

PayPal Unter dem Mikroskop

Recherche Dossier

Hintergrundinformationen und zusätzliche Ressourcen

September 2022

Carmen Amme
Alicjia Suchonska
Regilla Bastian
Anneke Bührma

Inhaltsverzeichnis

1	<i>PayPal: Geschäftsmodell</i>	3
1.1	PayPals Kerngeschäftsmodell	3
1.1.1	PayPal und Honey	4
1.2	PayPals Werbestrategien	4
1.3	PayPal und Schnittstellen zur Anwendungsprogrammierung	5
2	<i>PayPal: Benutzeroberfläche</i>	7
2.1	Allgemeine Geschäftsbedingungen	7
2.2	Wirkung nach Außen	7
2.2.1	Hintergrundinformationen zu täuschendem Design - Dark Patterns	7
2.2.2	Nudging	9
2.2.3	Dark Patterns und Nudging: PayPal	9
3	<i>Big Data und Datenschutz</i>	12
3.1	Hintergrund	12
3.2	PayPals Datenschutzerklärung (6. Mai 2022)	13
3.3	Sammeln und Teilen von persönlichen Informationen	14
3.4	PayPal und die Datenschutz-Grundverordnung (DSGVO)	15
3.5	Datenschutz und Kommunikation	16
3.6	Verbindung zu theoretischen Konzepten	17
3.6.1	Prädiktive Analytik	17
3.6.2	Proxy Diskriminierung	19
3.7	Beispiel - Kreditwürdigkeitsprüfung	20
4	<i>Kollektive Verantwortung – The Big Picture</i>	22
5	<i>Literaturnachweise</i>	23
6	<i>Anhang</i>	25

1 PayPal: Geschäftsmodell

1.1 PayPals Kerngeschäftsmodell

Online-Zahlungsanbieter wie PayPal verarbeiten umfangreiche Transaktionsdaten und sind die Vermittler zwischen Händlern und ihren Kunden. PayPal unterstützt weltweit über 400 Millionen aktive Verbraucher und Händler. Jede Minute finden mehrere tausend Zahlungstransaktionen statt. Die Beziehungen in diesem Zahlungsnetzwerk sind starke Prädiktoren für Verhaltensweisen und wichtige Risikoindikatoren, die Betrug aufdecken können.

Es gibt 426 Millionen aktive Konten bei PayPal. Im Jahr 2021 wurden 19,3 Milliarden Zahlungstransaktionen über diesen Dienst abgewickelt. Sie summierten sich auf 1,25 Billionen US-Dollar.

In einer Studie von Preibusch et al. (2016) wurden 881 US-amerikanische Webshops analysiert, und die Autoren fanden heraus, dass mehr als die Hälfte von ihnen Produktnamen und -details mit PayPal austauschen, sogar über sensible Produkte wie Medikamente und Sexspielzeug. Die Mindestdatenanforderungen für die Zahlungsabwicklung sind die Bestellsumme, der empfangende Händler und eine authentifizierte Zahlungsmethode. Bei Online-Einkäufen steht jedoch eine wesentlich umfangreichere Palette von Daten zur Verfügung, darunter ein Einzelverbindungs-nachweis oder Informationen über Käufer*innen. Das Sammeln von Daten, die für die Abwicklung von Zahlungstransaktionen nicht notwendig sind, ist auch eine finanzielle Entscheidung, denn es ist teuer, die Daten von 426 Millionen PayPal-Nutzern zu speichern. Das bedeutet, dass die gesammelten Daten in irgendeiner Weise verwendet werden müssen, um PayPal Gewinn zu bringen.

Datenschutzbedenken beziehen sich hier nicht nur auf die personenbezogenen Informationen, sondern auch auf das Verbraucherverhalten. Zahlungsanbieter sind in der Lage, in großem Umfang Kaufdaten zu sammeln und zu verknüpfen, um Verhaltensmuster von Verbraucher*innen zu erstellen. Auf diese Weise kann PayPal umfassende Konsumprofile über die Webseiten erstellen, auf denen Verbraucher*innen einkaufen, ein Abonnement abschließen oder spenden. Preibusch et al. (2016) fanden außerdem heraus, dass PayPal Einkaufsdetails an *Omniure* weiterleitet, einen Drittanbieter-Datenaggregator mit einer noch größeren Tracking-Reichweite. PayPal sendet auch Browsereigenschaften wie Plugins und Bildschirmgröße und ermöglicht es *Omniure* daher, Nutzer anhand ihrer Browser-Fingerabdrücke zu verfolgen, selbst wenn sie Cookies blockieren oder den privaten Browsing-Modus verwenden (Eckersley, 2010).

Außerdem sammelt PayPal bei den meisten Zahlungen Daten über Nutzer*innen. Diese Option kann von den Händlern deaktiviert werden, aber die meisten sind sich dieses Prozesses nicht bewusst oder wissen nicht, wie sie diese Option deaktivieren können. Wenn sich Nutzer*innen sicher fühlen, weil sie überprüfen können, ob alle Zahlungsdaten wie Kaufdaten, Zahlungsdaten, Adresse usw. korrekt sind, sind alle Daten einsehbar, die an PayPal weitergeleitet werden. Die meisten Tochterunternehmen von PayPal haben mit dem Zahlungsverkehr zu tun, aber PayPal hat auch begonnen, Unternehmen zu kaufen, die mehr mit Marketing zu tun haben.

Die folgenden Tochterunternehmen gehören zu PayPal:
Venmo, Xoom, PayLater, Paidy, Braintree, Hyperwallet, PayPalZettle, Simility, Chargehound, Happy Returns, **Honey**.

1.1.1 PayPal und Honey

Im Januar 2020 übernahm PayPal die Honey Science Corporation, die für die Entwicklung einer Browsererweiterung bekannt ist, die Online-Gutscheine auf E-Commerce-Websites sammelt und automatisch anwendet.

PayPal selbst behauptet, dass diese Übernahme getätigt wurde, weil "wir glauben, dass unsere Akquisition von Honey unser Wertangebot verbessern wird, indem sie es uns ermöglicht, Einkaufserlebnisse für Verbraucher weiter zu vereinfachen und zu personalisieren".

Nutzer*innen können ihre Honey- und PayPal-Konten miteinander verknüpfen, um Honey Gold-Prämienpunkte einzulösen, die auf ihr PayPal-Guthaben überwiesen werden, Angebote zu entdecken und Einkäufe zu tätigen. Die direkte Integration von Honeys Prämienprogramm mit PayPal soll mehr Honey-Nutzer*innen zur PayPal-App bringen, die Nutzerbasis vergrößern und Cross-Promotion-Möglichkeiten für andere Einkaufs- und Finanzdienste von PayPal schaffen.

Die Übernahme von Honey und die Verwendung von Modellen in Entscheidungsprozessen hat sofort einige ethische Bedenken aufgeworfen, dass die Erweiterung ein Sicherheitsrisiko darstellt und persönliche Informationen verkauft, da die Personalisierung des Erlebnisses bedeutet, dass die Daten der Nutzer*innen weit über die grundlegenden Sicherheitsmodelle hinaus verarbeitet werden. Laut den Unterlagen für die Aktionäre und dem Formular 10-K¹ von PayPal werden Modelle bei der Entscheidung über die Gewährung eines Kredits an einen Verkäufer und bei der Betrugserkennung eingesetzt. Wären dies die einzigen Modelle, die das Unternehmen verwendet, bräuchte es vor allem die Finanzdaten der Nutzer*innen, aber sie wären nicht in der Lage, die Nutzererfahrung mit dieser Art von Informationen wirklich zu verbessern. Die Übernahme von Honey durch PayPal bietet den Nutzer*innen eine neue Möglichkeit, Prämienpunkte einzulösen und Rabattcodes für Online-Einkäufe zu erhalten. Andererseits erhält PayPal dadurch auch eine große Menge an neuen Informationen über seine Kunden.

1.2 PayPals Werbestrategien

PayPal ist in verschiedenen Social-Media-Diensten stark vertreten. Die größte Sammlung an Marketingstrategien von PayPal ist auf YouTube zu finden, wo sogar TV-Werbespots zur Verfügung stehen, und bietet eine Menge kommerziellen Input, der an die jeweilige Plattform angepasst ist. Ihr YouTube-Kanal (Link im Anhang) scheint an sich dazu gedacht zu sein, allen Nutzer*innen (Privatkunden, Unternehmen usw.) zu helfen und hilfreiche Informationen darüber zu liefern, wie die Funktionen von PayPal genutzt werden können und welche Vorteile sie bieten, meist unabhängig von Informationen über ihre Datenschutzbestimmungen.

