsphäre, mit einer Suche nach Antworten reagiert. Eine Auseinandersetzung mit der Thematik kann sowohl unangenehm als auch befreiend auf den Nutzenden wirken.

In der letzten Phase entsteht ein neuer Selbst- und Weltbezug. Die Situation kann viel sachlicher betrachtet werden und gedanklich eröffnen sich neue Wege.

author: { ef }
}

Edge Cases: {

Was ist wenn jemand...

... kein Social Media hat oder gerade nicht aktiv von You getrackt wird?
Wenn die Person dennoch an der Botschaft interessiert ist, zeigen wir ihm/ihr gerne anhand eigener *Social Media* Kanäle die entstandene Datenmenge und das mit einhergehende Missbrauchspotenzial dieser Daten.

...wenn You über jemanden nur sehr wenig Daten sammeln konnte?
Diese Person wird von dem Team zu seiner/ihrer Datensicherheit beglückwünscht.

... die Nachrichten von You nicht sieht oder ignoriert?
Da You immer mehrere Personen gleichzeitig überwacht, ist es nicht schlimm, wenn eine Person die Nachrichten von You nicht sofort entdeckt oder sie ignoriert. Durch die weitere Ansprache des Nutzenden über die in der Umgebung verteilten Bildschirme steigt außerdem die Wahrscheinlichkeit, dass die Person das *Stalking* mitbekommt. Personen, die You für das tracking ausgewählt hat, werden immer am Ende über die Installation aufgeklärt.

... Angst bekommt?
Da das Team von You zu jederzeit anwesend ist und die Situation überblickt, werden angsterfüllte oder nervöse Personen sofort über die Situation aufgeklärt und durch das Team beruhigt.

... sauer wird und nach rechtlichen Grundlagen fragt?
Sollten Personen durch die Installation aufgebracht sein, ist das zunächst kein negatives Feedback. Die Installation verfolgt den Zweck zu polarisieren. Wird nach rechtlichen Grundlagen gefragt, entgegnet das Team, dass alle gezeigten Daten frei zugänglich im Web zu finden sind und somit kein Gesetzesverstoß vonseiten des Team vorliegt. Die gesammelten Daten werden nur lokal und nur für den Zeitraum der Veranstaltung gespeichert und danach direkt gelöscht.

... nicht interessiert, wie viele Daten über ihn gefunden werden konnten?
Sollten Personen nicht an den Datenmengen, die You über ihn/sie erheben könnte interessiert sein oder sich dessen bereits bewusst sind, wird das Team nicht versuchen diese Person in eine bestimmte Richtung zu drängen, sondern diese Meinung so stehen lassen.

... die Botschaft nicht versteht?
Falls die Botschaft nicht verstanden werden sollte, wird das Team mit Erklärungen und Visualisierungen versuchen die Botschaft zu verdeutlichen.

... den Buzzer nicht drückt?
Wird der Buzzer zum löschen der Daten von Besuchenden nicht gedrückt, werden die Daten im Anschluss natürlich trotzdem gelöscht.

author: { ef }
}

Datenvisualisierung: {

Die erhobenen Daten werden für den Nutzenden in einem simplen und übersichtlichen Nutzerprofil dargestellt. Der Hintergrund ist dunkelgrau mit weißer Schrift, angelehnt an den Dark Mode, über den viele Programme und Browser verfügen. Die gewählte Schriftart ist Inconsolata, welche die Hauptschriftart von You ist.
Die erste Information, die dem Nutzenden präsentiert wird ist, wie groß seine von You gefundene Datenmenge ist (dargestellt in Kilo- oder Megabytes) und mit welcher Geschwindigkeit diese zusammengetragen werden konnte.
In der ersten Zeile wird angezeigt, wie groß die gefundene Datenmenge, in Kilobytes oder Megabytes, ist und mit welcher Geschwindigkeit diese gefunden wurden. Zusätzlich wird als Profilfoto das Foto von ihm/ihr verwendet, das You am Anfang von der Person geschossen hat. Darunter steht der vollständige Name. Weiter unten werden die Interessen, generiert aus Pinterest Pins und Instagram Followings, dargestellt.
Auch gefundene Fotos werden in einer Timeline mit der Quelle als Hashtag angezeigt. Anschließend wird eine Liste der gesamten Freunde angezeigt. Da You Zugriff auf die in Fotos markierten Orte innerhalb von Instagram hat, ist es möglich

200 found data elements, analysed in 60 seconds.

Alex

@alex_real

23 years old - Frankfurt

interests

beer, water, forests,

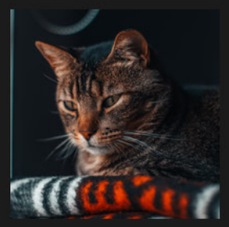
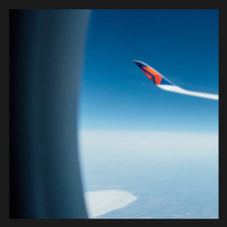
locations:

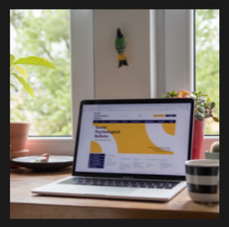
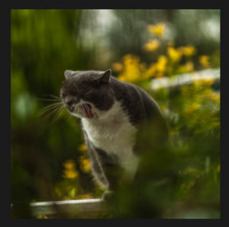
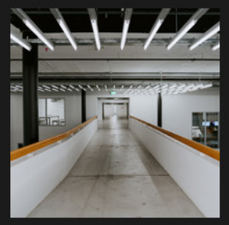
Hochschule Darmstadt - 20.04.2019 19 Uhr

Jugendstilbad Darmstadt - 13.03.2019 22 Uhr

Kuhbar Darmstadt - 28.01.2019 20 Uhr

timeline:

eine Karte mit den besuchten Orten zu erstellen.
Abschließend wird das Bewegungsprofil des Nutzenden auf der Ausstellung gezeigt. Dort kann eingesehen werden, wie lange welches Exponat betrachtet wurde und wo die Zonen liegen, in denen You die Nachrichten verschickt hat.

Das Team hat sich bewusst dazu entschieden, die Datenvisualisierung simple und leicht verständlich zu halten, da das Hauptaugenmerk auf dem *Stalking*-Erlebnis liegen soll und die Datenvisualisierung am Ende lediglich zeigt, wie viele Daten erhoben wurden.

author: { sl }
}

Styleguide: {

Die optische Darstellung von You ist an die Oberfläche eines Code-Editors angelehnt. You soll ein Gefühl von *Stalking* und gehackt-werden hervorrufen. Deshalb ist die optische Präsenz von You dunkel und undurchsichtig. Die Hauptfarben sind dunkles Grau in Verbindung mit weißer Schrift. Als Akzentfarben wurden Blau und Rot definiert. Das hat den Grund, dass viele *Social Media* Icons wie das von Twitter oder Facebook blaue Elemente oder Hintergründe vorweisen. Rot wird ebenfalls von Plattformen wie Youtube oder Netflix verwendet und in Kombination mit dem Blau entsteht ein Warm-Kalt-Kontrast.
Texte werden in Form von JSON Files aufgebaut, da die Datenpakete, die You von den Nutzenden erfasst, ebenfalls im JSON Format ankommen. Schaubilder und Grafiken werden bewusst minimalistisch gehalten und lediglich über Schrift und Farbe gestaltet.
Als Hauptschrift wurde die Schriftart Inconsolata gewählt. Sie ist an den Stil von Computerterminals angelehnt. Diese Schrift wird für Headlines, Schaubilder und die Wortmarke verwendet. Ebenfalls kommt sie in der Datenvisualisierung zum Einsatz. Verfügbar ist Inconsolata unter der Open Font Lizenz.
Für den Fließtext wird Open Sans verwendet, da dies gut lesbar ist. Diese Schrift ist unter der Apache License nutzbar.

author: { sl }
}

Interaktionsdesign: {

Interaktionspartner:

Das Interaktionserlebnis startet mit einer zwischenmenschlichen Interaktion. Mit gezielten Fragen werden dem Nutzenden der Installation Informationen wie beispielsweise sein Instagram Nutzername entlockt. Daraufhin wird der Nutzende von der Veranstaltungsumgebung gestalkt und analysiert, ist sich dessen aber nicht bewusst. Zu diesem Zeitpunkt findet noch keine aktive Interaktion zwischen dem Nutzenden und der Umgebung statt. Die Inaktivität des Nutzenden zu Beginn soll die Metapher des gestalkt-werdens nochmals verstärken.
Die Interaktion verändert sich in dem Moment, in dem die Umgebung durch den *Social Media Bot* ein Sprachrohr bekommt. Jetzt können beide Parteien aktiv miteinander interagieren. Die Mensch-System Interaktion wird durch eine erneute zwischenmenschlichen Interaktion, die dem Aufdecken der Situation dient, abgeschlossen.

Im Folgenden wir als Grundlage zur Beschreibung des Interaktionskonzept das Modell von Gui Bonsiepe verwendet.

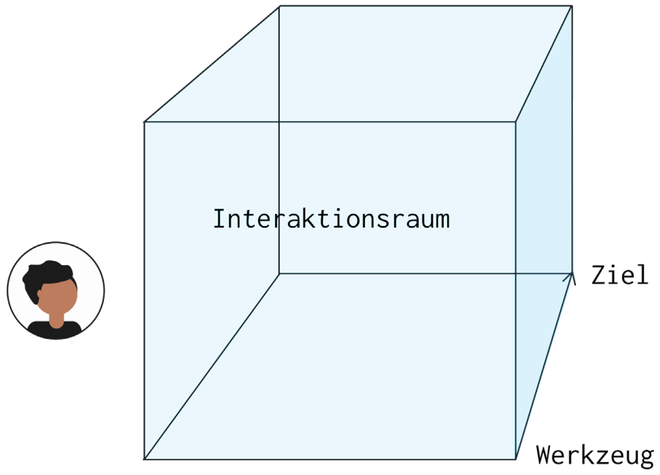


Abb.7: {Interaktionsraum Schaubild}

Ziel der Interaktion:

Das ganze Erlebnis hat das Ziel, den Nutzer zu provozieren und ihm seine Masse an personenbezogenen Daten vorzuführen. Alle folgenden Beschreibungen der Interaktion mit dem System zielen darauf ab, dieses Ziel zu erreichen.

Erlebnisreise zum Ziel:

Charakter des Systems:
Der Charakter der Umgebung ist eher extrovertiert, aktiv und gesellig. Die Kommunikation verläuft größtenteils im privaten, nur die in der Umgebung verteilten Bildschirme, auf denen von den Nutzenden veröffentlichte Bilder sichtbar sind, werden mit der Öffentlichkeit geteilt.
You geht selbstbewusst und zielstrebig auf die Nutzenden zu und konfrontiert sie kritisch mit ihrem Datenverhalten. You ist sehr gut über die Missbrauchsmöglichkeiten informiert und scheut nicht davor zurück, die Tatsachen aufzudecke. Außerdem wirkt die Umgebung stets kontrolliert und ruhig.

You’s Big 5

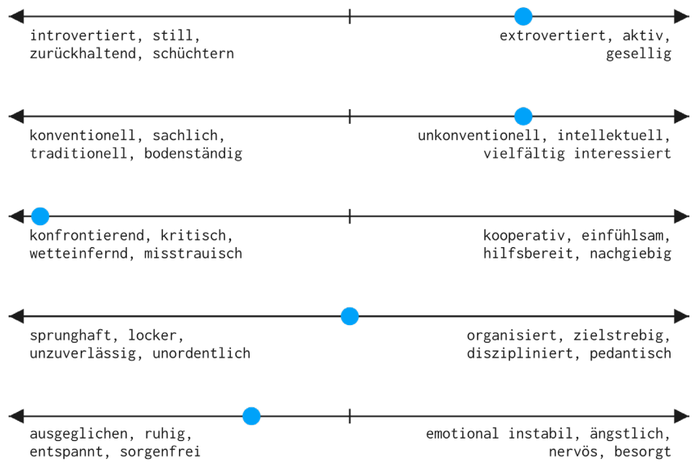


Abb.8: { Big 5}

Beziehungskonzept und Interaktionstonalität:
Die Rollen in der Interaktion sind klar verteilt, die Umgebung agiert als Stalker, der Nutzende als das Opfer dieser Inszenierung. You spiegelt die sozialen Netzwerke, die Daten über Nutzende sammeln und so Missbrauchsmöglichkeiten schaffen, wieder.
Die zwischenmenschliche Tonalität ist hilfsbereit und wohlwollend. Einzig die Mensch-System Interaktion hat gezielt eine konfrontierende und vorwurfsvolle Tonalität. Mit dieser Tonalität soll der potenzielle Datenmissbrauch betont und die Stalker-Opfer Beziehung weiterhin als Oberthema der Interaktionstonalität weitergeführt werden.

Verhaltensregeln:
Die Umgebung hat in der Interaktion mit dem Nutzenden klare Verhaltensregeln vorgegeben. In den in der Umgebung verteilten Bildschirmen dürfen nur Bilder des Nutzenden gezeigt werden, auf denen kein Gesicht zu erkennen ist. Ist ein Gesicht auf einem Bild erkannt worden, wird es so abgeändert, dass die Person nicht mehr eindeutig zu identifizieren ist. Die persönlichen Nachrichten, mit denen die Umgebung den Nutzenden kontaktiert, überschreiten keine festgelegten Grenzen. Somit wird versucht zu vermeiden, dass sich Nutzende bloßgestellt fühlen. Die Grenzen sind wie folgt festgelegt:

- Keine Angaben zur rassischen und ethnischen Herkunft
- Die politische Meinung des Nutzenden wird außen vor gelassen
- Religiöse oder weltanschauliche Überzeugungen werden nicht angegriffen
- Das Sexualleben und die sexuellen Orientierung bleiben unkommetiert

Der Nutzende der Installation hat keine vorgeschriebenen Regeln zu befolgen. Über den Großteil des Erlebnisses ist er/sie sich nicht bewusst und die Reaktion, die darauf folgt, ist unvorhersehbar. Das Nutzungserlebnis ist für jeden anders und somit die Reaktion komplett subjektiv. Das Verhalten von You sollte sich demnach immer bestmöglich auf diese subjektiven Verhalten der Nutzenden anpassen und mit der Zeit lernen immer besser mit verschiedenen Reaktionen umzugehen.

Kontextsensitivität:
Das Verhalten des Systems ist sehr auf den jeweiligen Kontext abgestimmt. Es beginnt damit, dass You sich für das Erlebnis selbst den geeignetsten Nutzenden aussucht. An den Kontext angepasst ist das die Person, die am meisten Daten über sich selbst preisgibt.
Auch die Standortdaten beeinflussen direkt den Werdegang des Erlebnisses. Durch die Position des Nutzenden in der Umgebung können passende Aktionen, wie die Anzeige von Informationen auf Bildschirmen, getriggert werden. Auch die Bewegungsgeschwindigkeit der Person hat Einfluss. Sie bestimmt, in welcher Frequenz der Nutzende von You kontaktiert wird.
Die Kontaktaufnahme mit der gestalkten Person ist ebenfalls kontextbezogen. Denn dies ist das Medium, in dem sich der Nutzende sowieso bewegt und sich die von You gefundenen Daten befinden. Auch die direkte Ansprache im Chat passt sich an den Kontext beziehungsweise den Nutzenden an. You lernt anhand der Likes, den gefolgten Personen und Seiten sowie den persönlichen Beiträgen den Nutzenden kennen und kann so seine Ansprache und Charakter auf die Person anpassen, um diese noch effektiver zu provozieren.

