PayPal unter dem Mikroskop - Daten und Fakten

PayPals Geschäftsmodell

Im Jahr 2021 wurden 19,3 Milliarden Zahlungstransaktionen über PayPal abgewickelt, die sich auf 1,25 Billionen Dollar belaufen. Die Beziehungen in diesem Zahlungsnetzwerk sind starke Prädiktoren für Verhaltensweisen und verlässliche Risikoindikatoren die Betrug aufdecken können. Bei Online-Käufen steht jedoch ein viel umfangreicherer Datensatz zur Verfügung, einschließlich eines detaillierten Rechnungsbelegs oder Informationen über den Käufer. Es kostet viel Geld, die scheinbar unzusammenhängenden Daten von 426 Millionen PayPal-Nutzern zu sammeln und zu speichern. Das bedeutet, dass sie in irgendeiner Weise verwendet werden müssen, die PayPal einen Gewinn bringt.

Mindestdatenanforderungen für die Zahlungsabwicklung:

- Auftragssumme
- der empfangende Händler
- eine authentifizierte Zahlung

Bedenken hinsichtlich des Datenschutzes hängen auch mit dem Verbraucherverhalten zusammen. Zahlungsanbieter können in großem Umfang Kaufdaten sammeln und miteinander verknüpfen, um ein Verhaltensprofil des Verbrauchers zu erstellen. Auf diese Weise kann PayPal umfassende Konsumprofile über verschiedene Webseiten hinweg erstellen.

PayPal wendet mehrere kommerzielle Strategien an, um Privatkund*innen anzusprechen. Ihre Werbung versucht, interne Bedürfnisse wie Vereinfachung, Schnelligkeit, Vielfalt und Sicherheit durch schnelle Kaufabwicklung, umfassenden Käuferschutz, Ratenzahlungsoptionen usw. zu erfüllen.

Beispiel Werbeslogan:
„Willste? Kriegst. Das ist der PayPal Unterschied.“

PayPal hat eine **Programmierschnittstelle (Application Programming Interface; API)** für Händler*innen mit einer grundlegenden Kreditkartenzahlungsfunktion eingeführt. Dadurch kann jedes kleine Unternehmen sein Geschäft mit nahezu keiner Investition starten und Zahlungen über das Internet via PayPal annehmen.
APIs werden zunehmend in alltäglichen Dingen verwendet, wenn wir Apps auf unseren Smartphones nutzen, doch führt die Auslagerung der Datenspeicherung an einen Cloud-Betreiber zu Datenschutzproblemen. Je mehr APIs verwendet werden, desto anfälliger wird unsere Privatsphäre, wenn eine Cloud angegriffen wird. Die Anwerbung kleinerer Marketing- und Zahlungsdienste/-anbieter öffnet PayPal das Tor zum Erwerb viel umfangreicherer Datensätze und einer wesentlich umfassenderen Einschätzung der Profile ihrer Nutzer*innen.

Die **PayPal-Nutzungsvereinbarung** ist ein Dokument, das weitaus mehr Wörter enthält als die anderer Unternehmen und daher mehr Zeit zum Lesen benötigt. Experten behaupteten, PayPal verstoße gegen den Grundsatz der Transparenz und Nutzer*innen würden benachteiligt. Eine wissenschaftliche Textanalyse ergab, dass die Allgemeinen Geschäftsbedingungen (AGB) von PayPal formal unverständlich sind und der Aufwand, den die Nutzer betreiben müssen, unzumutbar ist.
Mit neueren Versionen hat PayPal seine AGB zwar verkürzt, aber im Vergleich zu anderen Unternehmen sind sie immer noch das längste Dokument. Außerdem sind die Sätze in den AGBs und Datenschutzerklärungen oft passiv und kompliziert formuliert.

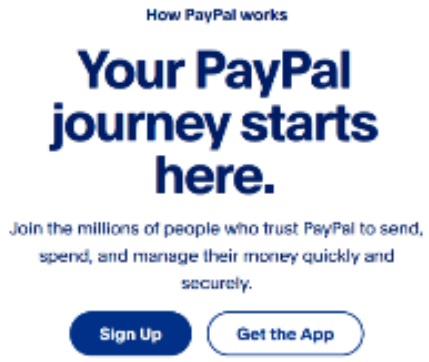
- Wörter und Ausdrücke wie **"möglicherweise"** und **"unter anderem"** machen diese Dokumente vage und schwierig zu verstehen.
- Durchschnittliche Nutzer*innen werden nicht **fast 1,5 Stunden** damit verbringen, ein Dokument zu lesen, auf das man keinen Einfluss hat und das man nicht ablehnen kann, da man die Möglichkeit behalten will den Dienst zu nutzen.