Kommerzielle Strategien können im Allgemeinen in die Ansprache von Privatkunden und Unternehmen unterteilt werden. Bei den Privatkunden werden die internen Bedürfnisse wie Einfachheit, Schnelligkeit, Vielfalt und Sicherheit angesprochen. PayPal bringt die Vorteile seines Services durch diese Bedürfnisse zum Ausdruck, indem es seinen "schnellen Checkout", die vielfältigen Einsatzmöglichkeiten des PayPal-Checkouts (z.B. Amazon, Deutsche Bahn, kleine Webshops, etc.) und seinen umfangreichen Käuferschutz hervorhebt. Darüber hinaus zeigt die Werbung für neue Implementierungen wie die neue Ratenzahlungsoption, dass PayPal die aktuellen Entwicklungen seiner Konkurrenten (in diesem Fall Klarna) stets im Auge behält. Einer von vielen Slogans für Privatkunden

¹ <https://investor.pypl.com/financials/sec-filings/sec-filings-details/default.aspx?FilingId=14673604>

lautet: "Willste? Kriegste. Das ist der PayPal Unterschied." (Links zu Privatkunden-Werbespots im Anhang.)

Für Geschäftskunden und Unternehmen scheinen die Tatsachen des intensiven Wettbewerbs und die Wurzeln der sinkenden Fluktuationsraten immanent zu sein. Soziale Normen werden als präskriptive Regeln genutzt, um die Aufmerksamkeit zu erlangen und die Vorteile der Nutzung von PayPal anhand von numerischen Visualisierungen und Entwicklungen zu unterstreichen. Ihre Vorschläge zur Steigerung des Vertrauens in Online-Shops und einer besseren Kundenerfahrung sollen dazu beitragen, den wirtschaftlichen Standpunkt des Unternehmens zu verbessern. Ein Slogan, der zur Darstellung des Hauptziels verwendet wird, lautet: "Einkaufen. Leichtgemacht." (Links zu Privatkunden-Werbespots im Anhang.)

1.3 PayPal und Schnittstellen zur Anwendungsprogrammierung

Unternehmen können Rechenzeit, Speicherplatz und Lizenzgebühren mieten, indem sie Apps über das Internet ausführen. Die Unternehmen müssen dann nicht in teure Hardware, Softwarelizenzgebühren und Personal für die Wartung der Anwendungen investieren. Sogenannte Application Service Provider (ASP)-Modelle ermöglichen eine monatliche Abonnementgebühr und flexible Verträge. Solche Cloud-Computing-Ressourcen sind vor allem für kleine Unternehmen von Vorteil, weil sie dann keine große Infrastruktur aufbauen müssen. PayPal hat die Programmierschnittstelle (Application Programming Interface; API)² für Händler*innen mit einer grundlegenden Kreditkartenzahlungsfunktion eingeführt. Damit kann jedes kleine Unternehmen sein Geschäft mit nahezu null Investitionen starten und Zahlungen über das Internet via PayPal annehmen. Wenn Nutzer*innen in einem Online-Shop auf die Schaltfläche "Kasse" klicken, wird eine Anfrage an PayPal gesendet. Nutzer*innen geben dann Kreditkartendaten ein, die dann an den Webshop zurückgesendet werden. Benutzer*innen werden dann auf die Bestätigungsseite für die Kaufabwicklung weitergeleitet.

APIs werden zunehmend in alltäglichen Dingen verwendet, wenn wir Apps auf unseren Smartphones nutzen. Die ethischen Bedenken, die sich daraus ergeben, sind, dass die Auslagerung der Datenspeicherung an einen Cloud-Betreiber zu Problemen mit dem Datenschutz führt. Je mehr APIs verwendet werden, desto anfälliger wird unsere Privatsphäre, wenn eine Cloud angegriffen wird. Auch wenn die Datenschutz-Grundverordnung (DSGVO) die Unternehmen rechtlich dazu verpflichtet, die Daten der Nutzer*innen zu schützen, muss darauf hingewiesen werden, dass selbst die besten und sichersten Systeme und APIs nie vollständig vor potenziellen Angriffen geschützt sein werden.

Zusammenfassung

PayPal behauptet, dass die Zahlungsdaten nicht an Verkäufer*innen weitergegeben werden. "Wir speichern Ihre persönlichen Daten in sicheren Datenbanken. Darüber hinaus verschlüsseln wir Ihre vertraulichen Informationen automatisch, wenn sie gespeichert und übertragen werden. Ihre Daten können nicht abgefangen werden, wenn sie von Ihrem Computer zu unserem gesendet werden. Und wenn Sie mit PayPal einen sicheren Einkauf tätigen, geben wir Ihre Zahlungsdaten nicht an den Verkäufer weiter."³

² What is the API (Application Programming Interface) actually? Rough explanation about the API:
<https://blog.mage.com/what-is-the-api-application-programming-interface-actually-36bf1045fd31>

³ How does PayPal store my data and keep my data secure?
<https://www.paypal.com/va/smarthelp/article/how-does-paypal-store-my-data-and-keep-my-data-secure-faq4468>

Wenn man sich jedoch ansieht, welche Informationen über APIs abgerufen werden können, wird deutlich, dass PayPal sensible und persönliche Daten auf Anfrage an den Verkäufer weitergibt. Darüber hinaus eröffnet die Anwerbung kleinerer Marketing- und Zahlungsdienste/-anbieter (wie Honey) PayPal die Möglichkeit, viel umfangreichere Datensätze zu erwerben und eine wesentlich fundiertere Einschätzung, Vorhersage und Analyse der Nutzerprofile vorzunehmen.

2 PayPal: Benutzeroberfläche

2.1 Allgemeine Geschäftsbedingungen

Dies ist ein Vergleich der Anzahl der Wörter, die in den Allgemeinen Geschäftsbedingungen verschiedener Unternehmen die Online-Zahlungen anbieten, enthalten sind. Die PayPal-Nutzungsvereinbarung (engl.: User Agreement) ist ein Dokument, das weitaus mehr Wörter enthält als die anderer Unternehmen und daher auch mehr Zeit zum Lesen benötigt. Eine Umfrage von Marktwächter⁴ ergab, dass Nutzer*innen maximal 5 Minuten für das Lesen der Allgemeinen Geschäftsbedingungen aufwenden wollen:

Welches Dokument? ⁵	Wörteranzahl	Lesedauer (*durchschnittlich lesen Erwachsene 240 Wörter pro Minute)
PayPal User Agreement	20,586	1'26''
Klarna Terms for Service	5,850	24''
Amazon Pay User Agreement	10,748	44''
Paydirekt	7,047	29''

Im Januar 2018 hat PayPal Deutschland eine neue Version der Allgemeinen Geschäftsbedingungen in deutscher Sprache veröffentlicht. Dieses Dokument bestand aus mehr als 20.000 Wörtern und 1.000 Sätzen, wobei der längste davon mehr als 111 Wörter umfasste. Nach Ansicht von Experten verstößt PayPal damit gegen den Grundsatz der Transparenz und benachteiligt Nutzer*innen. Eine wissenschaftliche Textanalyse hat ergeben, dass die Allgemeinen Geschäftsbedingungen von PayPal formal unverständlich sind und der Zeitaufwand, den Nutzer*innen investieren müssen, unzumutbar ist. Man hat keine realistische Chance, dieses Dokument zu lesen und zu verstehen, und PayPal versucht sich dadurch eine bessere Position im Markt zu verschaffen. In neueren Versionen hat PayPal seine Allgemeinen Geschäftsbedingungen zwar gekürzt, aber es ist immer noch das längste Dokument im Vergleich zu anderen.

Außerdem sind die Sätze in den Allgemeinen Geschäftsbedingungen und den Datenschutzerklärungen oft kompliziert und als Passivkonstruktionen formuliert. Wörter und Formulierungen wie "möglicherweise" und "unter anderem" machen sie noch vager und schwerer verständlich.

2.2 Wirkung nach Außen

2.2.1 Hintergrundinformationen zu täuschendem Design - Dark Patterns

Sogenannte *Dark Patterns* beeinflussen die Entscheidungen von Nutzer*innen in eine Richtung, die sie sonst wahrscheinlich so nicht getroffen hätten. Oft ist diese Beeinflussung nicht im besten Interesse der Nutzer*innen, da sie dazu gebracht werden, z. B. mehr Geld auszugeben als sie beabsichtigen (Narayanan et al., 2020). Vor allem Online-Diensteanbieter versuchen Nutzer*innen zu täuschen, damit sie freiwillig Zugang zu ihren persönlichen Daten gewähren (Bösch et al. 2016). All dies geschieht durch die Ausnutzung kognitiver Gedankenmustern (engl.: cognitive bias). Es gibt viele

⁴ Marktwächter mahnen PayPal ab: <https://www.vzbv.de/pressemitteilungen/marktwaechter-mahnen-paypal-ab>

⁵ Basierend auf den englischen Versionen der Dokumente

Möglichkeiten, Verhaltenstatsachen in effektive Benutzeroberflächen umzuwandeln, z. B. die Aufdeckung von Verhaltensänderungen durch Nudge-Bewegungen und datengetriebene Optimierung (Nutzer*innen werden verschiedene Designs ausgesetzt, dann wird analysiert welches am besten funktioniert). Ausgehend von diesen Strategien befürchten Narayanan et al. (2020) einen kommenden Trend, bei dem Unternehmen Dark Patterns als Dienstleistung anbieten.