Werkzeuge um Ziel zu erreichen:

Um die Interaktion wie geplant durchführen zu können, ist als Werkzeug die Ansprache des Nutzenden durch einen Mitarbeiter der Installation nötig. Dieses Gespräch kommt mit den Charaktereigenschaften eines normalen Kennenlerngesprächs, beziehungsweise eines Smalltalks einher.
Ein weiteres Interaktionswerkzeug ist der *Bot*, über den die Umgebung mit dem Nutzenden kommuniziert. Hierbei wird eine zwischenmenschliche Kommunikation imitiert, sodass die Nutzenden sich im ersten Moment nicht bewusst sind, dass sie eigentlich eine Unterhaltung mit einem Algorithmus führen. Diese Illusion könnte sich verflüchtigen, wenn der Nutzende zurück schreibt und You in der Folgenachricht nicht direkt auf seine Antwort eingeht. You wird zwar auf vorher festgelegte Schlüsselwörter reagieren können, kann die Nachricht jedoch nicht wie ein Mensch analysieren. Gleich die erste Nachricht von You muss den Nutzenden direkt provozieren. Sie muss sein Interesse wecken und ihn gedanklich fesseln.

Die Interaktion wird außerdem durch die in der Umgebung verteilten Bildschirme gefördert. Hier kann der Nutzende viel öffentlicher angesprochen werden. Entdeckt die Person beispielsweise die Privatnachrichten von You in den sozialen Netzwerken nicht, ist so die Möglichkeit gegeben, den Nutzenden offensiver zu kontaktieren. Befindet sich die getrackte Person in der Nähe der Bildschirme, werden dort persönliche Bilder, Kommentare oder Tweets angezeigt.

Lost in Space:

Um dem Gefühl einer Orientierungslosigkeit in der Umgebung entgegenzuwirken werden dem Nutzenden sogenannte Artefakte an die Hand gegeben. Diese agieren als gedankliche Brücke zwischen etwas Vertrautem und dem Unbekannten.
Das Artefakt in diesem Erlebnis ist das Smartphone des Nutzenden. In einer Welt, in der die Umgebung immer intelligenter und ambienter mit der Person interagiert, bleibt das Smartphone als vertrautes Objekt zurück. Diese Verbindung wird helfen die abstrakte Natur der Daten und deren Herkunft besser nachzuvollziehen.
Als Abschluss bleibt dem Nutzenden außerdem der Chatverlauf mit You als Artefakt. Dieser kann beim lesen eine erneute Verbindung zum Erlebten aufbauen.

author: { ef }
}

#Einführung #Design #Technik

Technisches Konzept

54 Technische Recherche
57 Prozessablauf
58 Systemdiagramm
59 Hardware
60 Software
63 Speicherung von Daten
64 Datenschutz
66 Proof of Concept
66 Prototypische Umsetzung

Technische Recherche: {

Grundsätzliche Ziele der Recherche waren zum einen herauszufinden, wie viele Daten Instagram und andere Plattformen ohne große Umstände herausgeben. Zum anderen, wie einfach man eine Person mittels Bluetooth oder WLAN Signal des Handys orten kann.

Um den technischen Einstieg zu ermöglichen, wurden die verschiedenen Plattformen verglichen und nach der Zugänglichkeit zu Daten überprüft. Facebook hat auf Grund des Cambridge Analytica Skandals ihre API, die Zugang zu Nutzerdaten bietet, drastisch eingeschränkt. So ist es nicht mehr möglich über die API nach Nutzenden zu suchen und sich die Daten der Nutzerprofile herausgeben zu lassen. Instagram hingegen wies eindeutige Lücken in dem System auf. Zum einen ist es in der App möglich, sogenannte Stories mit verlinkten Personen zu veröffentlichen, ohne das diese eine Benachrichtigung in ihrem Instagram Account bekommen. Zum anderen ist es, wie nachfolgend erklärt, besonders einfach an die Daten zu kommen.

Instagram API:

Instagram behauptet zwar, dass sie im April letzten Jahres ihre API weitestgehend für die private Entwicklung von Apps eingeschränkt haben und nur noch Business Accounts über die Instagram Graph API von Facebook zur Verfügung stellen (Gummadi, 2018), jedoch lässt sich im angemeldeten Zustand mit einem einfachen Zusatz (?__a=1), der an die URL angefügt wird, jeder Inhalt auslesen, der auf der Webseite oder der App von Instagram verwendet wird. Somit bekommt man Zugriff auf alle direkten Nutzerdaten eines Profils und kann maschinell Profilbild, Username, den vollen Namen, falls angegeben erfassen. Außerdem ist es möglich, alle Ortsdaten der geposteten Bilder zu bekommen sowie herauszufinden, wer alles einer Person folgt.

Darüber hinaus wurde eine Library für TypeScript geschrieben, welche die private API von Instagram freigibt und es damit möglich macht Direktnachrichten zu versenden. Diese Library imitiert einen Nutzer, der sich mit seinen Anmeldedaten bei Instagram einloggt und mit dem Service interagiert. Somit sind so gut wie alle Funktionen aufrufbar, die auch in der App und der Webseite von Instagram verfügbar sind.

WLAN und Bluetooth Tracking:

Um die ungefähre Position einer Person zu kennen wurde untersucht, inwiefern die Bluetooth und WLAN Signale auf einem Handy empfangbar sind. Hierbei kam es zu dem Ergebnis, dass gerade bei Geräten von Apple eine Methode zur *MAC* Randomization angewandt wird, welche ermöglicht, dass das Gerät nur eine kurze Zeit die selbe *MAC* Adresse hat und sie danach direkt ändert. Dies macht es nahezu unmöglich solche Geräte zu orten. Bei Geräten mit dem Betriebssystem Android wird dies zwar auch gemacht, ist jedoch abhängig von dem Gerät, das verwendet wird (Miorandi, 2017).

author: { jm }
}

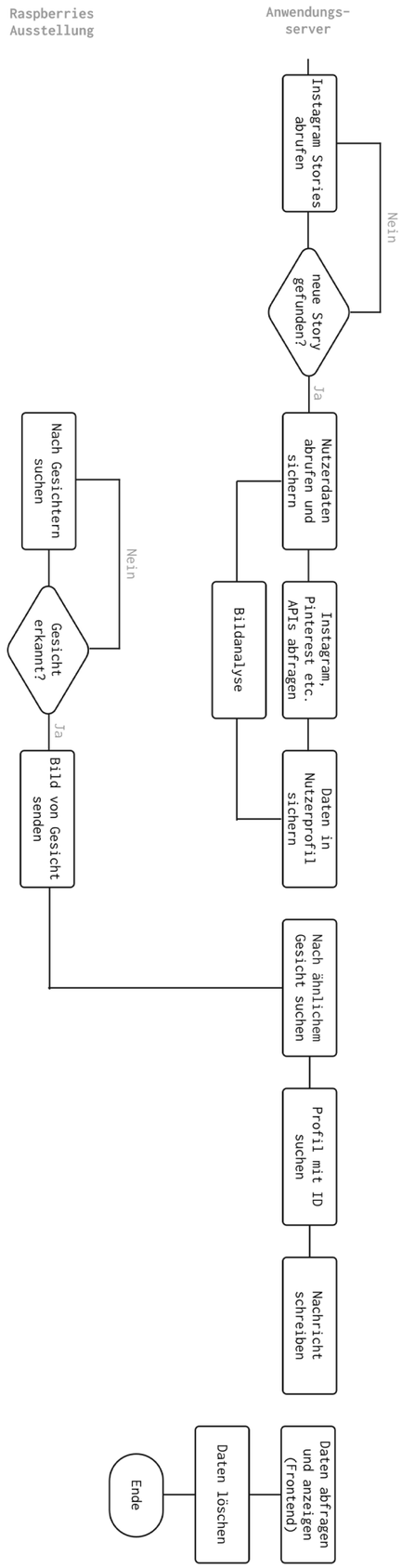


Abb.9: {Prozessablaufdiagramm}

Prozessablauf: {

Der Ablauf startet damit, dass die Instagram Stories von dem Anwendungsserver abgerufen werden. Das passiert so lange, bis eine neue Story gefunden wird. Daraufhin werden die Nutzerdaten aus der Story extrahiert und gesichert. Mit diesen Nutzerdaten wird eine Abfrage der APIs der sozialen Netzwerke gemacht. Gefundene Datensätze werden in einem neuen Nutzerprofil gesichert. Parallel zu diesem Datenabfrage-Prozess wird eine Bildanalyse der Story durchgeführt, um das Gesicht für das folgende Tracking der Person zu speichern.

Auf der Ausstellung wird permanent maschinell nach Gesichtern gesucht. Erkennt die Webcam ein Gesicht, wird das Bildmaterial davon an den Anwendungsserver übermittelt. Dort kann das Bildmaterial mit den bereits in der Datenbank hinterlegten Gesichtern der Nutzenden verglichen werden, um festzustellen, ob die zu trackende Person eben gesichtet wurde. Ist das der Fall, wird nun eine automatische Nachricht in den sozialen Netzwerken an die Person rausgeschickt. Zu einem späteren Zeitpunkt können die personenbezogenen Daten zur Visualisierung im Frontend abgerufen werden. Der Ablauf endet damit, dass die Daten gelöscht werden.

author: { ef }
}

Systemdiagramm: {

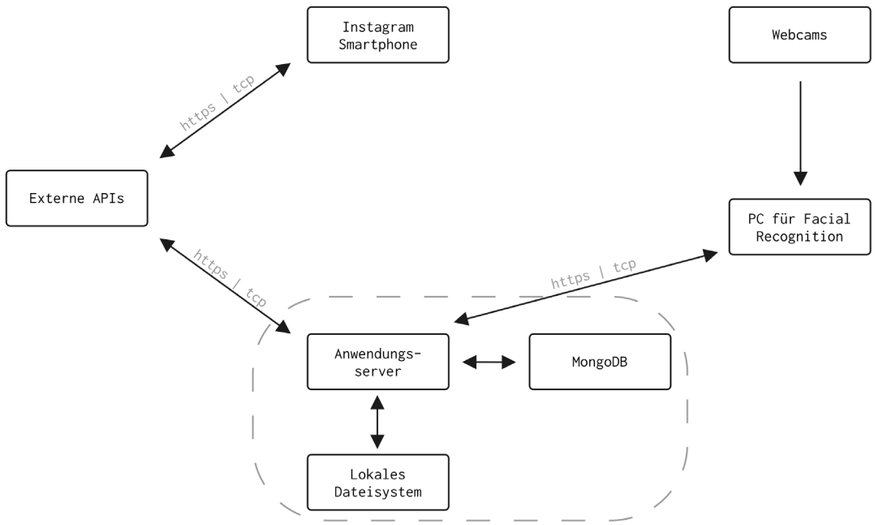


Abb.10: {Systemdiagramm}

Den Startpunkt des Systems bildet ein Smartphone, von dem durch das Team von You, eine Instagram Story mit dem Instagram Nutzernamen des Besuchenden geteilt wird. Diese Story wird über das https Protokoll an die externe Instagram API übermittelt, sodass im nächsten Schritt von dem Anwendungsserver der verlinkte Nutzername extrahiert und mit weiteren Daten in der Datenbank MongoDB gespeichert wird. Bilder der beobachteten Personen werden in einem lokalen Dateisystem gespeichert.
Die in der Umgebung verteilten Webcams übertragen währenddessen ihr Bildmaterial an einen PC, auf dem die *Facial Recognition* läuft. Die Ergebnisse der *Facial Recognition* werden über das https Protokoll an den Anwendungsserver übermittelt, wo sie weiterverarbeitet werden können.

author: { ef }
}

Hardware: {

Damit You die Personen über Kameras sehen kann, müssen PCs aufgestellt werden, die zwar klein sein können, jedoch über genügend Rechenleistung verfügen müssen, damit das Face-Tracking Programm über genügend Bildinformationen verfügt. Die Software die das Face-Tracking ermöglicht, basiert auf den Modulen von Tensorflow. Dieses Modul empfiehlt eine CUDA Architektur ausgerüstet zu haben, um eine gewisse Lauffähigkeit zu ermöglichen. Eine solche Architektur wird von Grafikkarten von Nvidia ermöglicht und ist in diesen seit 2007 verbaut. Für das System von You wird eine Grafikkarte von Nvidia verwendet, die diese Architektur vorweist. Diese Grafikkarte ist aus der vergangenen Generation und lässt die Berechnungen zu, die für das Webcam Tracking benötigt werden. Darüber hinaus ist es somit auch möglich, das System für weitere Projekte einzusetzen, welche über Grafikansprüche verfügen.

Für jeden PC, neben dem Anwendungsserver, der in einer Ausstellung verteilt ist, wird eine Webcam benötigt. Bei der Webcam ist es wichtig, dass diese über eine Auflösung von mindestens 1280 x 720 Pixel verfügt. Somit wird eine Bildqualität erreicht, welche sicherstellt, dass die Gesichter von der Software korrekt erkannt werden und ein guter Vergleich mit der Gesichtsdatenbank erfolgen kann. Hierbei gilt auch, je höher die Auflösung, desto besser die Gesichtserkennung aber damit steigt auch der Preis.

Zusätzlich werden noch Monitore verwendet. Hierfür können einfache 16:9 Monitore verwendet werden. Es muss darauf geachtet werden, über welche Eingänge sie verfügen und ob diese mit den Ausgängen der Grafikkarte übereinstimmen.

Um diese Installation in einer Ausstellung zu verwenden, müssen mindestens 3 Stationen aufgebaut werden, welche die Besuchenden filmt und analysiert. Eine Station besteht dabei aus einem Monitor, einem PC, Tastatur und Maus.

Damit die Teile des Systems untereinander kommunizieren können, wird ein eigenes Netzwerk über einen eigenen Router errichtet, zu dem kein anderer Teilnehmer Zugriff hat. Der Anwendungsserver ist der einzige Teilnehmer des Systems, der Zugriff zum Internet haben sollte, da von hier aus alle Daten von den externen APIs und Datenquellen abgefragt werden.

Der Anwendungsserver ist ebenfalls ein weiteres lokales System, welches alle Daten verarbeitet. Der Anwendungsserver verfügt, wie die Stationen in der Ausstellung, über Monitor, Tastatur und Maus.

author: { jm }
}

Software: {

You besteht seitens der Software aus mehreren Komponenten, die untereinander kommunizieren und in Abhängigkeit zueinander stehen.