Anbieter von Online-Diensten versuchen, Nutzer dazu zu verleiten, freiwillig Zugang zu ihren persönlichen Daten zu gewähren, indem sie kognitive Neigungen ausnutzen durch **„nudging“** und sogenannte **„dark patterns“** einbauen. Beispiele dafür sind Benutzeranmeldungen auf Startseiten, die eine offensichtliche Anmeldung mit persönlichen Konten wie Facebook, Google und eine weniger helle Schaltfläche "Erstellen Sie ein eigenes Konto" sowie eine versteckte Schaltfläche "Überspringen" (oft in der oberen rechten Ecke) zeigen. Die Absicht scheint zu sein, auf Freundeslisten, Fotos und Likes zuzugreifen und somit Informationen zu erhalten, die für den Dienst im Grunde nicht notwendig sind, indem absichtlich schlechtes Design, User-Experience-Tricks und Erkenntnisse aus der Human-Computer-Interaction-Forschung genutzt werden.

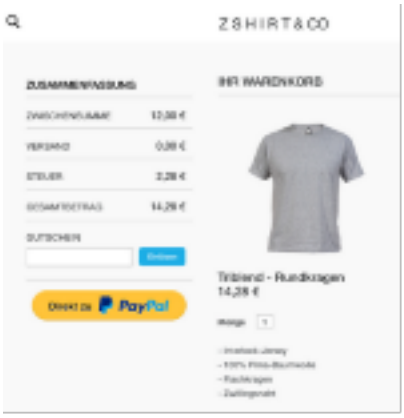
“Dark patterns” werden durch ihre Häufigkeit des Auftretens wirksam, die sich aus den psychologischen Untersuchungen zu diesen Strategien ableiten lässt. Ihr Fokus scheint auf der kognitiven Informationsverarbeitung und der psychologischen Konstitution zu liegen. Das grundsätzliche Bedürfnis, dazuzugehören, beeinflusst die Wirksamkeit dunkler Muster in hohem Maße. Dadurch wird die Bereitschaft zur Angabe persönlicher Daten stark erhöht.

Nudging-Strategien nutzen kognitive Abkürzungen, die bei der (irrationalen) Entscheidungsfindung beobachtet werden, um irrationales Verhalten erklärbarer und sogar vorhersehbarer zu machen. *Social Framing* hat sich als besonders wirksamer sozialer Verhaltensstimulus erwiesen. Da es beschreibende soziale Normen als präskriptive Regeln verwendet, kann es wirksam eingesetzt werden und wird bereits von Instanzen wie Regierungen, Arbeitgebern und Unternehmen übernommen. Außerdem werden je nach Sprache/Land unterschiedliche Muster verwendet.

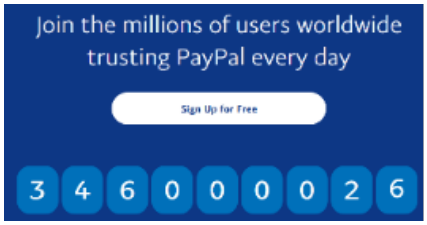
Beispiele:
"7 Personen schauen sich das gerade an!", "Dieses Angebot läuft in 15 Minuten ab!".
Diese Beispiele bringen die Nutzer dazu, mit einer Art Dringlichkeit zu handeln, indem sie ein abstraktes Prinzip in einen konkreten Anstoß verwandeln.



Ein *dark pattern* mit verschiedenen Schaltflächenfarben, um den Benutzer dazu zu bringen, sich bei PayPal anzumelden.



Express-Checkout-Schaltfläche in leuchtenden, auffälligen Farben. Sie impliziert "PayPal-Sicherheit" und erhöht damit das Vertrauen in die Shops.



PayPal spricht das grundlegende Bedürfnis der Nutzer nach Zugehörigkeit an. Der Zähler zählt nicht die tatsächliche Anzahl der Nutzer. Er beginnt bei 346.000.000 Nutzern, wenn man die Website öffnet.

PayPal stellt auch ausführliche Informationen zur Verfügung, in denen sie Unternehmen dabei helfen, die PayPal-Vorteile zu nutzen, indem sie den Kunden mitteilen, dass PayPal für sie zur Verfügung steht. In dem Leitfaden wird ausführlich erklärt, wie die Schaltfläche für die Express-Kaufabwicklung genau platziert werden muss, um die Aufmerksamkeit der Nutzer zu erregen und sie zum Kauf von Artikeln in ihrem Geschäft zu bewegen.
Ziel ist es, "digitalen und physischen Handel zu verschmelzen, um nahtlose Kundenerlebnisse zu schaffen".