Bösch et al. (2016) heben das Beispiel von Nutzerlogins auf Startseiten hervor, die einen Login mit persönlichen Konten wie Facebook oder Google in den Focus stellen und einen weniger hellen und auffälligen "Erstelle einen separaten Account"-Button sowie einen versteckten Skip-Button (oft in der oberen rechten Ecke) zeigen. Der Hintergrund scheint zu sein, durch absichtlich schlechtes Design auf z.B. Freundeslisten, Fotos und Likes zuzugreifen und damit an Informationen zu gelangen, die für den Dienst im Grunde nicht notwendig sind.

Muster und Strategien

Es gibt verschiedene Arten von Strategien und Mustern, die beschreiben, wie Schnittstellenmuster implementiert werden können, sowie verschiedene Ansätze zur Analyse dieser Schnittstellenstrategien.

Bösch et al. (2016) beschreiben die Entwicklung von Dark Patterns wie folgt: In den anfänglichen Prinzipien für "Privacy Design", aus denen die verschiedenen Datenschutzmuster entstanden sind, ging es vor allem darum, die Privatsphäre der Nutzer*innen zu bewahren und zu verbessern, indem den Entwickler*innen strukturierte Problemlösungsbeschreibungen mit Hilfe von standardisierten und leicht nachzuschlagenden Vorlagen zur Verfügung gestellt werden. Da eine beträchtliche Anzahl von Gruppen oder Einzelpersonen versucht, die Privatsphäre der Nutzer*innen absichtlich aus kriminellen oder finanziellen Gründen auszunutzen, indem sie diese Muster in umgekehrter Weise verwenden, haben Bösch et al. (2016) die Entwicklung von Datenschutzstrategien und -mustern in "Dark Privacy"-Strategien und "Dark Privacy"-Muster zurückentwickelt (zusammengefasst in Abbildung 1 im Anhang). Mit den daraus entstandenen dunklen Datenschutzmustern wollen Bösch et al. (2016) nicht-technisch versierte Endnutzer*innen ansprechen und ihnen helfen, sich zu informieren.

Hoepman (2014) bildet darüber hinaus seine Strategien auf rechtliche Prinzipien ab, die mit den (damals) bestehenden Datenschutzgesetzen übereinstimmen (siehe Abbildung 2 im Anhang) und setzt sie in ein Datenbankschema, um ihr Zusammenspiel zu visualisieren (siehe Abbildung 3 im Anhang).

Psychologischer Hintergrund

Es ist bekannt, dass ein gewisses Maß an Bewusstsein über die Existenz von "Dark Privacy"-Strategien unter Nutzern*innen verbreitet ist. Nichtsdestotrotz sind solche versteckten Strategien aufgrund ihrer Häufigkeit, die sich aus den psychologischen Untersuchungen zu diesen Strategien ableiten lässt, immer noch wirksam. Deren Hauptaugenmerk scheint auf der kognitiven Informationsverarbeitung und der psychologischen Verfassung zu liegen (Bösch et al., 2016).

Bösch et al. (2016) beschreiben zwei Denkprozesse:

1. **System-1-Denkprozess:** automatisch, unbewusst und mit wenig Aufwand (z.B. einer Liste von Bedingungen, die unnötig komplex und unverständlich sind, schnell, intuitiv und automatisch zustimmen).
2. **System 2:** kontrollierter, bewusster und anstrengender Denkprozess; angetrieben durch abwägende, anstrengende Entscheidungsfindung → langsames Ausführungsverhalten

Darüber hinaus heben Bösch et al. (2016) das "menschliche Grundbedürfnis nach Zugehörigkeit" als großen Einfluss auf die Wirksamkeit von Privacy Dark Patterns hervor. Dies erscheint logisch, da der Mensch danach strebt, ein akzeptiertes Mitglied einer bestimmten Gruppe zu sein und die Reduzierung des eigenen Wohlbefindens zu vermeiden. Dies berücksichtigend behaupten Bösch et al. (2016), dass die Bereitschaft der Menschen, persönliche Daten preiszugeben, deutlich steigt.

Empfehlungen für den Umgang mit Dark Patterns

Versteckte Strategien und Muster, die mit Datenschutz und Privatsphäre zusammenhängen, sind aufgrund mangelnder Motivation und Möglichkeiten der Menschen, sich zu wehren, wirksam. Nach den Erkenntnissen aus den psychologischen Hintergründen müssen die Denkprozesse des Systems 2 trainiert und gestärkt werden. Dies kann durch die Erhöhung der Motivation geschehen, indem die negativen Folgen von solchen versteckten Strategien immer wieder in den Vordergrund gerückt werden.

2.2.2 Nudging

Nudging-Strategien nutzen kognitive Abkürzungen, die bei (irrationalen) Entscheidungen beobachtet werden, um irrationales Verhalten erklärbarer und sogar vorhersehbar zu machen. Da sie deskriptive soziale Normen als präskriptive Regeln verwenden, können sie wirksam eingesetzt werden und werden bereits von Instanzen wie Regierungen, Arbeitgebern und Unternehmen angewendet (Narayanan et al., 2020).

Ein von Narayanan et al. (2020) vorgeschlagenes Beispiel, um Nutzer*innen zu schnellen Entscheidungen zu bewegen, sind Sätze wie der folgende: "7 Leute schauen sich das gerade an!" oder "Dieses Angebot läuft in 15 Minuten ab!". Diese Beispiele bringen Nutzer*innen dazu, mit einem Gefühl der Dringlichkeit zu handeln, indem sie ein abstraktes Prinzip in einen konkreten Anstoß verwandeln.

2.2.3 Dark Patterns und Nudging: PayPal

PayPal setzt Dark Patterns und Nudging-Strategien nicht so offensichtlich wie viele andere Dienste ein. Man kann argumentieren, dass dies auf ihren Ruf zurückzuführen ist und sie diese Strategien nicht so stark einsetzen müssen. Einige Beispiele von der Website, bei denen eine Art von Dark Patterns oder Nudging verwendet werden, sehen wie folgt aus (je nach Sprache/Land werden unterschiedliche Muster angezeigt):

Private Kund*innen:

How PayPal works

Your PayPal journey starts here.

Join the millions of people who trust PayPal to send, spend, and manage their money quickly and securely.

Sign Up

Get the App

Ein Beispiel für ein Dark Pattern, bei dem verschiedene Schaltflächenfarben verwendet werden, um Benutzer*innen dazu zu bringen, sich bei PayPal anzumelden.

PayPal richtet sich an das grundlegende Bedürfnis der Nutzer*innen, dazuzugehören. Der Zähler zählt nicht die tatsächliche Anzahl der Nutzer*innen. Er beginnt immer bei 346.000.000 Nutzern, wenn man die Website öffnet.

Join the millions of users worldwide trusting PayPal every day

Sign Up for Free

3 4 6 0 0 0 0 2 6

Join the millions around the world who love PayPal

Easily and securely spend, send, and manage your transactions—all in one place. Download the app on your phone or sign up for free online.



Scan the code or enter your number to get the app.

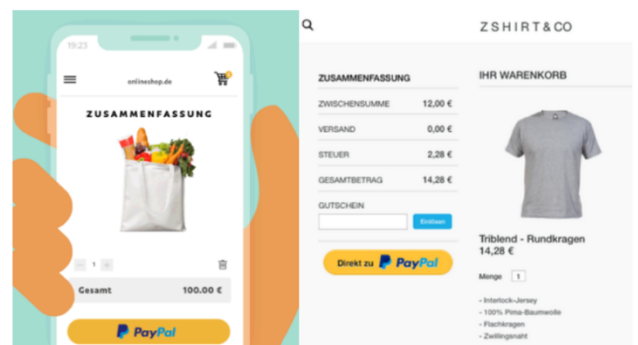
Phone number

Send Link

By clicking Send Link you agree to receive a text message with a link to the PayPal app. Message and data rates may apply.

PayPal zwingt Nutzer*innen, sich die App überhaupt zu besorgen. Außerdem wird versucht, die Aufmerksamkeit und das Bedürfnis zu wecken, indem man Nutzer*innen sagt, dass viele Menschen PayPal bereits lieben und die Vorteile hervorhebt.

Ein Beispiel für die Schaltfläche "Express-Kasse" mit leuchtenden Farben, die auffallen. Sie suggeriert "PayPal-Sicherheit" und erhöht damit das Vertrauen in die Shops.



Unternehmen:

For Small-to-Medium Business

Everything starts with your Business account

Join over 30 million merchants who rely on PayPal.

Contact Sales




Sign Up

PayPal bietet darüber hinaus viele Zahlenbeispiele und benutzerfreundliche Optionen, die das eigene Geschäft profitabler machen.

Ein Dark Pattern mit verschiedenfarbigen Schaltflächen, damit sich das Unternehmen/der Online-Shop bei PayPal anmeldet.