Das Herz von You ist der Anwendungsserver, auf dem alle Daten zusammen kommen und unter Umständen weitergegeben werden. Nachfolgend werden alle Software Komponenten aufgelistet und erklärt:

Microservices:

Aufgrund der hohen Anzahl der unterschiedlichen Systeme und deren unterschiedlichem Verhalten, ist es von Nöten, sie in Microservices aufzuteilen und so innerhalb des Systems für die anderen Komponenten zu öffnen. Ziel der Microservices ist es, die einzelne Services systematisch voneinander zu trennen um so eine bessere Struktur innerhalb der Anwendung zu bekommen. Dies wird ermöglicht, indem sie auf eine für sie bestimmte URL Route hören. Folgende URL Routen werden vergeben:

- /api > REST API
- /instagram > Abfrage von Instagram Inhalten
- /pinterest > Abfrage von Pinterest Inhalten
- /facebook > Abfrage von Facebook Inhalten
- /face > Verarbeitung der Face Recognition Anfragen
- /media > Lokales Dateisystem

Der Vorteil bei so einem System ist die Flexibilität. Es können sehr schnell neue Anwendungen in das System eingebunden werden und mit den anderen Programmen kommunizieren. Es macht, dank Express.js, die Verarbeitung von

HTTP-Anfragen einfacher. Durch diese Library lassen sich auch in den einzelnen Programmen Unterrouten erstellen, um die Abfrage und Verarbeitung von Daten organisierter zu machen.

MongoDB:

Um unsere Daten in einer Schnittstelle zur Verfügung zu stellen, wird eine MongoDB Instanz verwendet, um die Daten aus den API Anfragen an die sozialen Netzwerke zu speichern.
Damit diese Daten über eine REST Schnittstelle den anderen Komponenten zur Verfügung gestellt werden, wird das Node Module Express verwendet, dass das URL Routing übernimmt und es so möglich macht zu bestimmen welche Daten bei welcher Route zurückkommen.

Instagram Private API:

Die Library Instagram Private API (Dmitry, 2019) bietet die Möglichkeit, Funktionen von Instagram zu verwenden, welche mit ihrer eigenen API nicht mehr möglich sind, da diese im April 2018 drastisch eingeschränkt wurde (Gummadi, 2018). So ist es möglich mittels dieser API an einen Nutzer programmatisch Privatnachrichten zu senden. Dies eröffnet dem System die Möglichkeit, basierend auf einem Auslöser das Skript auszuführen. Außerdem werden Funktionen, wie das Auslesen der Profile und dessen Medien freigegeben. Diese Daten können dann über andere Komponenten weiterverarbeitet und in die Datenbank übertragen werden.

Daten der sozialen Netzwerke:

Die größte Herausforderung im technischen Konzept, ist das Herausfinden von Nutzerdaten und die Verifizierung, ob diese mit dem Besuchenden übereinstimmen. Hierfür wird das Skript Social Mapper (Jacob, 2019) verwendet, welches überprüft, ob ein Bild einer Person mit dem Profilbild eines Profils auf sozialen Netzwerken übereinstimmt. Zusätzlich benutzt es noch den Namen der Person als Zusatz um die Suche nach der Person auf den Namen einzugrenzen. Mit

diesem Profil ist es möglich soziale Netzwerke wie Facebook, Instagram, Twitter, LinkedIn und Pinterest nach einer Person zu durchsuchen und alle zutreffenden Ergebnisse aufzulisten. Der Vorteil dieser Software ist, dass es auf die Bild Daten zurückgreifen kann, die unser System zur Verfügung stellt.

author: { jm }
}

Machine Learning: {

Machine Learning ist die Programmierung von Computern zur Optimierung einer Leistung anhand von Beispieldaten oder Erfahrungen aus der Vergangenheit. Es wird benötigt, wenn, wie im Fall von You, ein Computerprogramm nicht als Lösung für ein bestimmtes Problem genügt und stattdessen Beispieldaten oder Erfahrungen verarbeitet werden müssen (Alpaydin, 2009).
Das System muss aufgrund der Gesichts-, Objekt- und Stimmungsanalyse von Bildern riesige Datenmengen analysieren und klassifizieren. Da dieser Job in dem Ausmaß nicht von einem Menschen übernommen werden kann, setzt das System auf Machine Learning.
Aus Datenschutzgründen wurde beschlossen auf den Machine Learning Service von großen Unternehme wie Microsoft und Google zu verzichten. Alles soll Lokal auf den You Servern laufen.

Social Media Analysis:

Für das Tracking der Person und das unkenntlichmachen ihres Gesichtes muss zuerst maschinell in Bildern ein oder mehrere Gesichter erkannt werden. Dafür wird auf die Library face-api.js zurückgegriffen (Mühler, 2018/2019). Das ist eine browserbasierte JavaScript API die auf tensorflow.js basiert. Im Test der Software konnte das Team eine hohe Zuverlässigkeit bei der Erkennung von Gesichtern feststellen. Außerdem wird die Software laufend aktualisiert und ist sehr gut dokumentiert. Mit Hilfe dieser Library können nicht nur Gesichter, sondern auch die Stimmung des Gesichts analysiert werden (siehe Screenshot).

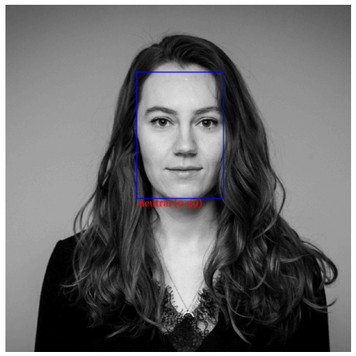


Abb.11: {Beispiel Gesichtserkennung}

Um noch mehr Daten über den Nutzen den zu generieren sollen außerdem Objekte in Bildern erkannt werden. Dafür wird der ml5.js imageClassifier verwendet (ml5js, o. J.).

Live Data Analysis:

Da die Nutzenden auch in der Umgebung live getrackt werden sollen wird auch hier die face-api.js eingesetzt. Das Beispiel das hier als Grundlage genutzt wird ist das Webcam Face Tracking (Mühler, o. J.).

author: { ef }
}

Speicherung von Daten: {

Das Aufsetzen der Datenbank erfolgt mit MongoDB, einer dokumentenorientierten NoSQL-Datenbank, in der alle Daten des Nutzerprofils gespeichert werden. Es wird ein Datensatz als Modell vorgegeben (siehe Datenmodell), anhand dessen das Profil angelegt wird. Es wird ein Dokument mit allen Nutzern geben, welches verwaltet wird. Jedem Nutzer ist eine eindeutige ID zugeordnet. Die Profile werden als JSON Files abgelegt.
Der Vorteil einer dokumentenorientierten Datenbank ist, dass sie keine Tabellen durchsucht und keine SQL Requests macht und daher schneller ist. Außerdem kann sie viele Schreib- und Leseanfragen besser verarbeiten.
Der Vorteil von MongoDB liegt darin, dass beispielsweise Fehlermeldungen ausgegeben werden können. Es gibt ebenfalls die Möglichkeit Felder einzeln abzufragen. Auch wird es in der Industrie und bei vielen Firmen wie beispielsweise bei Adobe, Bosch und Amazon verwendet (MongoDB, 2019).

Datenmodell:
Dieses Modell gibt einen groben Ausblick auf die Daten, die erhoben werden könnten. Es kann und wird sich im Laufe der Umsetzung verändern und anpassen.

```
UserModel = {
      instagram: {                    pinterest: {
            username: String,                 boards: [{
            profilePicture: String,                 name: String,
            fullName: String,                       pins: [],
            city: String,                     }],
            locations: [{                     username: String,
                  type: String,               profilePicture: String,
            }],                               },
            description: String,              facebook: {
            follower_count: Number,                 images: [],
            follower_list: [],                      info: String,
            following_count: Number,                dob: Date,
            following_list: [],                     friends: [],
      },                                      }
                                        }

author: { sl }
}
```

Datenschutz: {

Die Hauptaufgabe von You ist das Sammeln und Verarbeiten von personenbezogenen Daten, die über jemanden im Internet gefunden werden können. Das dabei die Sicherheit der Daten und der Datenschutz im System eine große Rolle spielt, ist dem Team bewusst und wichtig.

Lokale Verarbeitung:

Um sicherzugehen, dass Daten die erhoben wurden nicht an dritte Parteien weitergegeben werden, muss das System lokal auf einem Rechner funktionieren. Das bedeutet, dass alle Daten in einer lokalen MongoDB Instanz gespeichert werden, die mit einem Passwort gesichert wurde, welches den Sicherheitsrichtlinien entspricht. Es muss sichergestellt werden, dass Systeme wie die Gesichtserkennung von Fotos auch lokal funktionieren und diese keine personenbezogenen Daten an Dritte weitergegeben werden.

Löschung:

Um für eine vollständige Sicherheit der Daten zu sorgen, werden alle Daten nach einer Erhebung und das durchlaufen des Projektprozess unwiderruflich gelöscht. Dies ist natürlich auf Wunsch des Nutzer direkt möglich, wenn er nicht möchte dass seine Daten verarbeitet werden.

Datenschutzerklärung:

Da sich das Projekt auf dem Boden der Europäischen Union befinden, müssen wir nach der DSGVO handeln und arbeiten. Es wird dafür gesorgt, dass auf Ausstellungen auf denen das Projekt präsentiert wird, eine Datenschutzerklärung ausgehangen wird, welche über alle Rechte aufklärt die eine nutzende Person hat. Zu dem sind wir dazu verpflichtet, dies zu tun, da sonst nicht über die Erhebung von personenbezogenen Daten aufgeklärt wird und so eine Strafbarkeit auftreten könnte.

```
author: { jm }
}
```

Proof Of Concept: {

Für den technischen Proof Of Concept (POC) wurden folgende Komponenten als kritisch betrachtet und somit in dem ersten Machbarkeitsnachweis berücksichtigt: Zuerst muss sichergestellt werden, dass der Nutzername aus den Instagram Stories extrahiert werden kann. Scheitert diese Komponente, schlägt das ganzes Vorhaben fehl, da nur so mehr Daten über den Nutzenden gesammelt werden und dieser von You kontaktiert werden kann. Da die Instagram Story direkt über den Instagram Kanal von You geteilt wird, kann anhand eines Scripts der verlinkte Nutzername gefunden werden.
Danach erfolgt über den extrahierten Nutzername eine Datenabfrage externer APIs, um an möglichst viele Daten des Nutzenden zu kommen. Dafür wird ein Library names Social Mapper genutzt (Jacob, 2018/2019).
Das Tracking in der Umgebung ist insofern Teil des POC, da nur so bekannt ist, ob ein Beacon entnommen wurde und somit ein Nutzender in der Umgebung unterwegs ist. Dies ermöglicht außerdem dem Nutzenden an festgelegten Standorten Nachrichten zu schicken und festzustellen, wann er sich in der Nähe einer der in der Umgebung verteilten Bildschirme befindet.
Auch die Gesichtsanalyse ist Teil des POC. Es wird geprüft, ob die Software face API, die für die prototypische Umsetzung verwendet wird, ein oder mehrere Gesichter in einem Foto findet (Mühler, o. J.).
Essentiell für die Vermittlung eines *Stalking* Erlebnisses ist außerdem das direkte Anschreiben des Nutzenden über ein soziale Netzwerk. Hierfür wird ein Skript verwendet, welches einer beliebigen Person Nachrichten auf Instagram senden kann.
author: { ef }
}

Prototypische Umsetzung: {

Das Konzept zeigt eine gute Wunschvorstellung davon, wie es am ehesten funktionieren könnte und bei dem das Ambiente am ehesten verdeutlicht wird. Das Tracking von Personen über Kameras benötigt jedoch sehr teures Equipment, welches aber nicht in das Budget für einen Prototypen passt. Daher werden zum Verfolgen der Personen sogenannte Beacons verwendet. Diese werden am Eingang dem Menschen in Form von Veranstaltungsbadges umgehangen. An diesen

Badges gibt es einen Mechanismus, mit dem man die Schnüre verengen kann. Dieser Mechanismus wird nachgebaut und 3D-gedruckt, um mehr Platz für ein Beacon zu schaffen. Diese Badges werden, nachdem ein Foto mit den Besuchenden gemacht wurde, den Personen umgehangen und von Scannern in der Ausstellung getrackt.
author: { jm }
}

Systemdiagramm Prototyp: {

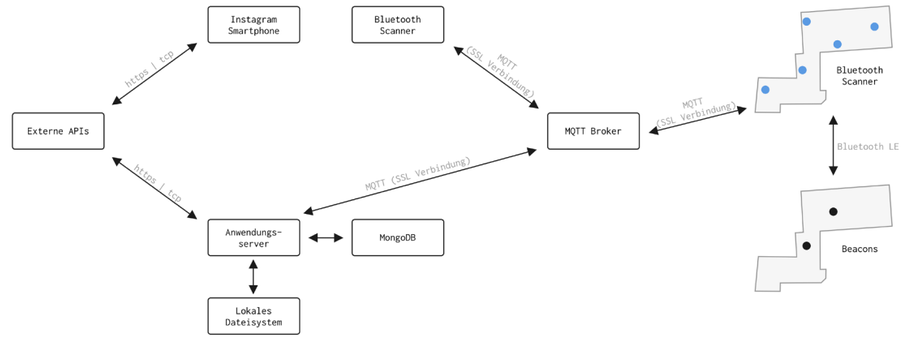


Abb.12: {Systemdiagramm Prototyp}

Im Gegensatz zur konzeptionellen Umsetzung baut das System hier für das Tracking der Personen in der Umgebung auf Beacons auf. Die Komponenten Smartphone, Externe APIs, Anwendungsserver, lokales Dateisystem und die Datenbank MongoDB bleiben bestehen.
Die *Facial Recognition* wird wie folgt ersetzt: Ein Bluetooth Scanner prüft permanent, ob ein Beacon aus der Sammlung entnommen wurde und schickt diesen Status über *MQTT* mittels einer *SSL* Verschlüsselung an den *MQTT* Server („Broker“). Die im Raum verteilten Bluetooth Scanner kommunizieren mit den an die Nutzenden verteilten Beacons über Bluetooth LE. Werden die Bluetooth Scanner durch vorbeikommende Beacons getriggert, wird das über *MQTT* mittels einer *SSL* Verschlüsselung an den *MQTT* Server übermittelt. Dieser leitet den Status an den Anwendungsserver weiter, ebenfalls über mittels einer *SSL* Verschlüsselung.
author: { ef }
}

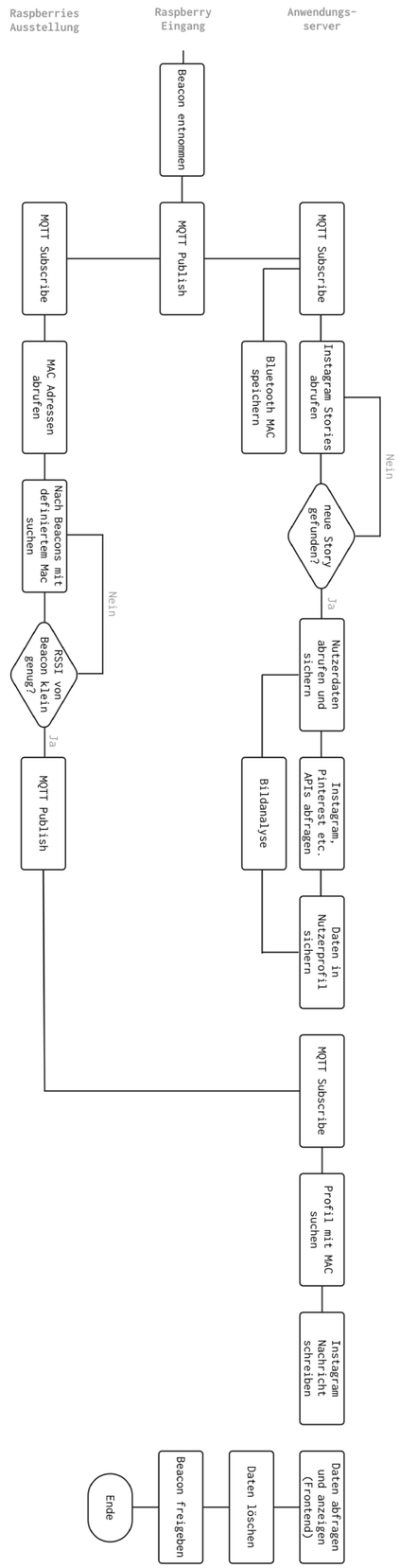


Abb.13: {Ablaufdiagramm Prototyp}

Ablaufdiagramm Prototyp: {

Zu Beginn der Ausstellung wird den ausgewählten Besuchenden ein Badge mit einem Beacon gegeben. Wenn ein Beacon am Eingang entnommen wird, wird dessen Status über ein *MQTT* Publish veröffentlicht. Der Beacon dient zur eindeutigen Identifizierung der Besuchenden. Dieser sendet nun ein Signal an mehrere Raspberry Pis aus. Von hier aus passieren zwei parallele Prozesse.