Big Data, Privatsphäre und PayPal

Die Summe der persönlichen Daten einer Person bilden eine **digitale Identität** die als Ware oder Kapital gehandelt werden kann. Später kann diese als Grundlage für Modelle zur Vorhersagung von Verhalten verwendet werden. Dies führt zu einer "Datendiktatur", in der man nicht mehr auf der Grundlage unserer Handlungen beurteilt werden, sondern auf der Grundlage dessen, was unsere Daten über wahrscheinliche Handlungen schließen lassen. Da unsere digitale Identität Ausdruck der eigenen Identität ist, müssen diese Daten geschützt werden.

Nutzer*innen stimmen in den Allgemeinen Geschäftsbedingungen zu, dass PayPal unter anderem die folgenden Daten für Werbung und Marketing, Analysen, Personalisierung des Produkts, App-Funktionen und zur Verbesserung der Nutzererfahrung sammeln darf:

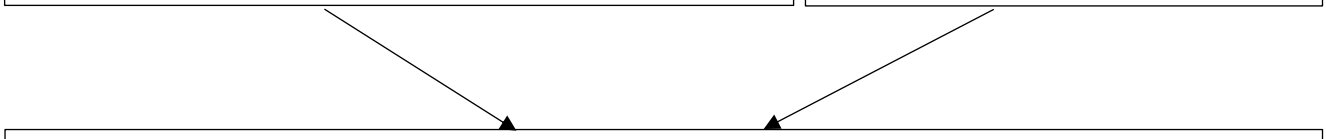
- Einkaufsverlauf, Kontaktdaten, Browserverlauf, Informationen zu Finanzen, Lokalisierung

Dies steht im Widerspruch zur Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU), die besagt, dass der Grundsatz der "**Datenminimierung**" anzuwenden ist. Dies bedeutet, dass so wenig Informationen wie möglich für einen bestimmten Zweck gesammelt werden sollen. Das Problem ist, dass das EU-Recht nicht definiert, was "angemessene, erhebliche und notwendige" Daten sind. Daher kann PayPal beliebige Daten sammeln, wenn sie dies mit ihren Geschäftsinteressen rechtfertigen können, die für Nutzer*innen nicht offensichtlich sind.

Warum ist das ein Problem?
Je mehr Daten gesammelt werden, desto größer ist der Erfolg von künstlicher Intelligenz (KI) und Algorithmen für maschinelles Lernen (ML) in diesen Daten verborgene Muster finden, um unser Verhalten vorherzusagen.

Proxy Diskriminierung
Um eine Vorhersage über ein Mitglied einer geschützten Klasse (z. B. Menschen unterschiedlicher Herkunft) zu treffen, kann eine nicht geschützte Variable, die in hohem Maße mit der geschützten Klasse korreliert, ein so genannter Proxy, für eine solche Vorhersage verwendet werden. Wenn Algorithmen auf großen Datensätzen trainiert werden, um Vorhersagen zu treffen, stützen sie sich auf Proxys, um präzise Vorhersage zu treffen. Dies führt zur Verwendung von Gruppenmerkmalen, was wiederum zu Stereotypisierung und Diskriminierung führt, da Personen gleich behandelt werden wie andere Personen, die sich in der Vergangenheit ähnlich verhalten haben.

Prädiktive Analytik
Auf Grundlage großer Datenmengen von vielen verschiedenen Personen werden Verhaltensmuster und Interessen von Personen vorhergesagt, die sich entschieden haben, ihre Daten nicht zu teilen. Dadurch wird ein sensibler privater Bereich von Personen verletzt, die entschieden haben, wenig private Informationen teilen.



Beispiel: Kreditwürdigkeitsprüfung
KI wird eingesetzt, um Datenpunkte über eine Person in eine Kreditbewertung umzuwandeln, wobei Proxy Diskriminierung und prädiktive Analytik eine Rolle spielen. Dies kann zu ungerechten und diskriminierenden Entscheidungen führen, da Personen eine schlechtere Kreditwürdigkeit erhalten können, nur weil sie sich ähnlich verhalten, wie eine andere Person, die tatsächlich nicht vertrauenswürdig ist. Dadurch werden die Spirale aus Diskriminierung, ungleichen Chancen und die Kluft zwischen Arm und Reich verschärft. Außerdem ist die Art und Weise, wie ein Algorithmus eine Vorhersage ableitet, für Menschen nicht nachvollziehbar, so dass es unmöglich ist zu erklären, warum eine Person eine bestimmte Kreditwürdigkeitsstufe erhalten hat.