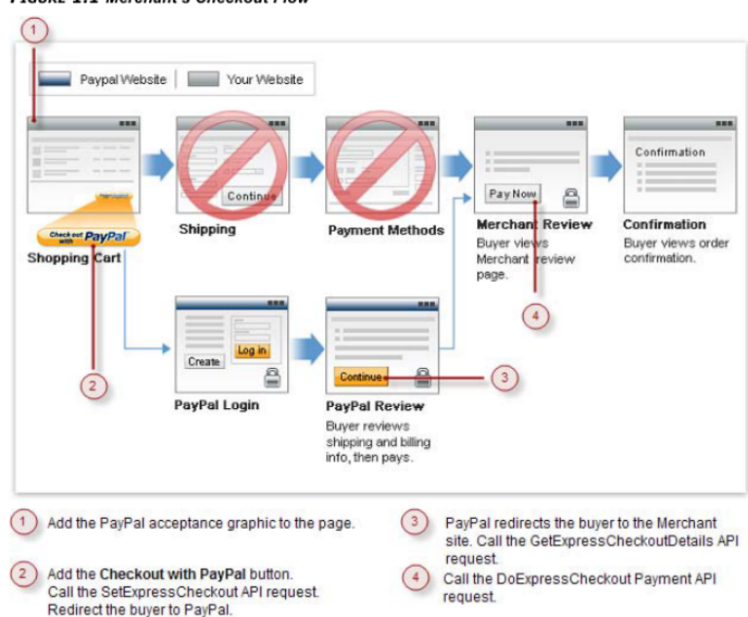
The one stop solution with more payment options

Transparent pricing with no monthly commitment. Here's what's included:

 Manage risk PayPal can help make the way you do business more secure.	 More payment options Accept the most popular payment methods your customers use.	 Trust in PayPal Do business backed by a company you and your customers can trust.
<ul style="list-style-type: none">✓ Reliable security<ul style="list-style-type: none">• Powerful fraud protection• Data-security (PCI) compliance coverage✓ Seller Protection for merchants on eligible transactions¹✓ Chargeback Protection⁴✓ Dispute management	<ul style="list-style-type: none">✓ Global payment with single integration<ul style="list-style-type: none">• 200+ markets• 100+ different currencies✓ Debit and credit cards✓ Payment methods available only from PayPal✓ Instant Transfer (Fees apply)✓ Payment links for getting paid remotely	<ul style="list-style-type: none">✓ Used by over 400 million customers worldwide✓ Over 20 years experience helping businesses✓ 69% of PayPal users report they are more likely to trust a retail website that offers payment through PayPal⁵

Neben anderen Optionen wie Entwicklertools (APIs usw.) stellt PayPal auch detaillierte Informationen zur Verfügung (PayPal, Inc. 2013), in denen sie Unternehmen dabei helfen, die "Vorteile" von PayPal zu nutzen, indem sie Kund*innen mitteilen, dass PayPal für sie verfügbar ist. Der Leitfaden erklärt detailliert, wie die Schaltfläche für die Express-Kaufabwicklung genau platziert werden muss, um die Aufmerksamkeit der Nutzer*innen zu erhalten und sie zum Kauf von Artikeln in ihrem Shop zu bewegen. Sie wollen "digitalen und physischen Handel miteinander verbinden, um nahtlose Kundenerlebnisse zu schaffen".

FIGURE 1.1 Merchant's Checkout Flow



3 Big Data und Datenschutz

3.1 Hintergrund

Heutzutage können personenbezogene Daten wie eine Währung gehandelt werden. Es gibt unterschiedliche Meinungen darüber, inwieweit diese Situation ethisch vertretbar ist. Im Handelsmodell für personenbezogene Daten bietet die Übermittlung personenbezogener Daten den Menschen die Möglichkeit ihre digitale Identität zu kontrollieren und genaue Vereinbarungen über die gemeinsame Nutzung von Daten zu treffen. Die Idee der transparenten Daten basiert auf dem Argument, dass Daten frei verfügbar sein sollten. Die Bereitschaft, Daten zu teilen, ist jedoch von Person zu Person unterschiedlich.

Die Summe der personenbezogene Daten einer Person bildet eine **digitale Identität**. Eine digitale Identität hat den Vorteil, dass sie schnellen Zugang zu Online-Inhalten und damit verbundenen Diensten bietet. Ihre Nutzung kann zu Diskriminierungen führen, die auf der Darstellung einer Person anhand ihrer Online-Daten beruhen, die oft nicht der Realität entsprechen. Wir scheinen in einem Prozess gefangen zu sein, der "Datendiktatur" genannt wird, in dem „wir nicht mehr auf der Grundlage unserer Handlungen beurteilt werden, sondern auf der Grundlage dessen, was alle Daten über uns auf unsere wahrscheinlichen Handlungen hinweisen“.⁶

Eine grundlegende Frage im Zusammenhang mit der Ethik der Big-Data-Forschung lautet: Wem gehören die Daten? Dabei geht es um die Frage der Eigentumsrechte und -pflichten. Im europäischen Recht besagt die Datenschutz-Grundverordnung (DSGVO)⁷, dass Personen das Eigentum an ihren eigenen personenbezogenen Daten haben. Die DSGVO hat die Datenlandschaft in der Europäischen Union (EU) seit ihrer Umsetzung im Mai 2018 grundlegend verändert. Laut einer Umfrage der Data and Marketing Association (DMA) unter britischen Verbrauchern geben 62% der Verbraucher an, dass die DSGVO ihr Vertrauen in die Weitergabe von Daten an Unternehmen stärken wird. Der Schutz personenbezogener Daten einer Person beruht auf der Auffassung, dass sie einen direkten Ausdruck der eigenen Identität darstellen.

Die Beziehung zwischen denjenigen, die die Daten zur Verfügung stellen, und denjenigen, die sie verwenden, ist oft indirekt. Zwischen dem Akzeptieren von Allgemeinen Geschäftsbedingungen (AGBs) oder Cookies, die das Weitergeben von Daten in Mengen und Kombinationen von Daten erlauben die schwer vorstellbar sind, und der tatsächlichen Nutzung dieser Daten durch Unternehmen klafft eine große Lücke. Dritte können an verschiedenen Schritten der Kette beteiligt sein oder am anderen Ende der Kette darauf warten, Daten zu erhalten, die wir nicht direkt mit ihnen geteilt haben. Diese Daten sind entscheidend für die Identität einer Person und sollten sorgfältig behandelt werden, was in der Regel jedoch nicht der Fall ist.

⁶ Norwegian Data Protection Authority, 2013, from N. Sfetcu

⁷ <https://gdpr.eu> (Englisch); <https://dsgvo-gesetz.de> (Deutsch)

3.2 PayPals Datenschutzerklärung (6. Mai 2022)

In der Datenschutzerklärung³ führt PayPal auf welche personenbezogenen Daten von den Kund*innen gesammelt werden:

- Name, Adresse, Telefonnummer, E-Mail, Daten zur Identifizierung
- Gesendeter oder angeforderter Geldbetrag, gezahlter Betrag für Produkte oder Dienstleistungen, Händlerinformationen, einschließlich Informationen über alle Finanzierungsinstrumente, die zum Abschluss der Transaktion verwendet wurden, Geräteinformationen, technische Nutzungsdaten und Geolokalisierungsinformationen
- Personenbezogene Daten jedes Teilnehmers an einer Transaktion
- Wenn Nutzer*innen eine Verbindung zwischen dem persönlichen Gerät oder einer Social-Media-Plattform und dem eigenen PayPal-Konto herstellen, verwendet PayPal die Informationen aus der Kontaktliste der Person (z. B. Name, Adresse, E-Mail-Adresse), um das Nutzererlebnis des Services zu verbessern.

Es wird weiter erklärt, warum personenbezogene Daten gesammelt werden und wie lange diese gespeichert werden:

"Wir bewahren personenbezogene Daten in einem identifizierbaren Format so lange auf, wie es für die Erfüllung unserer gesetzlichen oder behördlichen Verpflichtungen und für unsere Geschäftszwecke erforderlich ist. Wir können personenbezogene Daten länger als gesetzlich vorgeschrieben aufbewahren, wenn dies in unserem legitimen Geschäftsinteresse liegt und nicht gesetzlich verboten ist. Wenn Ihr Konto geschlossen wird, können wir Maßnahmen ergreifen, um personenbezogene Daten und andere Informationen zu maskieren, aber wir behalten uns die Möglichkeit vor, die Daten so lange aufzubewahren und auf sie zuzugreifen, soweit die geltenden Gesetze eingehalten werden. [...] Wir können Ihre personenbezogenen Daten auch verarbeiten, wenn wir glauben, dass dies in unserem oder dem berechtigten Interesse anderer liegt, wobei Ihre Interessen, Rechte und Erwartungen berücksichtigt werden."⁸

Die Datenschutzerklärung von PayPal und auch die AGBs sind Verträge, bei denen Nutzer*innen keine Möglichkeit haben, etwas zu ändern, sondern nur ablehnen oder akzeptieren können. Nutzer*innen könnten daher weniger motiviert sein diese Dokumente zu lesen. Da Nutzer*innen das Produkt sind und die Unternehmen mit dem Sammeln ihrer Daten Gewinne erzielen, sind die Unternehmen nicht daran interessiert, die Dokumente verständlicher zu gestalten. Ihr Ziel ist es, dass Nutzer*innen sie schnell akzeptieren und ihren Service nutzen. Dies zeigt auch, dass PayPal, anders als in der Datenschutzerklärung behauptet, nicht nach den Interessen und Erwartungen der Nutzer*innen fragt und diese berücksichtigt.