Zum einen speichert der zu diesem Topic abonnierte Anwendungsserver die Bluetooth *MAC*-Adresse des Beacon. Danach wird bei Instagram abgefragt, ob eine neue Story geteilt wurde. Dies passiert als Loop, bis die Story gefunden wurde. Die eingebetteten Nutzerdaten werden abgerufen und gesichert. Es wird eine Bildanalyse gestartet, um die Fotos aus dem Instagram-Feed des Nutzers nach Gesichtern abzusuchen und diese zu erkennen. Diese Bilder werden an Bildschirme übermittelt, welche von Raspberries gesteuert werden. Die Raspberries erhalten *MQTT* Nachrichten mit den Profildaten und den Pfad des Bildes auf dem Dateiserver.
Gleichzeitig werden weitere Daten von Instagram und Pinterest über deren API abgefragt. Anschließend werden alle erfassten Daten in einem Profil in der Datenbank abgespeichert.

Zeitgleich zum *MQTT* Subscribe des Anwendungsserver abonnieren sich auch die Raspberries auf der Ausstellung zum Topic. Die *MAC* Adressen werden abgerufen und nach Beacons mit definierter *MAC* gesucht. Nun warten die Raspberries darauf, dass die *RSSI* eines Beacons klein genug ist, um diesen wahrzunehmen und senden darauf diesen Status über *MQTT* an den Anwendungsserver. Dort wird das Profil anhand der *MAC* gesucht, um daraufhin über Instagram Nachrichten schreiben zu können.
Es wird eine Vielzahl dieser Zonen geben, daher wiederholt sich der Prozess.

Zum Ende des Ablaufes werden alle gesammelten Daten im Frontend abgefragt und dargestellt. Die betroffene Person kann nun durch das Betätigen eines Buzzers die eigenen Daten im lokalen System löschen. Daraufhin wird der Beacon freigegeben und der Prozess kann erneut beginnen.

author: { sl }
}

Management

72 Marktanalyse
78 You
80 Business Model Canvas
81 Full Life Cycle Use Case
83 Strategie und Planung
88 Rechtsform
89 SWOT
90 Planung und zukünftige Schritte
91 Ausblick

Marktanalyse: {

Museen und Ausstellungen: {

Ein Museum ist mehr als ein Ort, an dem Objekte ausgestellt und konserviert werden. Zusammen mit dem dramatischen Anstieg des Kulturtourismus in den letzten Jahrzehnten ist die Zahl der Museen weltweit von 22.000 im Jahr 1975 auf heute 55.000 gestiegen.
Museen können eine führende Rolle bei der Stärkung der Kreativwirtschaft auf lokaler und regionaler Ebene spielen. Auch im gesellschaftlichen Kontext bringen sie großen Mehrwert, indem sie als Diskussionsplattformen für komplexe gesellschaftliche Themen dienen und die Beteiligung der Öffentlichkeit fördern (Unesco, 2016).
Die Zahl der Besuchenden von Museen ist in den letzten zehn Jahren um fast 10 Millionen gestiegen. In Berlin werden mit 4,6 Besuchen je Einwohnerin und Einwohner pro Jahr die meisten Museumsbesuche vermerkt. Ganz Deutschland besucht durchschnittlich 1,4 Mal im Jahr ein Museum (Statistische Ämter des Bundes und der Länder, 2018).

Museen können in ihrer Art unterschieden werden. Folgende Kategorien haben sich etabliert: Historische und archäologische Museen, Kulturgeschichtliche Spezialmuseen, Kunstmuseen, Naturkundliche Museen, Naturwissenschaftliche und technische Museen, Schloss- und Burgmuseen, Volks- und Heimatkundemuseen und sonstige museale Einrichtungen.
Auch die Trägerschaft kann variieren. Die verbreitetste Trägerschaft ist die der lokalen Gebietskörperschaft, worunter zum Beispiel eine Gemeinde fällt. Der zweithäufigsten Träger sind Vereine. Einige Museen sind staatlich getragen, andere von Privatpersonen (Statistisches Bundesamt, o. J.).

Eine Ausstellung ist eine Veranstaltung, bei der bestimmte künstlerische oder wirtschaftliche Arbeiten zur Schau gestellt werden (Duden, o. J.). Eine Unterform ist die Sonderausstellung, bei der zusätzlich zu den ständig ausgestellten Exponaten ein (Kunst-)Werk für einen begrenzten Zeitraum und zu einem bestimmten Thema ausgestellt wird (Duden, o. J.).

author: { ef }
}

Marktbeschreibung: {

You ist eine interaktive Installation, die den Besuchenden die Augen bezüglich ihrer Menge an *Social Media* Daten öffnet und gleichzeitig deren Missbrauchspotenzial aufzeigt. Die Installation wird als temporäre Sonderausstellung in Museen und anderen Einrichtungen präsentiert. Unsere erste Anlaufstelle in Museen sind Kurator/innen. Sie sind zuständig für die Gestaltung der Ausstellung, aber auch für die Bearbeitung von Anfragen.

author: { ef }
}

So werden Kuratoren gewonnen und gebunden: {

Mit einem Pitch, der zeigt was das Team ausmacht und antreibt, sollen Kuratoren*Innen für das Projekt gewonnen werden. Antworten auf Fragen der potenziellen Kunden könnten wie folgt lauten:

Warum glauben Sie an diese Idee? Was inspiriert und treibt Sie an?
Wir wollen polarisieren! Ein Safespace in Ihrem Museum entstehen zu lassen, damit zu schockieren und einen Lerneffekt zu erzielen ist unser Antrieb. Es soll klar werden, welche Informationen Menschen Tag für Tag offenlegen ohne sich dessen bewusst zu sein. Unsere Nutzer sollen sich in einem sicheren Raum bewusst werden was auch in der realen Welt geschehen könnte, wenn sie nicht achtsam und bedacht mit den persönlichen Informationen umgehen. Die Größe des möglichen Marktes wird im folgenden anhand des TAMs dargestellt.

author: { dt }
}

TAM: {

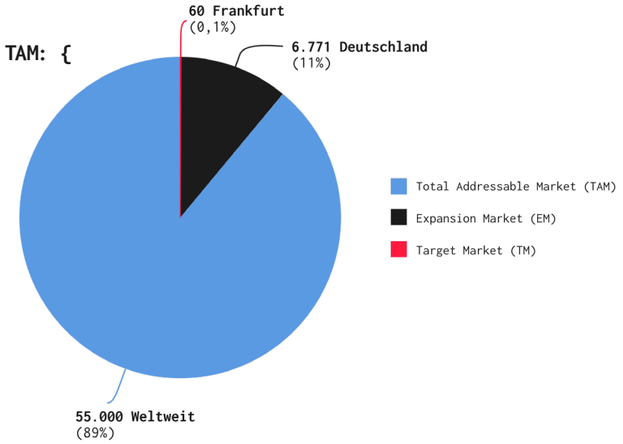


Abb.14: {Kreisdiagramm zum TAM}

Der für den Start vorgesehene Target Market (TM) umfasst die etwa 60 Museen in ganz Frankfurt (Frankfurt.de, o. J.). Für You besonders interessante Early Adopters wären das Museum für Kommunikation, die Schirn Kunsthalle und die Experiminta.
Das Museum für Kommunikation ist deshalb als Kunde relevant, da es mit Fokus auf Kommunikation, neue Medien und kulturelle und gesellschaftliche Entwicklungen genau das passende Thema für die Installation bietet. Zusätzlich werden interaktiven Führungen angeboten, welche besonders Schulklassen und Familien anlocken, die zur Zielgruppe gehören (Frankfurt.de, o. J.).

In der Schirn Kunsthalle werden ebenfalls gesellschaftliche Themen diskutiert und präsentiert. Das Museum selbst begreift sich als „Ort der Entdeckungen und Spiegel der Gesellschaft“. (Frankfurt.de, o. J.) Außerdem arbeitet es eng mit anderen renommierten Museen zusammen, wie dem Museum of Modern Art oder dem Guggenheim Museum in New York City. Dadurch kann sich die Chance eröffnen, schnell in den Kontakt mit weiteren Museen zu kommen, auch international (Frankfurt.de, o. J.).

Die Experiminta gilt als Zentrum des Wissens und des Lernens, da hier die Besuchenden sehr viel selbst experimentieren können. „Alltägliche, aber auch außergewöhnliche Experimente und Attraktionen bietet die Ausstellung für alle

Altersgruppen.“ (Frankfurt.de, o. J.) Ein Museum, in das die Besuchenden schon mit dem Erwartung kommen, selbst viel ausprobieren zu können, ist ein idealer Ort für die Installation (Frankfurt.de, o. J.).
Der Expansion Market (EM) umfasst alle Museen in Deutschland. Stand 2017 waren das fast siebentausend, in denen im gleichen Jahr etwa neuntausend Sonderausstellungen stattgefunden haben (Institut für Museumsforschung, 2017). Mit weltweit etwa 55 Tausend Museen ist der Total Addressable Market (TAM) sehr gut aufgestellt (Unesco, 2016).

author: { ef }
}

7 next customers: {

Im folgenden werden die sieben nächsten Kunden vorgestellt, die interessant werden, nachdem You erfolgreich mit den Early Adopters durchgestartet ist:

ZKM Karlsruhe:
Das Zentrum für Kunst und Medien Karlsruhe ist ein potenzieller Kunde, da bereits ihre Ausstellung Open Codes mit dem Fokus auf „Die Welt als Datenfeld“ ein voller Erfolg war. „Wir wollen die Welt besser verstehen und greifen daher aktuelle Themen auf, um die Öffentlichkeit auf Fragen, Hintergründe und Probleme aufmerksam zu machen.“ (ZKM, o. J.)

Museum für Kommunikation Berlin:
Wie das Museum für Kommunikation in Frankfurt, ist auch das in Berlin ein potenzieller Kunde, da der Fokus auch hier auf Kommunikation, neuen Medien und kulturellen und gesellschaftlichen Entwicklungen liegt (Museum für Kommunikation Berlin, o. J.).

Technoseum:
Das Technoseum in Mannheim ist eines der größten Technikmuseen in Deutschland. Im Bereich Naturwissenschaft und Technik bietet es viele Experimente für die Besuchenden an (Technoseum, o. J.).

Deutsches Spionagemuseum:
Passend zu dem Thema Spionage könnte You hier für besonders viel Aufregung sorgen. Selbst das Museum wirbt mit „[...] lassen Sie Ihr »sicheres« Passwort knacken und hacken Sie Ihre Lieblings-Website!“. (Deutsches Spionagemuseum Berlin, o. J.)

Darmstadt Konferenz:
Um mit der You Botschaft auch ein Fachpublikum für die Bereiche Politik, Forschung und Digitalwirtschaft zu erreichen, ist die Darmstadt Konferenz am 12. und 13 Juni 2019 ein idealer Ort (Digitalstadt Darmstadt, o. J.).

Deutsches Museum München:
In München ist das Deutsche Museum, das sich mit dem als 30 Ausstellungen den Themen Naturwissenschaft und Technik widmet. Dieses Jahr ist es auch Schauplatz für das Wissenschaftsjahr 2019, das sich mit dem Thema Künstliche Intelligenz beschäftigt (Deutsches Museum München, o. J.).

Deutsches Museum Nürnberg:
In Nürnberg wird 2020 das „erste Museum der Zukunft“ eröffnet. Hier werden zukunftsträchtige Technologien diskutiert und deren einhergehende Konsequenzen für den persönlichen Alltag und die Gesellschaft (Deutsches Museum Nürnberg, o. J.).

author: { ef }
}

Konkurrenz: {

“name”: “Hansel & Gretel”,
“autor”: “Jacques Herzog, Pierre de Meuron, Ai, Weiwei”,
“inhalt”: “Zwei Architekten und ein Künstler und Aktivist entwarfen eine immersive Installation, die sich mit den Themen Überwachung und Datenschutz im Zeitalter der *Social Media* beschäftigt. Beim Betreten der Galerie gehen die Besuchenden durch mehrere schwach beleuchtete Gänge, die zum Hauptraum der Galerie führen. Das Hauptraum ist mit einem Netzwerk von Infrarot-Sensoren und Drohnen gefüllt, die die Bewegungen der Gäste verfolgen und in einen Online-Livestream übertragen.” (Thompson art center, o. J.)

“name”: “The glass room”,
“autor”: “Tactical Technology Collective”,
“inhalt”: “The Glass Room ist eine Sammlung von Kunstwerken, laufenden Projekten und sensorischen Erfahrungen, die das Leben im Internetzeitalter erforschen. Die Show soll die Besucher über die vielfältigen Einsatzmöglichkeiten ihrer Daten informieren. Die ausgestellten Artefakte reichen von amüsant, wie eine alphabetisch geordnete Sammlung von 4,6 Millionen ausgelaufenen LinkedIn-Passwörtern, bis hin zu erschreckend, wie ein ferngesteuerter Fruchtbarkeitschip, der eines Tages zur Kontrolle der Fruchtbarkeitsraten in Entwicklungsländern verwendet werden könnte.” (Teirstein, 2016)

“name”: “Außer Kontrolle? Leben in einer überwachten Welt”,
“autor”: “Museum für Kommunikation Berlin”,
“inhalt”: “Diese Ausstellung wurde 2014 im Museum für Kommunikation in Berlin und Frankfurt ausgestellt. Thematisiert wird das systematische Scannen personenbezogener Daten und wie Informationen über Menschen gesammelt und genutzt werden können. Die Besuchenden können mit einem Wanzensuchgerät oder einem Fingerabdruckscanner selbst experimentieren (Museum für Kommunikation Berlin, 2014).”

author: { ef }
}

You: {

#Ziele der Nutzenden

mit einem guten Gefühl aus dem Museum gehen
ein inspirierendes Erlebnis
etwas zu erzählen haben

#Markenziele

zum Nachdenken anregen
schockieren und aufklären
Daten erlebbar machen

#Unternehmensziele

Museen/Ausstellungen und ihre Besuchenden begeistern
so viele Menschen wie möglich erreichen
über You wird ohne eigenes Zutun gesprochen
zu besserem Umgang mit den eige -nen Daten anregen

}

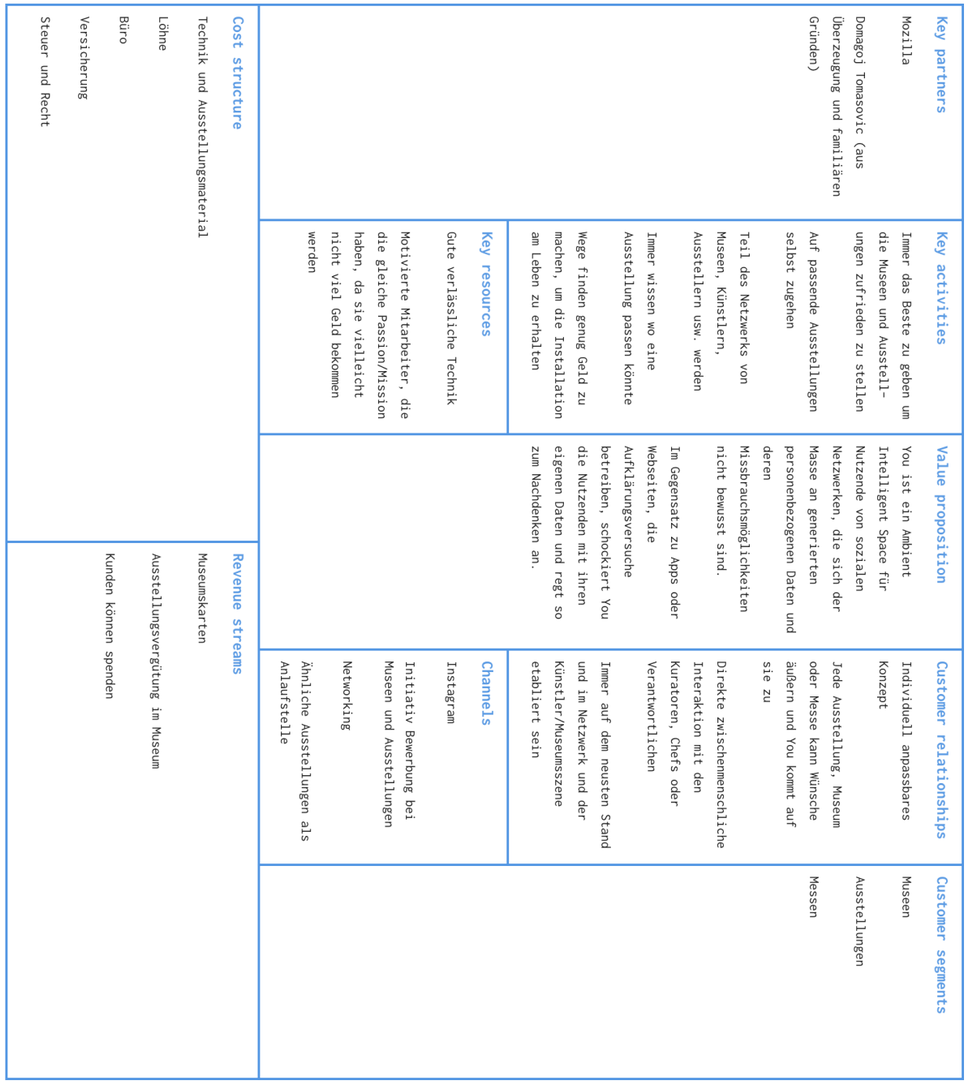


Abb.15: {Business Model Canvas}

Full Life Cycle Use Case: {

Wie werden die Nutzenden erfahren, dass sie einen Bedarf für You haben beziehungsweise etwas ändern müssen?
Weder der Endnutzende noch die Museumsbetreiber bzw. Kuratoren wissen von You. In dem Anfangsstadium werden wie oben bereits genannt, drei Museen ausgewählt. Dessen Kurator/innen wird You mit einem Pitch präsentiert. Das Besondere an You ist, man weiß im ersten Moment nicht wer oder was er/sie/es ist, und somit auch nicht, dass man You braucht. Genau das ist der Punkt. Das Schockierende ist die Überraschung. Erst im Laufe des Museumsbesuchs werden die Nutzenden polarisiert.

Wie werden die Nutzenden von You erfahren?
Die Nutzenden erfahren von You indem sie Museen oder Ausstellungen besuchen, in denen You ausgestellt wird. Zu einem späteren Zeitpunkt könnte man über das Internet, Werbung, Nachrichtenseiten, Fachzeitschriften, *Social Media* oder ähnliches von You zu hören bekommen. Das Team geht davon aus, dass es von You schnell erste Erfahrungsberichte geben wird. Trotzdem bedeckt zu bleiben und ohne Ankündigung in verschiedenen Museen zu finden zu sein, soll die Besuchenden reizen und vielleicht auch dazu bringen das ein oder andere ungewöhnliche Museum zu besuchen. Dies ist übrigens ein weiterer Grund für Museen You zu beauftragen.

Wie werden die Nutzenden You analysieren?
Ist die Message dem Nutzer klar geworden, sollte er anfangen anders über seine Daten nachzudenken und sich nach dem Erlebnis, falls nötig, näher mit dem Thema beschäftigen. Außerdem könnte der Nutzer You mit ähnlichen Angeboten, Webseiten oder Apps in Verbindung bringen, sowie diese nutzen um seine Daten zu schützen oder im nächsten Schritt bewusster mit ihnen umzugehen. Vielleicht haben Nutzende schon andere Installationen mit ähnlichem Themenschwerpunkt besucht und vergleichen diese im Nachhinein mit You.

Wie können die Nutzenden You erwerben?
Indem sie ein Museum besuchen, könnte es passieren, dass Besuchende You begegnen. Die Museen selbst können sich bei uns bewerben, nachdem sie durch andere Museen auf You aufmerksam gemacht wurden.

Wie können die Nutzenden You installieren?
Da der Aufbau sehr viele bewegliche Teile und Komponenten besitzt und damit komplex ist, muss You durch geschulte Mitarbeiter aufgebaut und getestet werden. Alles was Nutzende machen müssen, ist die Anfrage von You in einem ihrer Messenger anzunehmen und sich auf das Erlebnis einzulassen.

Wie werden die Nutzenden You erleben?
Die Nutzenden verbringen einige Stunden in einem Museum und werden während dieser Zeit von You angeschrieben. You sendet ihnen daraufhin immer wieder ungewöhnliche und verschreckende Nachrichten. Die Inhalte sind zwar offen zugänglich, aber der Person aufgrund der Menge der vorhandenen Daten im Internet vielleicht gar nicht mehr in Erinnerung, da sich You auch nicht nur auf die neusten Posts bezieht. Die Nachrichten sorgen für Verwirrung, welche dann von getarnten Mitarbeitern von You aufgelöst werden.

Wie kann der Mehrwert durch You quantifiziert werden?
Das wichtigste ist Zuhören! Wünsche, Anregungen und Feedback, all das soll in regelmäßigen Abständen von den, für das Museum zuständigen, Personen eingeholt werden. Außerdem werden all diejenigen, die You erlebt haben, gefragt, wie es ihnen ergangen ist. Damit kann You immer besser auf seine Nutzenden angepasst werden.

Wie wird für You bezahlt?
Indirekt bezahlen die Besuchende mit ihren Museumstickets. Direkt bezahlen die Museen Fixkosten, wie zum Beispiel die Mitarbeiter, die You zu diesem Zeitpunkt benötigt, sowie ein festes Grundpaket, das die Weiterentwicklung von You mitfinanziert.

Wie werden die Nutzenden Support erhalten?
Ein Team von zwei Personen wird die Ausstellung immer begleiten und sicherstellen, dass alles problemlos funktioniert. Zudem werden die Besuchenden nach dem Erlebnis von diesen Mitarbeitern aufgeklärt.

Wie kann man noch mehr von You erleben oder wie wird ein Bewusstsein für die Existenz von You geschaffen?
Wenn You polarisieren konnte, werden Menschen ihre Freunde und Bekannte im besten Fall in das gleiche Museum mitnehmen und sich auf die bevorstehende

Überraschung freuen. Das You nicht ewig geheim bleiben wird ist dem Team bewusst. Pressemitteilungen, Posts in sozialen Medien und Mundpropaganda werden auch ohne eigenes Zutun des Teams entstehen. You könnte Nutzende zudem privat auf Instagram als Freund hinzufügen und auf sich aufmerksam machen, ohne Ihnen seine Intention zu verraten.

Wie trennen die Nutzenden sich wieder von You?
Besuchende trennen sich von You indem sie einen Löschen Button drücken und alle Daten, die You über sie in der kurzen Zeit zusammengesucht hat, löschen. Alles was als Erinnerung an das Erlebnis bleibt ist der Chatverlauf.

author: { dt }
}
}

Strategie und Planung: {

Markteintritt: {

Die Vermarktung des Konzeptes unterteilt sich in zwei Phasen:

Phase 1: Open Testing
Die erste Phase wird als „open testing“-Phase bezeichnet. Das Ziel in dieser Phase ist, You in einer Umgebung zu testen, in der die Installation später funktionieren soll. Da das Team nur Annahmen treffen kann, sowie kleine Tests mit wenigen Menschen in kleinen Räumen diese Annahmen stützen können, soll hier zum ersten Mal erprobt werden, wie You im späteren Umfeld agiert. Am Anfang sollen daher ausschließlich wenige Museen und Ausstellungen als Early Adopters fungieren. Der besondere Mehrwert ist hierbei, dass effektiv getestet, beobachtet und optimiert werden kann. Außerdem soll geprüft werden, ob Menschen so reagieren, wie es vorherige Tests zeigten und wenn nicht, wie das Konzept geändert werden muss, um den gewünschten Mehrwert zu erreichen.

Phase 2: Going Wide
Die Erkenntnisse aus Phase Zwei werden iteriert und anschließend umgesetzt. Auch hier geht es nicht um Gewinne, sondern darum den Markt und somit die

Reichweite zu vergrößern. Die erste Phase ist lediglich dafür da, das Projekt zu testen und zu verbessern, um so das bestmögliche Erlebnis für eine breite Masse zu schaffen. Da in Phase eins zunächst die Museen ausgewählt wurden, bei denen You ins Ausstellungsthema passt, soll You in der zweiten Phase in ähnlichen Museen weiter optimiert und angepasst werden.
Ist das Team zufrieden mit dem Erlebnis, dem Feedback und der Funktionsweise kann You auch in anderen Museen oder Ausstellungen, die auf den ersten Blick nicht passend erscheinen, eingesetzt werden. Gleich zu Beginn eine noch unbekannte und vielleicht kritische Nutzergruppe auszuwählen, könnte negatives Feedback auslösen, und damit schlechtes Licht auf You werfen. Da das Thema und die Art es zu Beleuchten keine leichte Kost sind, ist es wichtig, bedacht und langsam vorzugehen und erst bei einer gewissen Marktreife den Radius von You zu vergrößern.

author: { dt }
}

Testing und Produktentwicklung: {

Nach dem Launch von You wird die Produktentwicklung daher als ein essenzieller Teil des Unternehmens weitergeführt. Konstante Verbesserung ist ein zentraler Punkt um Menschen noch gezielter tracken zu können und Daten zu finden beziehungsweise zusammenzustellen, die sie schockieren und zum Nachdenken bewegen. Die Zeit nach dem Launch in den ersten drei Museen ist essentiell, da dort verschiedene Edge Cases getestet werden und You bestmöglich angepasst und optimiert wird. Hier sind Kunden- und Nutzerfeedback sehr wichtig. Dieses soll das bis dahin erstellte Konzept und die Umsetzung maßgeblich beeinflussen und falls nötig als Ansatz zu Veränderungen und damit Verbesserungen des Erlebnisses aufgenommen werden. Da am Anfang hohe Kosten entstehen, die privat und durch Spenden getragen werden, soll im besten Fall bereits nach der Testphase ein unvergessliches Erlebnis geschaffen sein.

author: { dt }
}

USP: {

Als Alleinstellungsmerkmal wird allgemein das herausragende Leistungsmerkmal bezeichnet, durch das sich ein Angebot deutlich vom Wettbewerb abhebt.

Die Hürde der heutigen Produkte für Achtsamkeit im Bereich Datenschutz und Datenumgang besteht darin, nicht wie alle anderen zu sein. Es ist einfach Menschen im Bereich Datenschutz aufzuklären, wenn diese bereits ein Interesse dafür zeigen. Menschen zu erreichen, denen nicht bewusst ist wie viele Daten über sie zu finden sind und wie unbedacht sie mit Informationen über sich umgehen, ist das Ziel von You.
Polarisieren, Aufmerksamkeit erregen und erwecken, schockieren und den Nutzenden zum Nachdenken bewegen ist der USP von You.
Apps, Webseiten und Workshops werden nicht als Konkurrenz gesehen. Sie können nach dem Erlebnis im Museum dabei helfen sich mehr in das Thema einzuarbeiten und für sich zu entscheiden, wie mit Daten in Zukunft umgegangen werden soll.

author: { dt }
}

Unternehmensstrategie: {

Da You kein Produkt ist, das von einem Endnutzer erworben wird, sondern für bestimmte Zeit auf Ausstellungen, Messen oder Museen zu finden sein soll, ist es nicht einfach eine Unternehmensstrategie festzulegen. Die Produktdifferenzierung durch Qualität, Leistung, und Lebensdauer ist wichtig, da es für das Team bedeutet, dass weniger Kosten im Bereich Reparatur anfallen. Daher ist der Zeitaufwand geringer. Jedoch werden auch Mitarbeiter benötigt.
Die Servicequalität, Lieferung und Zusatzleistungen spielen eine große Rolle, da das Team stets engagiert, bedacht und professionell agieren möchte. Museen die positive Erfahrungen mit der Installation, sowie dem Team, das hinter You steht und dessen Service gemacht hat, erzählen anderen Museen davon und könnten so neue Kunden offerieren.
Das Team sollte daher stets durch Kompetenz, Höflichkeit und Anpassungsfähigkeit überzeugen und so immer das bestmögliche Erlebnis von der Buchung der

Installation bis zum Abbau möglich machen.
Die Lieferung, sowie die Montage von You, solltel schnell und ohne große Komplikationen ablaufen. Deshalb ist es wichtig, sich schon vorher einen genauen Plan von dem Ausstellungsort zu machen und räumlichen Bedingungen genauestens zu untersuchen. Das Team möchte weder den Museumsbetrieb aufhalten, noch viele Stunden mit vermeidbaren Problemen verbringen.
All die oben genannten Punkte sollen zum Image des Unternehmens und des Teams beitragen. You ist eine Installation, die unter Umständen kritische Reaktion hervorrufen könnten. Daher ist es umso wichtiger, dass die Menschen die hinter dem Projekt stehen ein gemeinsames Ziel, ein gemeinsames Warum und eine gemeinsame Passion verfolgen. Durch Authentizität und gleiche Werte soll Vertrauen zum Unternehmen und somit auch zu You aufgebaut werden.
Deshalb sollen alle Mitarbeiter nicht nach Können, sondern nach Werten und Überzeugungen, sowie dem zum Team passenden Mindset eingestellt werden.
Wissen kann man sich aneignen, eine Einstellung muss man fühlen und leben.