In der Datenschutzerklärung erklärt PayPal weiter, dass die personenbezogenen Daten der Nutzer*innen für den Betrieb der Website, die Verwaltung der geschäftlichen Anforderungen (einschließlich der Analyse, Überwachung und Verbesserung seiner Website), dem Risikomanagement und die Bereitstellung personalisierter Dienste, auch "interessenbasiertes Marketing" genannt, verwendet werden. Mit dem Einverständnis der Nutzer*innen setzt PayPal Cookies⁹ und Tracking-Technologien ein, um die Erfahrungen und Dienste des Nutzers anzupassen, die Wirksamkeit von Werbeaktionen zu messen und potenziellen Betrug zu verhindern.

Beim sogenannten interessenbasierten Marketing wird Werbung präsentiert, die auf Grundlage früherer Suchanfragen und der Analyse von Verhaltensdaten persönlichen Interessen

⁸ Basierend auf der englischen Version von PayPals Privacy Statement: <https://www.paypal.com/de/legalhub/privacy-full>

⁹ This is an explanation of how PayPal uses cookies: <https://www.paypal.com/US/webapps/mpp/ua/cookie-full>

entspricht. Wird dies zum Beispiel im politischen Wahlkampf angewandt, werden den Menschen immer extremere Meinungen zu politischen Themen präsentiert, um ihre Haltung zu beeinflussen. Dies kann schließlich zu einer Polarisierung führen, die nicht auf neutralen Fakten beruht, sondern auf einem Algorithmus, der dem Einzelnen Themen und Anzeigen präsentiert, die scheinbar zu den individuellen Interessen passen und auf die die Person schließlich klickt.

In der Datenschutzerklärung von PayPal heißt es weiter, dass das Unternehmen gesammelte statistische Daten individueller Person, die Aufschluss darüber geben, wie, wann und warum Nutzer*innen eine Website besuchen und seine Dienste in Anspruch nehmen an Dritte weitergibt, wobei versprochen wird, dass diese Daten keine Rückschlüsse auf einzelne Personen zulassen. PayPal erklärt personenbezogene Daten der Nutzer*innen nicht ohne Zustimmung an Dritte für deren Marketingzwecke weiterzugeben.

Schließlich erklärt PayPal, dass die personenbezogenen Daten seiner Nutzer*innen zu Geschäftszwecken oder im Rahmen der gesetzlichen Bestimmungen an andere Dritte weitergibt. PayPal entscheidet, ob es notwendig ist, die personenbezogenen Daten an Dritte weiterzugeben, um körperliche Schäden oder finanzielle Verluste zu verhindern, oder wenn eine Person in eine Untersuchung mutmaßlicher oder tatsächlicher illegaler Aktivitäten eingebunden ist. PayPal beschreibt nirgendwo, welche Geschäftsinteressen verfolgt werden und welche personenbezogenen Daten zur Erfüllung dieser Interessen erforderlich sind. Sie sind intransparent gegenüber ihren Geschäftsinteressen, was einen Nachteil für Nutzer*innen darstellt, da nicht klar ist, welche Daten gesammelt werden und wofür diese Daten verwendet werden. Auf der Grundlage dieses Teils der Datenschutzerklärung könnte PayPal jede beliebige Information sammeln und stets argumentieren, dass dies zur Erfüllung der Geschäftsinteressen erforderlich ist, wobei auch hier nicht klar ist, was diese sind. Verbraucherschützer*innen kritisieren, dass PayPal mehr Daten als nötig sammelt¹⁰. Bei der Registrierung und Bezahlung werden zwischen 4 und 13 Einzelangaben erhoben. Bis zu 11 Tracker werden eingesetzt, um Informationen über das Verhalten der Verbraucher*innen für gezielte Werbung zu sammeln. Die Datenschutzgrundverordnung schützt die Nutzer*innen in solchen Situationen nicht.

Abschließend heißt es in der Datenschutzerklärung, dass PayPal mit Zustimmung der Nutzer*innen automatisierte Entscheidungsprozesse für Kreditentscheidungen einsetzen kann.

3.3 Sammeln und Teilen von persönlichen Informationen

Basierend auf den Informationen, die im AppStore zur Verfügung gestellt werden, sammelt PayPal folgenden Daten für Werbung und Marketing, Analyse, Personalisierung des Produkts und der App-Funktionalität:

- Einkaufshistorie
- Kontaktdaten (E-Mail-Adresse + Vorname + Nachname)
- Suchverlauf
- Browsing-Verlauf
- Informationen zur persönlichen Identifizierung
- Nutzungsdaten (u. a. Produktinteraktionen)
- Finanzielle Informationen (u. a. Informationen über Zahlungen, Kreditinformationen)
- Lokalisierung (genauer Standort und geschätzter Standort)

¹⁰ Kritik an Datenhunger von PayPal & Co: <https://help.orf.at/v3/stories/2878112/>

PayPal gibt an, dass die personenbezogenen Daten der Nutzer*innen an andere Mitglieder der PayPal-Unternehmensfamilie weitergegeben werden, zu denen Honey, Braintree, Paidly und Venmo gehören, um den Zahlungsservice bereitzustellen und möglichen Betrug zu bekämpfen.

PayPal gibt die personenbezogenen Daten der Nutzer*innen auch an andere Unternehmen weiter, die mit PayPal kooperieren, um die Identität der Nutzer*innen zu überprüfen, Werbung für PayPal-Dienste zu zeigen oder Kundendienst zu leisten. Die Daten der Nutzer*innen werden auch an andere Finanzinstitute weitergegeben, um den Nutzern*innen Vorteile zu gewähren und die Finanzdaten der Nutzer*innen auf dem neuesten Stand zu halten. Dies wirft ein ethisches Problem auf, denn es bedeutet eine ständige "Überwachung" des finanziellen Status eines Nutzers aus vielen verschiedenen Quellen, zu verschiedenen Zeitpunkten und aus einer Kombination von verschiedensten Quellen.

Verbrauchsverhalten, das mit einer Zahlungsmethode verknüpft ist, ist nicht pseudonym, sondern durch Offline-Details wie Kreditkartennummern oder Bankkontodaten identifizierbar. Wenn ein Unternehmen also daran interessiert ist, die Person hinter den pseudonymen Daten zu identifizieren, kann es dies tun indem es andere Informationen sammelt, die als Verbindung zwischen den pseudonymen Daten und der Person dienen und sogar die Verknüpfung mehrerer Transaktionen über verschiedene Logins oder Konten hinweg ermöglichen. Verbraucherdaten werden transaktionsübergreifend gesammelt und zusammengeführt, selbst bei sensiblen Produkten und Händlern.

Das Data-Science-Team von PayPal kann durch so genannte "Transaktionsdaten" dazu beitragen, Menschen gezielter anzusprechen. Transaktionsdaten sind Informationen wie Zeit, Ort, Geldbetrag, Zahlungsmethode usw. die während Transaktionen erfasst werden. Diese Art von Daten ist der solideste Faktor der Datenwissenschaftler*innen hilft das Kaufverhalten von Menschen vorherzusagen. **Transaktionsdaten sind der stärkste Anhaltspunkt bei der Vorhersage des Kundenverhaltens bei PayPal,** sogar stärker als Daten darüber, wie viele Personen sich ein Produkt angesehen haben, welche Website sie besucht haben usw..

3.4 PayPal und die Datenschutz-Grundverordnung (DSGVO)

In Artikel 5 der DSGVO wird festgelegt welche personenbezogenen Daten erhoben werden dürfen:

DSGVO Artikel 5. c):

(1) „Personenbezogenen Daten müssen

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).“

Die DSGVO hält fest, dass der Grundsatz der "Datenminimierung"¹¹ angewandt werden sollte. Das bedeutet, dass so wenig Informationen wie möglich für einen bestimmten Zweck erhoben werden sollen. Das Problem ist, dass das EU-Recht nicht definiert, was "angemessene, erheblich und auf ein notwendiges Maß beschränkte" Daten sind. Welche Daten benötigt und erhoben werden hängt vom Zweck ab, aber ein Unternehmen sollte nie mehr Daten erheben als für den Zweck, den es erfüllen will, notwendig sind. Die Datenerhebung ist unzureichend, wenn der Zweck der Verarbeitung nicht möglich

¹¹ What is "data minimization" under EU Data Protection Law? <https://medium.com/golden-data/what-is-data-minimization-under-eu-data-protection-law-b0e30fbb856e>

ist, und auch, wenn eine Entscheidung nicht getroffen werden kann, weil Informationen fehlen. Wenn Daten zur Entscheidungsfindung verwendet werden, liegt es im Interesse der Nutzer*innen so viele Daten wie nötig bereitzustellen, um eine faire Entscheidung treffen zu können. Der Nachteil ist jedoch, dass Nutzer*innen nie wissen ob die Erhebung dieser bestimmten Informationen wirklich notwendig ist und wie diesen Daten weiter verwendet werden könnten.

Wie oben dargestellt, heißt es in Artikel 5: "Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf die Zwecke der Verarbeitung notwendige Maß beschränkt sein (Datenminimierung)." **Da in der DSGVO nicht näher beschrieben wird, was "angemessene, erheblich und notwendige Daten" sind, kann PayPal alle Daten sammeln, solange sie dies mit den Geschäftsinteressen begründet werden kann, die für die Nutzer*innen nicht offensichtlich sind.**

3.5 Datenschutz und Kommunikation

PayPal selbst behauptet sehr an der Privatsphäre der Nutzer*innen interessiert zu sein, geht aber nicht klar darauf ein, wie die Privatsphäre geschützt wird. Basierend auf dem Dokument *Form-10k*¹² und der Unterlagen für Aktionäre scheint es dem Unternehmen eher um Datensicherheit zu gehen. Für das Unternehmen ist es sehr wichtig, dass die Daten der Nutzer*innen, insbesondere Finanzdaten wie Kreditkarteninformationen, nicht nach außen dringen. Die Erstellung von Nutzerprofilen wird jedoch nicht als etwas angesehen, das gegen den Datenschutz der Nutzer*innen verstößt. PayPal sammelt so viele Daten wie möglich und verwenden sie, um deren „Erfahrung zu verbessern“ und das Risiko für sich selbst zu verringern.

PayPal gibt an, dass sein globales Datenschutzprogramm auf den folgenden 8 Grundsätzen beruht:

- Verwaltung
- Transparenz
- Wahlmöglichkeit und Zustimmung
- Sicherheit
- Daten-Lebenszyklus-Management
- Datenqualität
- Verantwortlichkeit
- Standardisierung

Sie behaupten, dass sie die Kultur der "Data Hygiene by Default" und des "Privacy by Design" im gesamten Unternehmen integrieren, und das tun sie auch im gewählten Umfang. Darüber hinaus organisieren sie jährliche obligatorische Compliance- und Ethikschulungen für alle Mitarbeiter*innen und Auftragnehmer*innen. Man kann nicht behaupten, dass sie ihre Versprechen zum Datenschutz nicht einhalten. Dies ist jedoch nur deshalb der Fall, weil sie diese Versprechen so definieren, wie es ihnen passt, und sie sogar als Teil des Marketings für ihr Zahlungssystem als eine sicherere Option genutzt werden können.

¹² <https://investor.pypl.com/financials/sec-filings/sec-filings-details/default.aspx?FilingId=14673604>

3.6 Verbindung zu theoretischen Konzepten

Anhand der obigen Abschnitte wird deutlich, dass PayPal Daten sammelt die weit über die Informationen hinausgehen, die für die Verarbeitung einer Zahlung erforderlich sind. Je mehr Daten gesammelt werden, desto größer der Erfolg für Algorithmen der künstlichen Intelligenz (KI) und des maschinellen Lernens (ML) in diesen Daten verborgene Muster zu finden die unser Verhalten vorhersagen. Darüber hinaus erleichtern riesige Datenmengen die Anwendung von *Prädiktiver Analytik*, um Vorhersagen über die künftige Entwicklung der Wirtschaft und der Marktaktivität im Allgemeinen oder über das künftige Kaufverhalten einer Person zu treffen. Außerdem kann dies zu einer Vorhersage über Personen führen, die Dienste wie PayPal überhaupt nicht nutzen. Mit immer leistungsfähigeren KI und einer zunehmenden Verfügbarkeit von großen und umfassenden Datenmengen wird *Proxy Diskriminierung* eine größere Herausforderung für Antidiskriminierung darstellen (Prince & Schwarcz, 2020).

3.6.1 Prädiktive Analytik

Prädiktive Analytik beschreibt eine Art Verhaltensmuster miteinander zu vergleichen (Mühlhoff, 2022). Riesige Datensätze werden automatisch analysiert und helfen Unternehmen besser zu verstehen, wie sich Menschen in bestimmten Situationen verhalten (Mishra & Silakrai, 2012). Neugier und der Versuch, künftige Ereignisse vorherzusagen, werden oft als Teil der menschlichen Natur definiert. Dadurch hat sich die Vorhersage künftiger Ereignisse auf der Grundlage zuvor gesammelter und analysierter Daten durch ML-Algorithmen und die Berechnung der Wahrscheinlichkeit des Eintretens einer bestimmten Situation schnell entwickelt (Mishra & Salikrai, 2012; Kumar et al., 2016). Auf dieser Grundlage definieren Mishra & Salikrai (2012) den Kern von Verhaltensprognosen als "Erfassung von Beziehungen zwischen erklärenden Variablen und den vorhergesagten Variablen aus vergangenen Ereignissen und deren Nutzung zur Vorhersage zukünftiger Ergebnisse".

Vereinfacht sieht ein Vorhersageprozess wie folgt aus (Ongsulee et al., 2018):



In der Phase der *Projektdefinition* werden die Ergebnisse und Projektrichtlinien festgelegt. Dazu gehören die Interessen der Unternehmen (auch als Prädiktoren bezeichnet), sowie ihre bevorzugten und möglichen Ergebnisse (Ongsulee et al., 2018). Ein Prädiktor beschreibt in diesem Fall die zu bestimmende Variable. Beispielsweise könnten Kreditkartenunternehmen an dem Risikofaktor (= Ziel) interessiert sein, der durch die Definition von Prädiktoren bestimmt werden kann, die berücksichtigt werden sollten: Alter, Einkommen, Kredithistorie und mehr (Mishra & Silakrai, 2012).

Die *Datenerhebung und -analyse* umfasst alles, was mit den Daten geschieht, angefangen bei der Quelle und der Art der Datenerhebung bis hin zur Analyse der Daten im Hinblick auf die vordefinierten Ziele (Ongsulee et al., 2018). Für das Kreditkartenunternehmen würde das bedeuten, dass die Datenanalyse Daten berücksichtigen muss, die das Alter, das Einkommen und die Kredithistorie der Nutzer*innen umfassen (Mishra & Silakrai, 2012).

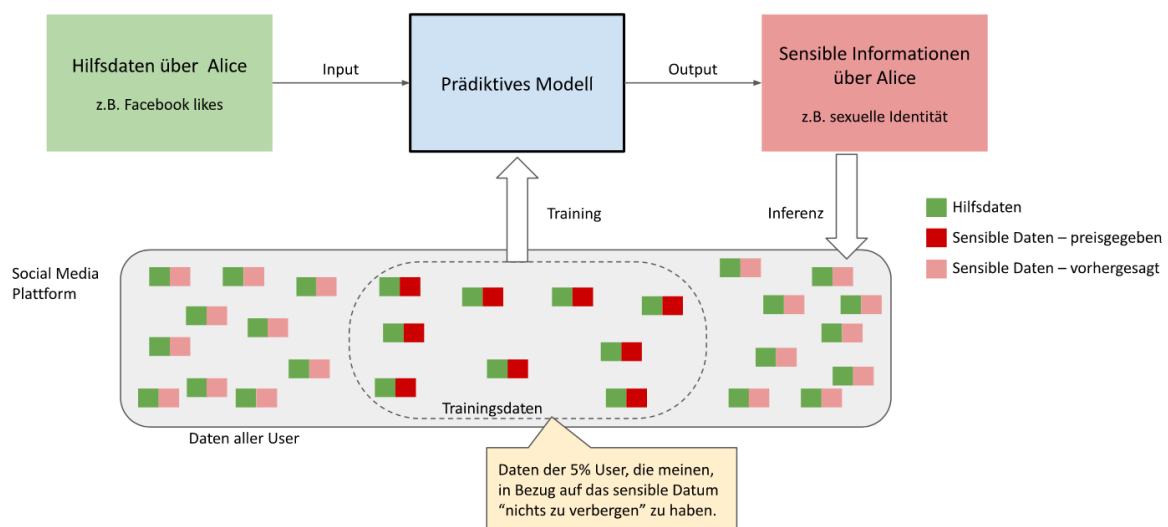
Die Durchführung von *Statistik und Modellierung* ermöglicht die Validierung und das Testen möglicher Ergebnisse, gefolgt von der Erstellung präziser Vorhersagemodelle für zukünftige Situationen (Ongsulee et al., 2018). Im Fall des Kreditkartenunternehmens werden Muster in Abhängigkeit von den Prädiktoren gefunden mit denen das Modell gefüttert und trainiert wird (Mishra & Silakrai, 2012).