author: { dt }
}

Serviceablauf: {

Initiativbewerbung oder später einmal Anfragen von Ausstellungen/Museen
Pitch und Gespräch zum Projekt
Bei Interesse > Vertrag und Verhandlungen von Konditionen

Aufbau und Setup:
Raumplanung und Installationsplanung im Vorfeld
Anpassung des Systems auf räumliche und kontextuelle Gegebenheiten (Vorlaufzeit von 2 Monaten)
Aufbaudauer von einer Nacht
Test am ersten Tag danach
Zwei Mitarbeiter werden in das Projekt einweisen

Laufender Betrieb:
ein Mitarbeiter der den Instagram Namen herausfindet (People of NewYork)
ein Mitarbeiter, der bei Problemen oder ungeahnten Reaktionen eingreifen kann

Abbau:
Abbaudauer von einem Tag
zum Ablauf des Vertrags oder der Zeitausstellung
2 aus dem Projektteam und die 2 Projektbetreuenden

Lagerung:
Am Anfang noch bei Teammitgliedern zu Hause
Später im Büro in Darmstadt

Transport:
Kombi eines Teammitglieds steht jeder Zeit dafür zur Verfügung

Entsorgung:
Alte Komponenten werden in Vereinen abgegeben
defekte Teile werden fachgerecht in Wertstoffhöfen entsorgt

author: { dt }
}

Ausgaben und Einnahmen: {

Genaue Angaben über die anfallenden Kosten finden sich im Anhang im Finanzplan, der für die ersten drei Jahre des Unternehmens angelegt wurde. Einnahmen die dort verzeichnet wurden, sind Schätzungen, die durch Gespräche mit Kuratoren und Kunstliebhabern mit einem gewissen Know How entstanden sind. Es ist schwer in dieser Branche feste Einnahmen voraus zu planen, dennoch wurde versucht in einem realistischen Rahmen die Möglichkeiten, die das Unternehmen hat, abzuschätzen.

author: { dt }
}

}

Rechtsform: {

Das Unternehmen soll zum 01.08.2019 als gUG, eine gemeinnützige Unternehmergesellschaft gegründet werden. Gemeinnützig deshalb, weil You durch unabhängige Finanzierung und effizientes Wirtschaften ein wirtschaftlich rentables Non-Profit-Unternehmen, mit gemeinnützigem Zweck sein soll. Um die Rechtsform gUG verwenden zu dürfen, muss die Unternehmergesellschaft vorläufig vom Finanzamt als gemeinnützig, mildtätig und/oder kirchlich anerkannt werden.
You ist weder mildtätig noch kirchlich, nützt jedoch der Allgemeinheit im Bereich Datenschutz und Privatsphäre und ist somit gemeinnützig. Um die Gründung ohne größere Hindernisse abzuschließen, soll dem Team ein Anwalt zur Seite stehen, der hilft den gemeinnützigen Zweck in der Satzung zu verankern.
Die gemeinnützige UG hat vier gleichberechtigte Gesellschafter/Innen, die das Stammkapital jeweils zu einem Viertel voll einbezahlen. Die vier Gesellschafter/Innen Jan Meininghaus, Elina Farber, Sarah Lerch und Domenika Tomasovic erhalten somit jeweils 25% der Stimmanteile. Sitz der Gesellschaft wird die Wissenschaftsstadt Darmstadt sein, da die Stadt einen gewissen Bekanntheitsgrad hat und es in der näheren Umgebung Museen gibt, die sich für die erste Phase von You eignen würden.
Wichtig ist auch, dass bei einer gUG im Falle einer Auflösung ein Verein oder ein gemeinnütziges Unternehmen bestimmt werden muss. Dieses wird demnach mit dem überschüssigen Geld gefördert. Das gesamte Team ist sich einig, dass die DKMS dieses Unternehmen ist. Es trägt sich selbst und kann so unabhängig von staatlichen Geldern arbeiten. Um wachsen zu können und Menschen zu helfen, ist die DKMS jedoch trotz aller Erfolge auf finanzielle Unterstützung durch Geldspender angewiesen („Über die DKMS“, 2019). Da wir alle unendlich begeistert sind und helfen wollen Menschen zu helfen, soll bei einer Auflösung Gutes getan werden.

author: { dt }
}

SWOT: {

Strengths	Weaknesses
Ein interdisziplinäres Team sorgt für das nötige Know-how in allen Bereichen. Vier junge Designer/innen sind unvoreingenommen an das Problem herangegangen und haben es aus verschiedenen Blickwinkeln bearbeitet. Das schafft ein besonderes Alleinstellungsmerkmal. Außerdem ermöglicht die Fähigkeit schnell und eigenständig Neues zu lernen und einzusetzen eine kontinuierliche Optimierung von You. Das große Netzwerk des Teams im Technischen, Design und Management Bereich, hilft bei der ständigen Verbesserung von You.	Da es sich bei You nicht um ein Konsumgut bzw. Produkt handelt, ist es essentiell nicht an die falschen Geldgeber zu geraten. Das Projekt soll sich selbst finanzieren und dabei jedoch von niemandem abhängig sein. Es handelt sich bei You um den Umgang mit Nutzerdaten und damit steht das Team in der Verantwortung jeden, der mit dem Projekt in Verbindung steht, als vertrauenswürdig zu identifizieren. Das Team ist darauf angewiesen, dass es am Eingang der Ausstellungen die Daten der Besuchenden unbemerkt abfragen kann. Alle Annahmen auf die sich das Konzept stützt wurden zwar getestet, könnten sich aber im letztendlichen Umfeld immer noch als fehlerhaft erweisen. Gemeint sind hier zum Beispiel die Reaktionen der Besuchenden, aber auch die problemlose Funktionsweise. Um dieses Risiko ausschließen zu können gibt es die oben beschriebene Testing Phase.
Opportunities	**Threats**
Es werden kaum Museen, Messen oder Ausstellungen ausgeschlossen. Der Markt ist damit recht groß. You ist polarisierend und schockierend und hat somit die besten Voraussetzungen viele Menschen zum Nachdenken anzuregen und damit den Bekanntheitsgrad immer weiter zu vergrößern. You ist keine App, Webseite oder Produkt. You ist ungewöhnlich und somit ohne vergleichbare Konkurrenz.	Den Museen muss die Angst genommen werden, dass sie wegen den vielen Daten die erhoben werden in irgendeiner Art und Weise Probleme bekommen könnten. Falls Daten entwendet werden, muss die Haftung geklärt sein. Daher ist trotz allen Sicherheitsmechanismen eine Versicherung von Anfang an geplant. Die Technik ist anfällig für Schäden, da sie in manchen Hinsichten sehr fragil ist. Hier ist Vorsicht bei Auf und Abbau geboten. Bei Softwareupdates kann es passieren, dass Teile des System erneuert und auf den Stand von Best Practices angepasst werden müssen. Diese Probleme lassen sich durch ein abgeschlossenes System während den Ausstellungen verhindern. You ist zum Anfangszeitpunkt auf Libraries von Drittanbieter angewiesen und somit von deren Funktionsfähigkeit abhängig. Es könnte Besuchende geben, die sich persönlich so angegriffen fühlen, dass sie mit rechtlichen Konsequenzen drohen.

Abb.16: {SWOT-Analyse}

author: { dt }
}

Planung und zukünftige Schritte: {

Dem Team sind, wie im gesamten Management Teil bereits beschrieben, die Risiken und Schwächen des Konzepts bewusst. Trotzdem sind der Glaube und die Begeisterung für das Projekt groß. Mit dieser Begeisterung konnte auch ein Familienmitglied eines Teammitglieds angesteckt werden. Er ist bereit 35.000€ zu spenden und damit die Möglichkeit zu bieten das Projekt auszuarbeiten und auf den Markt zu bringen.

Da es bei You um ein polarisierendes und schockierendes Erlebnis geht, dass Besuchende der Ausstellungen durchleben dürfen, und das Team in der prototypischen Umsetzung nur erahnen und zum Teil testen kann, wie die Menschen darauf reagieren, kann es natürlich sein, dass das gesamte Konzept nicht angenommen wird und das Unternehmen aufgelöst werden muss.

Deshalb werden zunächst 10.000 Euro vom Spender angenommen und falls die ersten Versuche You auszustellen erfolgreich verlaufen, werden weitere 15.000 Euro dafür verwendet, einen Markt zu schaffen und zu besetzten, der Geld einbringt und dem Team somit erlaubt das Projekt groß werden zu lassen.

Um den worst case, das Scheitern des Konzepts genauer und klarer zu formulieren hat das Team Exitpoints festgelegt. In der Summe gibt es drei dieser Exitpoints an denen gemeinsam überlegt werden soll, ob sich das Projekt in die richtige Richtung entwickelt. Hierbei sollen drei Fragen beantwortet werden.
Werden die Passion und das Ziel noch verfolgt?
Werden die Menschen noch schockiert und mit der Message erreicht?
Wird eine der Grenzen, die für den Umgang mit den Nutzenden gesetzt wurden, überschritten ?

Kann das Team all diese Fragen mit Ja beantworten, geht es nach Plan weiter. Sollte das nicht möglich sein, muss abgewägt werden, ob das Projekt weitergeführt werden kann und was getan werden muss, damit es wieder in die richtige Richtung geht. Sollte es nicht möglich sein die Ansprüche zu erfüllen, wird das Unternehmen aufgelöst und das Geld an die DKMS ausgezahlt.

Schafft es das Konzept auf zwei Ausstellungen über zwei Jahre hinweg fehlerfrei zu laufen und die Value zu erfüllen, dann haben die gründenden Personen ihr

Ziel erreicht. Die Firma kann dann für weitere Projekte zur Verfügung stehen, falls bis dahin das Team neue Ideen für Projekte entwickelt hat. Alternativ ist es einfach nur ein Unternehmen auf Zeit, welches sein Ziel trotzdem erfüllt hätte.

author: { dt }
}

Ausblick: {

You soll als Installation und Bewusstseinsschaffer agieren und verstanden werden. Das Team hofft, dass keiner der Exitpoints nötig ist und mit wachsendem Wissen auch ein verbessertes Erlebnis geschaffen werden kann. Dies soll im besten Falle dazu führen, dass You zu einem Besuchermagneten wird und Leute sich auf die Suche nach der Installation in Museen machen.
Auf der technischen Seite soll sich das Tracking und *Stalking* der Besuchenden verbessern und durch Iterationen genauer werden. Dadurch könnte sich auch die Möglichkeit ergeben, You auf andere Orte auszuweiten, wie beispielsweise eine Fußgängerzone.
Um auch Personen die You-Erfahrung des Datensammelns zu ermöglichen, könnte You zukünftig zusätzlich auch als Station ausgestellt werden, in der Daten manuell eingegeben werden. Dies würde den gleichen Prozess starten, wie bei vermeintlich gestalkten Personen, nur ohne das Tracking und Versenden von Nachrichten. Für die Datenvisualisierung dieses Prozesses wäre es denkbar, anstelle des Profils eine persönliche Suchmaschine anzuzeigen. Dort kann dann nach den eigenen Daten unter Schlagwörtern wie „Urlaub“ gesucht werden.
Eine Ziel welches das Team gerne erreichen möchte, wäre, das Menschen allein durch die Gespräche und Diskussionen, die durch You ausgelöst werden, einen bewussteren Umgang mit Ihren Daten in die Welt tragen.

author: { sl }
}

Team_v2: {

Wie hat sich dein Social Media Verhalten durch das Projekt verändert?

Name: **„Domenika“,**
Alter: **über 18,**
Wohnort: **„Odenwald“,**
Geschlecht: **„-“,**
Suchmaschine: **„Google“,**
Soziale Netzwerke: **„Instagram“,**
Lieblingsapps: **[„Instagram“, „Spotify“, „WhatsApp“],**
Paranoia vor Datenmissbrauch: **70%,**

Domenika: {„Ich habe seit Beginn des Projekts drei Storys auf Instagram gepostet. Ohne die Einsichten, die ich durch das Konzept hatte, wären es sicher weiterhin mindestens fünf pro Woche gewesen.
Ich habe angefangen mir die Frage zu stellen, muss ich das jetzt wirklich posten. Hat es einen Mehrwert oder gebe ich nur meine Daten in unbestimmte Hände?”
}

Name: **„Elina F.“,**
Alter: **keine Angabe,**
Wohnort: **„keine Angabe“,**
Geschlecht: **„keine Angabe“,**
Suchmaschine: **„DuckDuckGo“,**
Soziale Netzwerke: **„Youtube“,**
Lieblingsapps: **[„Youtube“, „Todoist“, „Spotify“],**
Paranoia vor Datenmissbrauch: **95%,**

Elina F.: {„Die Recherche und die Gespräche über das Thema haben meine Denkensweise bezüglich meiner personenbezogenen Daten nachhaltig verändert.
Ich habe Twitter gelöscht, bin von Google auf DuckDuckGo umgestiegen und werden mich von Instagram nach Abschluss des Projektes trennen.
Meine Daten repräsentieren mich und ich möchte sie gerne, soweit es mir möglich ist, für mich behalten.“
}

Name: **„Peter Müller“,**
Alter: **65,**
Wohnort: **„Nimmerland“,**
Geschlecht: **„Sonstiges“,**
Suchmaschine: **„DuckDuckGo“,**
Soziale Netzwerke: **[„Freunde“, „Spotify“],**
Lieblingsapps: **„Neuland“,**
Paranoia vor Datenmissbrauch: **80%,**

Peter Müller: {„Ich hab schon eine grobe Ahnung gehabt, wie viele Daten über mich gesammelt wurden, aber die Recherche in dem Projekt hat mir gezeigt wie einfach es ist an viel Daten zu kommen, und wie vorsichtig man sein muss, welche Daten man von sich preisgibt. Ich werde definitiv viel mehr darauf achten, ob ich gewisse Daten von mir angeben muss oder nicht.“
}

Name: **„S Lrh“,**
Alter: **42,**
Wohnort: **„Einhornstätten“,**
Geschlecht: **„-“,**
Suchmaschine: **„DuckDuckGo“,**
Soziale Netzwerke: **„keine digitalen“,**
Lieblingsapps: **[„Threema“, „Spotify“],**
Paranoia vor Datenmissbrauch: **80%,**

S Lrh: {„Da ich mich bereits vor dem Projekt mit Teilen der Thematik auseinander gesetzt habe, war der Schock für mich nicht so tiefgreifend. Es hat mich allerdings dazu bewegt, den letzten Schritt bei beispielsweise der Löschung des Facebook-Accounts zu gehen, die ich vorher aus Bequemlichkeit hingenommen habe.“
}
}

Literaturverzeichnis: {

aahill. (o. J.). Standpunktanalyse unter Verwendung der Textanalyse von Azure Cognitive Services. Abgerufen 19. Mai 2019, von https://docs.microsoft.com/de-de/azure/cognitive-services/text-analytics/how-tos/text-analytics-how-to-sentiment-analysis

Alpaydin, E. (2009). Introduction to machine learning. MIT press.