In der *Einsatzphase* können die Ergebnisse in die alltägliche Entscheidungsfindung übertragen werden die auch weitere Ergebnisse erzeugt die wiederverwendet werden können, um das Modell zu trainieren und noch präziser zu machen. Diese Ergebnisse werden wiederum in der Phase der *Modellüberwachung* verwaltet und überwacht, um die Leistung des Modells zu steigern (Ongsulee et al., 2018).

Neben Kreditkartenunternehmen definieren Kumar et al. (2016) auch allgemeinere Anwendungen für Prädiktive Analytik:

- Direktmarketing und Vertrieb: Das Nutzungs- und Kundenverhalten auf der Website des Unternehmens kann analysiert werden, um die Wahrscheinlichkeit eines Verkaufs zu ermitteln und gezielt Werbung zu schalten.
- Kundenbeziehungen
- Optimierungen der Preisgestaltung: Anpassung von Nachfrage und Preis, um eine effiziente Preisstrategie zu erreichen.
- Gesundheitliche Ergebnisse: Verknüpfung von Symptomen mit Behandlungen und damit Erhöhung der Reaktionszeit bei der Diagnose von Krankheiten (z. B. Herzinfarkt)
- Versicherungsbetrug: Identifizierung von Mustern mithilfe statistischer Modelle für Prävention und Ermittlungen
- Unrechtmäßige Zahlungen von öffentlichen Leistungen und Betrug: Weniger Steuerverschwendung und Gewährleistung von Unterstützung für diejenigen, die sie benötigen
- Steuereintreibung: Identifizierung geschuldeter Steuern
- Vorhersage und Prävention von Straßensriminalität, häuslicher Gewalt und Terrorismus: Ermittlung von Hochrisikosituationen und -orten

Neben den von Kumar et al. (2016) genannten positiven Effekten bringt die prädiktive Analytik einige Herausforderungen mit sich, die es zu berücksichtigen gilt. Die wichtigsten Herausforderungen die Mishra & Silakrai (2012) nennen, sind der Schutz der Privatsphäre und des Eigentums sowie von Datenökosysteme und -austausch. Dies bedeutet, dass ein hohes Potenzial für den Missbrauch von Daten besteht, ohne dass das Gesetz etwas davon erfasst, so dass dies zu Diskriminierung und sozialer Ungleichheit führen kann (Mühlhoff, 2022). Darüber hinaus wird die sensible Privatsphäre aller Menschen in hohem Maße verletzt, indem leicht zugängliche Daten für Vorhersagen verwendet werden (siehe Abbildung; Mühlhoff, 2022).



Es ist schwer zu behaupten, dass PayPal aktiv Datenerfassung betreibt, aber durch die Art und Weise, wie sie auf dem Markt navigieren und an Datenerfassung herangehen, scheinen sie mit

Sicherheit große Mengen an Informationen über ihre Nutzer*innen zu sammeln. Durch das Zwischenschalten verschiedener Tochterunternehmen gelingt es ihnen, umfassendere Nutzerprofile mit einer Vielzahl von Informationen zu erstellen, von Google-Suchanfragen über Mobiltelefon-Metadaten bis hin zu Transaktionsdaten, Kreditwürdigkeitsinformationen und vielem mehr. Dies ermöglicht es, diese Profile auf eine Weise zu nutzen die wir uns als Nutzer kaum vorstellen können, sei es, dass sie direkt von PayPal verwendet oder an Datenbroker oder andere Unternehmen verkauft werden. Dies ist der beunruhigende Teil und sollte uns dazu veranlassen, uns zu fragen, warum PayPal all diese Informationen über uns benötigt und wie sie diese verwenden, möglicherweise ohne uns darüber zu informieren.

3.6.2 Proxy Diskriminierung

Es gibt Gesetze, die die Verwendung von Informationen über die Zugehörigkeit zu geschützten Gruppen verbieten (Prince & Schwarcz, 2020). Jede Person ist vor Diskriminierung aus Gründen der nationalen Herkunft, des Geschlechts, einer Behinderung, der Religion, des Glaubens oder der Weltanschauung, des Alters oder der sexuellen Orientierung geschützt¹³. Ziel ist es, Menschen vor sozial benachteiligten und ungerechten Ergebnissen basierend auf Gruppenzugehörigkeit zu schützen (Prince & Schwarcz, 2020). Wenn man jedoch eine Vorhersage über das Verhalten eines Mitglieds einer geschützten Gruppe treffen möchte, kann eine nicht geschützte Variable die hoch mit der geschützten Klasse korreliert, ein sogenannter "Proxy", verwendet werden, um eine solche Vorhersage zu treffen (Prince & Schwarcz, 2020). Die nächstbeste Information wird verwendet, um eine solide Vorhersage zu erhalten. Dies wird als "absichtliche Proxy-Diskriminierung" bezeichnet, da die Korrelation zwischen der geschützten Klasse und einer anderen Variablen wissentlich genutzt wird (Prince & Schwarcz, 2020).

Proxy Diskriminierung kann auch unbeabsichtigt erfolgen, da sie dazu beitragen kann ein Ziel zu erreichen. Diskriminierung kann dann ein unbeabsichtigtes Nebenprodukt sein, das auf eine Korrelation zwischen einer geschützten und einer nicht geschützten Variablen zurückzuführen ist (Behrendt & Loh, 2022). Programmierer*innen und Ingenieur*innen konzentrieren sich oft nur auf den Erfolg und die Vorhersagekraft einer KI und berücksichtigen nicht die "Black Box", d. h. die Algorithmen, die die KI anwendet, um eine Vorhersage zu treffen (Prince & Schwarcz, 2020). Das Zurückgreifen auf Proxys führt zur Verwendung von Gruppenmerkmalen, was wiederum auf Stereotypisierung hinausläuft, da Personen mit dem allgemeinen Merkmal einer geschützten Klasse in Verbindung gebracht werden (Prince & Schwarcz, 2020). Bereits benachteiligte und schutzbedürftige Gruppen können zur Zielscheibe einer verstärkten Ausbeutung werden, indem ihnen Kredite mit erhöhten Zinssätzen angeboten werden. Dies führt zu einer gefährlichen Rückkopplungsschleife, die die finanziellen Bedingungen dieser Gruppen verschlechtert und schließlich die finanzielle und soziale Kluft zwischen Arm und Reich vergrößert (Favaretto, De Clercq, & Elger, 2019).

Unsere Gesellschaft produziert jeden Tag eine große Menge an Daten, und diese Daten enthalten noch immer die historische Voreingenommenheit gegenüber geschützten Klassen wie nationale Herkunft und Geschlecht und werden weiterverwendet, um Algorithmen für Vorhersagen zu trainieren (D'Alessandro, O'Neil, & Lagatta, 2017). Die Hinterlassenschaften historischer Diskriminierung werden verstärkt, weil sie für genaue Vorhersagen von Vorteil sind, die zu höheren Gewinnen von Unternehmen führen (Prince & Schwarcz, 2020). Dies führt zu einer Über- oder Unterrepräsentation in den Trainingsdaten, die zum Trainieren eines Algorithmus verwendet werden, was zu einer Aufrechterhaltung der Diskriminierung führt (Barocas & Selbst, 2018; D'Alessandro et al., 2017). Die Umkehrung dieser Diskriminierung kann für diejenigen, die am meisten davon profitieren, kostspielig und nachteilig sein (Prince & Schwarcz, 2020). Dies zeigt, dass die Proxy Diskriminierung

¹³ <https://www.antidiskriminierungsstelle.de/EN/homepage/homepage-node.html>

durch KI normativ schädlich ist, weil sie Menschen aus geschützten Klassen diskriminiert, die durch Antidiskriminierungsgesetze geschützt werden sollen (Prince & Schwarcz, 2020).

Den Zugang zu Proxy-Informationen zu verweigern ist jedoch keine Lösung, da der Algorithmus wieder die nächstbeste Information nutzen wird, die als Proxy für die Klassendiskriminierung dient, um eine Vorhersage zu bestimmen (Gillis & Spiess, 2019; Prince & Schwarcz, 2020). Um Verzerrungen in den Trainingsdaten und Algorithmen zu berücksichtigen, müssen sensible und geschützte Daten über z.B. Herkunft oder Geschlecht gesammelt und im Modellierungsprozess verwendet werden, um die Verzerrungen zu korrigieren und Diskriminierung zu verhindern (Žliobaitė & Custers, 2016). Um Diskriminierung durch KI zu verhindern, muss sie aufgespürt und benannt werden (Gillis & Spiess, 2019).

3.7 Beispiel - Kreditwürdigkeitsprüfung

Die Kreditwürdigkeitsprüfung ist ein Beispiel dafür, wie das Sammeln von Daten in großem Umfang zu unfairen und diskriminierenden Ergebnissen führen kann, da sie auf Proxy Diskriminierung und prädiktiver Analytik beruht. Die Kreditwürdigkeitsprüfung kann sich drastisch auf das Leben von Personen auswirken, ohne dass ein direkter und offensichtlicher Zusammenhang mit dem persönlichen Online-Fußabdruck besteht¹⁴. Oft werden bei der Kreditwürdigkeitsprüfung große Datenmengen einer Person analysiert, um dieser Person die Aufnahme eines Kredits, die Eröffnung eines Bankkontos, die Zahlung von Raten usw. zu ermöglichen. Betroffene Personen sind sich jedoch nicht unbedingt der Aktivitäten bewusst, die im Hintergrund ablaufen, und erfahren es vielleicht nicht einmal.