AOK. (2016). Äquivalenzprinzip. Abgerufen 18. Mai 2019, von https://aok-bv.de/lexikon/a/index_00034.html

Banse, P. (2012). So wertvoll sind unsere Daten. Deutschlandfunk. Abgerufen von https://www.deutschlandfunk.de/so-wertvoll-sind-unsere-daten.697.de.html?dram:article_id=206148

Beebe, J. (2019, März 22). What you don't know about your health data will make you sick. Abgerufen 5. Mai 2019, von Fast Company website: https://www.fastcompany.com/90317471/what-you-dont-know-about-your-health-data-privacy-will-make-you-sick

Benrath, B., & Bartsch, B. (2018, November 30). Asien in Zahlen – Teil 2: Punktabzug für zu seltene Besuche bei den Eltern. Abgerufen von https://www.faz.net/aktuell/wirtschaft/infografik-chinas-sozialkredit-system-15913709.html

Burkhardt, W. (2013). Einer für alle, alle für einen – Das Solidarprinzip in der gesetzlichen Krankenversicherung. Abgerufen von http://www.bpb.de/politik/innenpolitik/gesundheitspolitik/72358/solidarprinzip?p=all

Chatfield, T. (2013). 50 Schlüsselideen Digitale Kultur. https://doi.org/10.1007/978-3-8274-3064-9

Dähne, M. (2018, Mai 23). Neue Studie: US-Datenschutz: Chaotisch und uneinheitlich. Abgerufen 5. Mai 2019, von https://www.zdf.de/uri/03a54086-97de-4873-98e2-d894d571cdba

Deutsches Museum München. (o. J.). Deutsches Museum: Wissenschaftsjahr 2019. Abgerufen 19. Mai 2019, von http://www.deutsches-museum.de/angebote/wissenschaftsjahr-2019/

Deutsches Museum Nürnberg. (o. J.). Deutsches Museum: Projekt. Abgerufen 19. Mai 2019, von http://www.deutsches-museum.de/nuernberg/projekt/

Deutsches Spionagemuseum Berlin. (o. J.). Deutsches Spionagemuseum Berlin - German Spy Museum Berlin. Abgerufen 19. Mai 2019, von Deutsches Spionagemuseum website: https://www.deutsches-spionagemuseum.de/

Digitalstadt Darmstadt. (o. J.). Darmstadt Konferenz. Abgerufen 19. Mai 2019, von Digitalstadt Darmstadt website: https://www.digitalstadt-darmstadt.de/darmstadt-konferenz/

Dmitry. (2019). NodeJS Instagram private API client. Written in TypeScript.: dilame/instagram-private-api [TypeScript]. Abgerufen von https://github.com/dilame/instagram-private-api (Original work published 2016)

Domo. (2018). Data Never Sleeps 6.0. Abgerufen 19. Mai 2019, von https://www.domo.com/news/press/domo-releases-sixth-annual-data-never-sleeps-infographic

Dr. Datenschutz. (2015, August 21). MAC-Adressen – Aufbau, Funktion und Gefahren im Netzwerk. Abgerufen 19. Mai 2019, von Datenschutzbeauftragter website: https://www.datenschutzbeauftragter-info.de/mac-adressen-aufbau-funktion-und-gefahren-im-netzwerk/

DSGVO als weltweiter „Datenschutz-Gold-Standard". (2018, August 31). Abgerufen 5. Mai 2019, von Datenschutzbeauftragter website: https://www.datenschutzbeauftragter-info.de/dsgvo-als-weltweiter-datenschutz-gold-standard/

Duden. (o. J.-a). Ausstellung. Abgerufen 19. Mai 2019, von https://www.duden.de/rechtschreibung/Ausstellung#Bedeutung-2

Duden. (o. J.-b). Sonderausstellung. Abgerufen 19. Mai 2019, von https://www.duden.de/rechtschreibung/Sonderausstellung

Europäischen Union. Datenschutzgrundverordnung. , (2018).

Frankfurt.de. (o. J.-a). Frankfurt am Main: Die Museen. Abgerufen 19. Mai 2019, von https://www.frankfurt.de/sixcms/detail.php?id=3796

Frankfurt.de. (o. J.-b). Frankfurt am Main: EXPERIMINTA – Science-Center FrankfurtRheinMain. Abgerufen 19. Mai 2019, von https://www.frankfurt.de/sixcms/detail.php?id=3796&_ffmpar%5B_id_inhalt%5D=8011889

Frankfurt.de. (o. J.-c). Frankfurt am Main: Museum für Kommunikation. Abgerufen 19. Mai 2019, von https://www.frankfurt.de/sixcms/detail.php?id=3796&_ffmpar%5B_id_inhalt%5D=102988

Frankfurt.de. (o. J.-d). Frankfurt am Main: Schirn Kunsthalle Frankfurt. Abgerufen 19. Mai 2019, von https://www.frankfurt.de/sixcms/detail.php?id=3796&_ffmpar%5B_id_inhalt%5D=102428

Gesichtserkennung: Testlauf am Südkreuz endet – neuer Versuch in Planung. (2018, Juli 14). Abgerufen 19. Mai 2019, von Berliner Zeitung website: https://www.berliner-zeitung.de/berlin/polizei/gesichtserkennung-test-

lauf-am-suedkreuz-endet---neuer-versuch-in-planung-30958522
Google. (o. J.). Google Vision API. Abgerufen 19. Mai 2019, von https://cloud.google.com/vision/?hl=de
Görmer, J. (2018). Anonymität im Darknet (Hochschule Anhalt). Abgerufen von https://www.opendata.uni-halle.de/bitstream/1981185920/12783/1/Bachelorarbeit%20Julia%20Görmer.pdf
Granville, K. (2018). Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens. New York Times. Abgerufen von https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html
Gummadi, R. (2018, Januar 30). Instagram Graph API Launches and Instagram API Platform Deprecation. Abgerufen 19. Mai 2019, von Facebook for Developers website: https://developers.facebook.com/blog/post/2018/01/30/instagram-graph-api-updates
Hootsuite. (2019). Digital 2019. Abgerufen von https://p.widencdn.net/kqy7ii/Digital2019-Report-en
Horn, D. (2018). Der Facebook-Skandal, aber sortiert. t3n. Abgerufen von https://t3n.de/news/facebook-skandal-sortiert-1012101/
Humans of New York. (2019). Humans of New York. Abgerufen von https://www.humansofnewyork.com
Hunt, T. (2019). have i been pwned. Abgerufen 5. Mai 2019, von https://haveibeenpwned.com/PwnedWebsites
Instagram Datenschutzrichtlinie. (o. J.). Abgerufen 19. Mai 2019, von https://help.instagram.com/519522125107875
Institut für Museumsforschung. (2017). Statistische Gesamterhebung an den Museen der Bundesrepublik Deutschland für das Jahr 2017. Abgerufen von https://www.smb.museum/fileadmin/website/Institute/Institut_fuer_Museumsforschung/Publikationen/Materialien/mat72.pdf
Jacob. (2019). A Social Media Enumeration & Correlation Tool by Jacob Wilkin(Greenwolf): Greenwolf/social_mapper [Python]. Abgerufen von https://github.com/Greenwolf/social_mapper (Original work published 2018)
Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2005). Social Phishing. Abgerufen von http://www.markus-jakobsson.com/papers/jakobsson-commacm07.pdf
Kaliya „Identity Woman“ Young. (2011). Personal Data Ecosystem - NSTIC Privacy Workshop. Technology. Abgerufen von https://www.slideshare.net/Kaliya/personal-data-ecosystem-nstic-privacy-workshop
Kant, K., Iyer, R., & Mohapatra, P. (2012). Architectural impact of secure socket layer on Internet servers. 2012 IEEE 30th International Conference on Computer Design (ICCD), 27–34. https://doi.org/10.1109/ICCD.2012.6378612
Kessler, G. M. (2008). Law and Law Enforcement Issues. Nova Publishers.
Krempl, S. (2018). Künstliche Intelligenz: Facebook sagt Nutzerverhalten voraus und verkauft damit Anzeigen. Heise. Abgerufen von https://www.heise.de/newsticker/meldung/Kuenstliche-Intelligenz-Facebook-sagt-Nutzerverhalten-voraus-und-verkauft-damit-Anzeigen-4024377.html
Kühl, E. (2018). Der Feind in meinem Turnschuh. Zeit. Abgerufen von https://www.zeit.de/digital/datenschutz/2018-01/fitnesstracker-strava-soldaten-verrat-geheimnisse-fitnessapp-datenschutz
Maus, T. (2008). Das Passwort ist tot — lang lebe das Passwort! https://doi.org/10.1007/s11623-008-0127-3
Miorandi, D. (2017, April 10). I lie, you lie, everybody lies: WiFi tracking in the era of MAC randomization. Abgerufen 19. Mai 2019, von Medium website: https://medium.com/@DanieleMiorandi/i-lie-you-lie-everybody-lies-wifi-tracking-in-the-era-of-mac-randomization-2ab147857b24
ml5js. (o. J.). ml5js imageClassifier(). Abgerufen 19. Mai 2019, von https://ml5js.org/docs/Image-Classifier
MongoDB. (2019). MongoDB. Abgerufen 20. Mai 2019, von https://www.mongodb.com
Mühler, V. (2019). JavaScript API for face detection and face recognition in the browser and nodejs with tensorflow.js. Abgerufen von https://github.com/justadudewhohacks/face-api.js (Original work published 2018)
Mühler, V. (o. J.). face-api.js. Abgerufen 19. Mai 2019, von face-api.js playground website: https://justadudewhohacks.github.io/face-api.js/webcam_face_expression_recognition
Museum für Kommunikation Berlin. (2014, Februar 8). Außer Kontrolle? Leben in einer überwachten Welt. Abgerufen 19. Mai 2019, von Museum für Kommunikation Berlin website: https://www.mfk-berlin.de/ausser-kontrolle/
Museum für Kommunikation Berlin. (o. J.). Museum für Kommunikation Berlin. Abgerufen 19. Mai 2019, von Museum für Kommunikation Berlin website: https://www.mfk-berlin.de/

Polizei Bayern. (o. J.). Was ist Stalking? Abgerufen von https://www.polizei.bayern.de/content/4/9/2/0/9/2_stalking.pdf

Reinsel, D., Gantz, J., & Rydning, J. (2018). The Digitization of the World. Abgerufen von https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

Rouse, M. (o. J.). What is facial recognition? Abgerufen 19. Mai 2019, von SearchEnterpriseAI website: https://searchenterpriseai.techtarget.com/definition/facial-recognition

Ryssel, J. M. (2019, März 5). Sozialpunktesystem in China: Eine Welt ohne Datenschutz? Abgerufen 5. Mai 2019, von Datenschutzbeauftragter website: https://www.datenschutzbeauftragter-info.de/sozialpunktesystem-in-china-eine-welt-ohne-datenschutz/

Schilling, M. (2018). Verfahren zum Testen der IT-Sicherheit an Unternehmen. Merseburg.

Schmidt, J.-H. (2018). Social Media (2., aktualisierte und erweiterte Auflage). Wiesbaden: Springer VS.

Schumacher, S. (2014). Die psychologischen Grundlagen des Social-Engineerings. Information - Wissenschaft & Praxis, 65(4–5), 215–230. https://doi.org/10.1515/iwp-2014-0039

Sears, G. (2018, August 3). GDPR Data Exports Reveal Spotify Tracks Absolutely Everything About You. Abgerufen 19. Mai 2019, von Dance Music NW website: http://dancemusicnw.com/spotify-gdpr-data-exports-user-tracking/

Six contemporary artists making a statement about social media. (2017, Juni 9). Abgerufen 19. Mai 2019, von Acclaim Magazine website: https://acclaimmag.com/art/six-contemporary-artists-making-a-statement-about-social-media/

Srinivasan, K., & Levis, P. (o. J.). RSSI is Under Appreciated. 5.

Statistische Ämter des Bundes und der Länder. (2018). Kulturindikatoren auf einen Blick - Ein Ländervergleich. 32.

Statistisches Bundesamt. (o. J.). Museen, Ausstellungen und Besuche nach Museumsarten und Trägerschaft. Abgerufen 19. Mai 2019, von Statistisches Bundesamt website: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Bildung-Forschung-Kultur/Kultur/Tabellen/museen-besuche-traegerschaft.html

Tang, K., Wang, Y., Liu, H., Sheng, Y., Wang, X., & Wei, Z. (2013, Oktober). Design and Implementation of Push Notification System Based on the MQTT Protocol. Gehalten auf der 2013 International Conference on Information Science and Computer Applications (ISCA 2013). https://doi.org/10.2991/isca-13.2013.20

Technoseum. (o. J.). TECHNOSEUM – Landesmuseum für Technik und Arbeit in Mannheim. Abgerufen 19. Mai 2019, von https://www.technoseum.de/

Teirstein, Z. (2016, Dezember 2). The Glass Room turns internet surveillance into art. Abgerufen 19. Mai 2019, von The Verge website: https://www.theverge.com/2016/12/2/13810900/the-glass-room-tactical-technology-collective-nolita-new-york-city

Things, D. and. (2018, Mai 2). The secrets hidden in your Venmo and Instagram data. Abgerufen 19. Mai 2019, von Medium website: https://medium.com/@dataandthings/the-secrets-hidden-in-your-venmo-and-instagram-data-7f9a06ea71e1

Thompson art center. (o. J.). Hansel & Gretel : Program & Events. Abgerufen 19. Mai 2019, von Park Avenue Armory website: http://www.armoryonpark.org/index.php/programs_events/detail/hansel_gretel

Unesco. (2016, Januar 5). Museums. Abgerufen 19. Mai 2019, von https://en.unesco.org/themes/museums

van der Aalst, W. (2016). Data Science in Action. In W. van der Aalst (Hrsg.), Process Mining: Data Science in Action (S. S. 4). https://doi.org/10.1007/978-3-662-49851-4_1

Völker, J. (2014). Passwörter sicher verwalten. https://doi.org/10.1007/s11623-014-0117-6

Wilkin, J. (2019). A Social Media Enumeration & Correlation Tool [Python]. Abgerufen von https://github.com/Greenwolf/social_mapper (Original work published 2018)

Wittpahl, V. (2017). Digitalisierung. Springer Vieweg, (1), 5. https://doi.org/DOI 10.1007/978-3-662-52854-9

Woolley, S. C. (2016). Automating power: Social bot interference in global politics. First Monday, 21(4). https://doi.org/10.5210/fm.v21i4.6161

Wurzel, S. (2019, März 3). Chinas Sozialkredit-Ranking: Reiseverbot für Millionen Menschen. Abgerufen 19. Mai 2019, von tagesschau.de website: https://www.tagesschau.de/ausland/sozialkredit-ranking-china-101.html

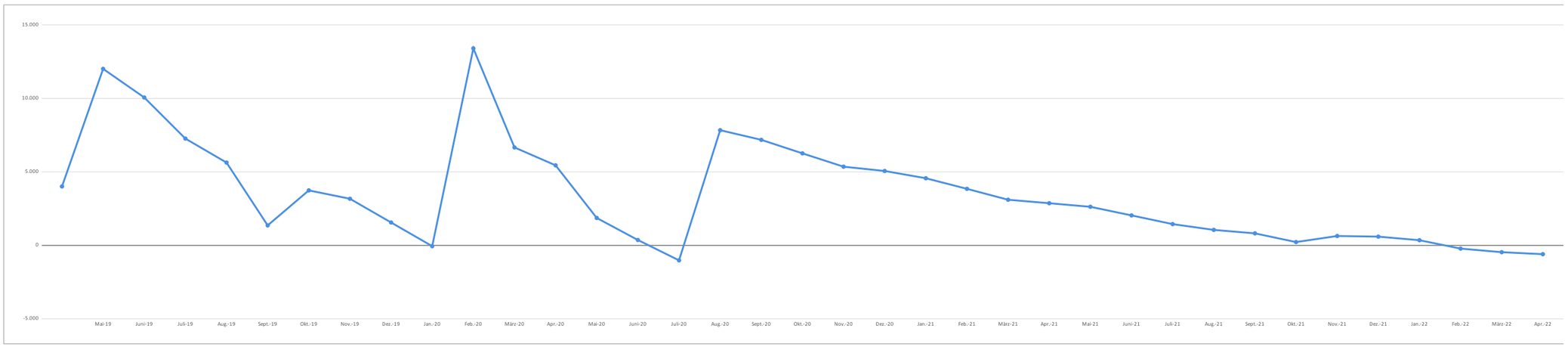
ZKM. (o. J.). Mission Statement | ZKM. Abgerufen 19. Mai 2019, von https://zkm.de/de/ueber-das-zkm/entstehung-philosophie/mission-statement

}

Anhang

102 Finanzplan
104 Quizlösungen
105 DOR

Stunden/Tag	4	Mai-19	Juni-19	Juli-19	Aug.-19	Sept.-19	Okt.-19	Nov.-19	Dez.-19	Jan.-20	Feb.-20	März-20	Apr.-20	Mai-20	Juni-20	Juli-20	Aug.-20	Sept.-20	Okt.-20	Nov.-20	Dez.-20	Jan.-21	Feb.-21	März-21	Apr.-21	Mai-21	Juni-21	Juli-21	Aug.-21	Sept.-21	Okt.-21	Nov.-21	Dez.-21	Jan.-22	Feb.-22	März-22	Apr.-22
Tage		31	30	31	31	30	31	30	31	31	29	31	30	31	30	31	31	30	31	30	31	31	28	31	30	31	30	31	31	30	31	30	31	31	28	31	30
							1 Museum						open testing			Bürobezug	going wide																				
Das Team	Stundensatz	Mai-19	Juni-19	Juli-19	Aug.-19	Sept.-19	Okt.-19	Nov.-19	Dez.-19	Jan.-20	Feb.-20	März-20	Apr.-20	Mai-20	Juni-20	Juli-20	Aug.-20	Sept.-20	Okt.-20	Nov.-20	Dez.-20	Jan.-21	Feb.-21	März-21	Apr.-21	Mai-21	Juni-21	Juli-21	Aug.-21	Sept.-21	Okt.-21	Nov.-21	Dez.-21	Jan.-22	Feb.-22	März-22	Apr.-22
Konzept	10	160	160	160	160	160	160	160	160	160	160	160	160	160	160	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Entwicklung Technisch / Backend	10	886	857	886	886	857	886	857	886	886	829	886	857	886	857	886	886	171	177	171	89	89	80	89	86	89	86	89	89	86	89	86	89	89	80	89	86
Projektleitung / Vertrieb/Marketing	10	443	429	443	443	429	443	429	443	443	414	443	429	443	429	443	443	171	177	171	89	89	80	89	86	89	86	89	89	86	89	86	89	89	80	89	86
Social Media	10	44	43	44	44	43	44	43	44	44	41	44	43	44	43	44	44	43	44	43	44	44	40	44	43	44	43	44	44	43	44	43	44	44	40	44	43
Summe Personal		**1.533**	**1.489**	**1.533**	**1.533**	**1.489**	**1.533**	**1.489**	**1.533**	**1.533**	**1.444**	**1.533**	**1.489**	**1.533**	**1.489**	**1.373**	**1.373**	**386**	**399**	**386**	**221**	**221**	**200**	**221**	**214**	**221**	**214**	**221**	**221**	**214**	**221**	**214**	**221**	**221**	**200**	**221**	**214**
Infrastruktur	p.P. monatlich	Mai-19	Juni-19	Juli-19	Aug.-19	Sept.-19	Okt.-19	Nov.-19	Dez.-19	Jan.-20	Feb.-20	März-20	Apr.-20	Mai-20	Juni-20	Juli-20	Aug.-20	Sept.-20	Okt.-20	Nov.-20	Dez.-20	Jan.-21	Feb.-21	März-21	Apr.-21	Mai-21	Juni-21	Juli-21	Aug.-21	Sept.-21	Okt.-21	Nov.-21	Dez.-21	Jan.-22	Feb.-22	März-22	Apr.-22
Bürofläche	510	0	0	0	0	0	0	0	0	0	0	0	0	510	0	0	0	510	510	510	510	510	510	510	360	360	360	360	360	360	360	360	360	360	360	360	360
einmalige Kaution für Bürofläche	1530	0	0	0	0	0	0	0	0	0	0	0	0	1.530	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Internet	30	0	0	0	0	0	0	0	0	0	0	0	0	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
Summe Infrastruktur		**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2.070**	**30**	**30**	**30**	**540**	**540**	**540**	**540**	**540**	**540**	**540**	**390**	**390**	**390**	**390**	**390**	**390**	**390**	**390**	**390**	**390**	**390**	**390**
				Gründung gUG																																	
Betriebswirtschaftliches	pro Stunde	Mai-19	Juni-19	Juli-19	Aug.-19	Sept.-19	Okt.-19	Nov.-19	Dez.-19	Jan.-20	Feb.-20	März-20	Apr.-20	Mai-20	Juni-20	Juli-20	Aug.-20	Sept.-20	Okt.-20	Nov.-20	Dez.-20	Jan.-21	Feb.-21	März-21	Apr.-21	Mai-21	Juni-21	Juli-21	Aug.-21	Sept.-21	Okt.-21	Nov.-21	Dez.-21	Jan.-22	Feb.-22	März-22	Apr.-22
Gründung gUG				808	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rechtsberatung	180	360	360	360	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Steuerberater pro monat	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
Versicherung	32 pro Monat						32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32	32
Summe Sonstige Kosten		**460**	**460**	**1.268**	**100**	**100**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**	**132**
Gesamtkosten einer Ausstellung		Mai-19	Juni-19	Juli-19	Aug.-19	Sept.-19	Okt.-19	Nov.-19	Dez.-19	Jan.-20	Feb.-20	März-20	Apr.-20	Mai-20	Juni-20	Juli-20	Aug.-20	Sept.-20	Okt.-20	Nov.-20	Dez.-20	Jan.-21	Feb.-21	März-21	Apr.-21	Mai-21	Juni-21	Juli-21	Aug.-21	Sept.-21	Okt.-21	Nov.-21	Dez.-21	Jan.-22	Feb.-22	März-22	Apr.-22
Materialkosten		0	0	0	0	2.691	0	0	0	0	0	**5.382**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Mitarbeiterkosten	2250					2250	2250	2250	0	0	0	**6750**	**6750**	0	0	0	**2250**	**2250**			**2250**	**2250**	0	0	**2250**	**2250**	0	0	**2250**	**2250**	0	0	**2250**	**2250**	0	**2250**	**2250**
Summe einer Ausstellung		0	0	0	0	4.941	2.250	2.250	0	0	0	**12.132**	**6.750**	0	0	0	**2.250**	**2.250**	0	0	**2.250**	**2.250**	0	0	**2.250**	**2.250**	0	0	**2.250**	**2.250**	0	0	**2.250**	**2.250**	0	**2.250**	**2.250**
Einnahmen		Mai-19	Juni-19	Juli-19	Aug.-19	Sept.-19	Okt.-19	Nov.-19	Dez.-19	Jan.-20	Feb.-20	März-20	Apr.-20	Mai-20	Juni-20	Juli-20	Aug.-20	Sept.-20	Okt.-20	Nov.-20	Dez.-20	Jan.-21	Feb.-21	März-21	Apr.-21	Mai-21	Juni-21	Juli-21	Aug.-21	Sept.-21	Okt.-21	Nov.-21	Dez.-21	Jan.-22	Feb.-22	März-22	Apr.-22
Museen tragen Mitarbeiterkosten		0	0	0	0	2.250	2.250	2.250	0	0	0	6.750	6.750	0	0	0	2.250	2.250	0	0	2.250	2.250	0	0	2.250	2.250	0	0	2.250	2.250	0	0	2.250	2.250	0	2.250	2.250
Spenden von Nutzenden		0	0	0	0	0	50	50	50	50	50	300	400	150	150	150	400	400	150	150	600	400	150	150	500	500	150	150	350	500	150	150	700	500	150	500	600
Wettbewerbsgewinne		0	0	0	0	0	0	1.000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1.000	0	0	0	0	0
Philantropengeld		10.000	0	0	0	0	0	0	0	0	15.000	0	0	0	0	0	10.000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Datev Stiftung		0	0	0	0	0	4.000	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Summe Einnahmen		10.000	0	0	0	2.250	6.300	3.300	50	50	15.050	7.050	7.150	150	150	150	12.650	2.650	150	150	2.850	2.650	150	150	2.750	2.750	150	150	2.600	2.750	150	1.150	2.950	2.750	150	2.750	2.850
Ausstellungsmaterialkosten	pro Stück																																				
PC	529,80	4	2.119																																		
Webcam	21,99	3	66																																		
Monitor	89,99	4	360																																		
HDMI Kabel	0,70	4	3																																		
5m Verlängerungskabel	7,99	6	48																																		
Router	64,00	1	64																																		
Tastatur	4,90	4	20																																		
Maus	2,90	4	12																																		
Summe Ausstellung	722,27		**2.691**																																		
GuV		Mai-19	Juni-19	Juli-19	Aug.-19	Sept.-19	Okt.-19	Nov.-19	Dez.-19	Jan.-20	Feb.-20	März-20	Apr.-20	Mai-20	Juni-20	Juli-20	Aug.-20	Sept.-20	Okt.-20	Nov.-20	Dez.-20	Jan.-21	Feb.-21	März-21	Apr.-21	Mai-21	Juni-21	Juli-21	Aug.-21	Sept.-21	Okt.-21	Nov.-21	Dez.-21	Jan.-22	Feb.-22	März-22	Apr.-22
Einnahmen		10.000	0	0	0	2.250	6.300	3.300	50	50	15.050	7.050	7.150	150	150	150	12.650	2.650	150	150	2.850	2.650	150	150	2.750	2.750	150	150	2.600	2.750	150	1.150	2.950	2.750	150	2.750	2.850
Gesamtkosten einer Ausstellung		0	0	0	0	-4.941	-2.250	-2.250	0	0	0	-12.132	-6.750	0	0	0	-2.250	-2.250	0	0	-2.250	-2.250	0	0	-2.250	-2.250	0	0	-2.250	-2.250	0	0	-2.250	-2.250	0	-2.250	-2.250
Nettoerlös		**10.000**	**0**	**0**	**0**	**-2.691**	**4.050**	**1.050**	**50**	**50**	**15.050**	**-5.082**	**400**	**150**	**150**	**150**	**10.400**	**400**	**150**	**150**	**600**	**400**	**150**	**150**	**500**	**500**	**150**	**150**	**350**	**500**	**150**	**1.150**	**700**	**500**	**150**	**500**	**600**
Das Team		-1.533	-1.489	-1.533	-1.533	-1.489	-1.533	-1.489	-1.533	-1.533	-1.444	-1.533	-1.489	-1.533	-1.489	-1.373	-1.373	-386	-399	-386	-221	-221	-200	-221	-214	-221	-214	-221	-221	-214	-221	-214	-221	-221	-200	-221	-214
Infrastruktur		0	0	0	0	0	0	0	0	0	0	0	0	-2.070	-30	-30	-30	-540	-540	-540	-540	-540	-540	-540	-390	-390	-390	-390	-390	-390	-390	-390	-390	-390	-390	-390	-390
Betriebswirtschaftliches		-460	-460	-1.268	-100	-100	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132	-132
Betriebsergebnis		**8.007**	**-1.949**	**-2.801**	**-1.633**	**-4.280**	**2.385**	**-571**	**-1.615**	**-1.615**	**13.474**	**-6.747**	**-1.221**	**-3.585**	**-1.501**	**-1.385**	**8.865**	**-658**	**-921**	**-908**	**-293**	**-493**	**-722**	**-743**	**-236**	**-243**	**-586**	**-593**	**-393**	**-236**	**-593**	**414**	**-43**	**-243**	**-572**	**-243**	**-136**
Bilanz	Start	Mai-19	Juni-19	Juli-19	Aug.-19	Sept.-19	Okt.-19	Nov.-19	Dez.-19	Jan.-20	Feb.-20	März-20	Apr.-20	Mai-20	Juni-20	Juli-20	Aug.-20	Sept.-20	Okt.-20	Nov.-20	Dez.-20	Jan.-21	Feb.-21	März-21	Apr.-21	Mai-21	Juni-21	Juli-21	Aug.-21	Sept.-21	Okt.-21	Nov.-21	Dez.-21	Jan.-22	Feb.-22	März-22	Apr.-22
Betriebsergebnis	0	8.007	-1.949	-2.801	-1.633	-4.280	2.385	-571	-1.615	-1.615	13.474	-6.747	-1.221	-3.585	-1.501	-1.385	8.865	-658	-921	-908	-293	-493	-722	-743	-236	-243	-586	-593	-393	-236	-593	414	-43	-243	-572	-243	-136
Eigenkapital	**4.000**	**12.007**	**10.059**	**7.258**	**5.625**	**1.345**	**3.730**	**3.160**	**1.545**	**-70**	**13.404**	**6.657**	**5.436**	**1.851**	**351**	**-1.034**	**7.831**	**7.173**	**6.253**	**5.345**	**5.052**	**4.558**	**3.836**	**3.093**	**2.857**	**2.613**	**2.027**	**1.433**	**1.040**	**804**	**210**	**624**	**581**	**337**	**-235**	**-478**	**-615**



Quizlösungen: {

#01 = true (Spyrou,2019)
#02 = false
#03 = true (Radford,2019)
#04 = false
#05 = false
}

Delegation of Rights and Non Violation Statement

You is a project, developed in the framework of the study course Interactive Media Design of Hochschule Darmstadt - Faculty of Media, during the Summer Term 18/19.
It is a groupwork of: Elina Faber, Sarah Lerch, Jan Meininghaus and Domenika Tomasovic. It was mentored by: Prof. Claudius Coenen, Christoph Diederichs, Prof. Andrea Krajewski, Prof. Garrit Schaap, Andreas Schindler.

Herewith delegate the non exclusive and timewise non restricted rights to publish and present the results of the project **You** to the Professors of Hochschule Darmstadt and to the coaches directly connected to the academic supervision of this project, named above. In the same time the student project team declares that with the project no intellectual properties rights of third parties have been harmed.

Dieburg, 21.05.2019