KI-gestützte Kreditwürdigkeitsprüfung

Die Privatsphäre und der Schutz der Verbraucher stehen im Mittelpunkt einer effizienten Datenerfassung¹⁵. Die persönlichen Informationen der Verbraucher sind einem hohen Risiko ausgesetzt, missbraucht zu werden. Die KI-basierte Kreditwürdigkeitsprüfung auf der Grundlage von Smartphone-Metadaten bietet eine für beide Seiten vorteilhafte Lösung, sowohl für die Verbraucher als auch für die Institute.

KI-Systeme werden eingesetzt, um Metadaten in Kreditbewertungen umzuwandeln. Metadaten sind Daten über andere Daten, die nicht personenbezogene, binäre (1 und 0) Version der gleichen Daten. Bei der KI-basierten Kreditwürdigkeitsprüfung werden Smartphone-Metadaten ausgewertet, um prädiktive Muster zu erkennen, und aus solchen alternativen Daten können zuverlässige Kreditwürdigkeitsprüfungen erstellt werden. Wenn Modelle zur Berechnung der Kreditwürdigkeit einer Person verwendet werden, greifen sie auf Proxys zurück. Die Personen werden in Kategorien von anderen Personen eingeordnet, die sich in der Vergangenheit ähnlich verhalten haben. Das Problem dabei ist, dass die Frage, die das Modell beantwortet, sich nicht darauf bezieht, wie *ich* mich in der Vergangenheit verhalten habe, sondern darauf, wie sich *andere wie ich* verhalten haben. Dies führt zur Stereotypisierung, zur Missachtung des Einzelnen und schließlich zur Diskriminierung. Wenn eine Person in eine Kategorie mit anderen Personen eingeteilt wird, die sich in der Vergangenheit ähnlich wie ich verhalten haben, aber einen Kredit nicht zurückgezahlt haben, muss die Person höhere Zinsen zahlen. Das Modell prüft nicht, ob die eine Person tatsächlich kreditwürdig ist. Diese Person hat dadurch schlechtere Chancen und Bedingungen, da sie sich ähnlich verhält wie kreditunwürdige Personen. Auch wenn die Verwendung von Proxys bei der automatisierten Entscheidungsfindung unethisch ist und zu Diskriminierung führt, helfen sie doch bei der Erstellung genauer Vorhersagen, was wiederum zu höheren Einnahmen und Sicherheit für Unternehmen führt.

¹⁴ Credit Scoring: Keeping Customer Privacy at the Forefront, Michele Tucci

¹⁵ How safe is customer data? <https://www.credolab.com/news-press/credit-scoring-keeping-customer-privacy-at-the-forefront>

Das Problem ist jedoch, dass es keine Möglichkeit gibt, dem System eine Rückmeldung zu geben, ob eine Entscheidung richtig war oder nicht. Solche Kreditscoring-Modelle sind Black Boxes, es ist fast unmöglich herauszufinden, warum ein System die Entscheidung getroffen hat und welche Variablen verwendet wurden. Menschen, die keinen Kredit oder einen Kredit mit höheren Zinsen erhalten, haben keine Möglichkeit herauszufinden, warum das so ist, und keine Chance, sich zu beschweren. Daher verschärft sich der Kreislauf aus Diskriminierung, ungleichen Chancen und der Kluft zwischen Arm und Reich (O'Neill, 2017).

Die Verwendung von Smartphone-Metadaten ermöglicht auch Echtzeitanalysen. Ein Kreditscore wird innerhalb von Sekunden nach dem Zugriff auf die Metadaten des Telefons erstellt. Infolgedessen können KI und maschinelles Lernen eine schnellere Bearbeitungszeit und in einigen Fällen eine sofortige Ablehnung oder Genehmigung ermöglichen. Kreditwürdigkeitsprüfungen werden auch manchmal bei Einstellungsprozessen verwendet. Menschen mit einer schlechteren Kreditwürdigkeit haben weniger Chancen auf einen Arbeitsplatz, was es wiederum erschwert aus dem Kreislauf der Armut zu entkommen. Eine gute Kreditwürdigkeit ist nicht nur ein Indikator für Verantwortung und kluge Entscheidungen, sondern auch für Wohlstand, der wiederum stark mit der nationalen Herkunft korreliert (O'Neill, 2017).

Positive und negative Nutzung von Daten für die Kreditwürdigkeitsprüfung

Die Verfügbarkeit von Big Data-Quellen schafft neue Möglichkeiten und Herausforderungen für die Kreditwürdigkeitsprüfung¹⁶. Diese Quellen können nützlich sein, um Kunden zu bewerten, denen es an Erfahrung bei der Kreditaufnahme mangelt (weil es z.B. ihr erster Kredit ist oder sie vor kurzem in ein neues Land gezogen sind) und die nach herkömmlichen Kreditbewertungsmodellen, die sich auf historische Informationen stützen, automatisch als riskant eingestuft würden. Die Nutzung dieser Datenquellen bringt auch Herausforderungen mit sich. Die erste betrifft den Datenschutz. Es ist wichtig, dass die Kunden angemessen darüber informiert werden, welche Daten zur Berechnung ihrer Kreditwürdigkeit verwendet werden. Es sollte immer eine Opt-out-Option vorgesehen werden.

Darüber hinaus kann die Verwendung von Daten aus sozialen Netzwerken für die Kreditwürdigkeitsprüfung ein neues Betrugsverhalten auslösen, bei dem Kunden ihr soziales Netzwerk strategisch aufbauen, um ihre Kreditwürdigkeit gezielt und böswillig zu verbessern. Schließlich könnte auch die Einhaltung von Vorschriften ein wichtiges Thema werden. In vielen Ländern ist die Verwendung von Geschlecht, Alter, Familienstand, nationaler Herkunft, ethnischer Zugehörigkeit und Glaubensrichtungen für die Kreditwürdigkeitsprüfung verboten. Da viele dieser Informationen leicht aus sozialen Netzwerken ausgelesen werden können, kann es schwieriger sein, die Einhaltung von Vorschriften zu überwachen, wenn soziale Netzwerke oder andere Daten für die Kreditwürdigkeitsprüfung verwendet werden.

¹⁶ Bart Baesens BDQ (Big Data Quarterly): Big Data for Credit Scoring: Opportunities and Challenges; <https://www.dbta.com/BigDataQuarterly/Articles/Big-Data-for-Credit-Scoring-Opportunities-and-Challenges-109999.aspx>

4 Kollektive Verantwortung – The *Big Picture*

Was bedeutet es, verantwortlich zu sein? Das hängt stark vom jeweiligen Kontext ab. Es kann folgendes bedeuten:

1. Eine Qualität des moralischen Charakters
2. Die Verantwortung, in einer bestimmten Eigenschaft zu handeln - *ex ante*
3. Ein Akteur zu sein, dem die Handlung oder ihre Folgen zugeschrieben werden können - *ex post*

In großen Unternehmen wie PayPal ist es ziemlich einfach, mit Schuld zu jonglieren wenn etwas schief geht, was wiederum dazu führt, dass die Entscheidungsfindung in großen Unternehmen katastrophal sein kann. Ohne eine angemessene Gesetzgebung gibt es nichts, was die Unternehmen ethisch auf Linie hält. Die Kund*innen müssen über alle potenziellen Risiken ihrer Handlungen informiert werden und wissen, worauf sie sich einlassen.

- Manche Menschen werden sich trotzdem dafür entscheiden, weniger sichere Systeme zu verwenden (selbst wenn sie alle Risiken kennen).
- Manche Menschen werden, wenn sie die Möglichkeit haben, sich zu informieren und zu entscheiden, kein Risiko einzugehen, und stattdessen sogar bereit sein, Geld (oder Datenwährung) zu verlieren.

Alle Personen sind ein Teil des Endprodukts bei diesen Unternehmen. Die Mitarbeiter*innen von großen Unternehmen wie PayPal sind Teil eines Kollektivs. Als Kollektiv haben sie die folgenden wichtigen Komponenten der Verantwortung:

- Kontrolle (über das Ergebnis)
- Wissen (Bewusstsein für die Konsequenzen)
- Verantwortlichkeit (ex-post für Fragen, Lob und Tadel zur Verfügung stehen und ex-ante für die Zukunft verantwortlich sein)

In Fällen, in denen es um Big Data geht, sind auch Nutzer*innen in diesen "Verantwortungsstrudel" verwickelt, da Nutzer*innen andere Nutzer*innen oder sogar Nichtnutzer*innen über Freundeslisten, Kontaktlisten usw. in den sozialen Medien oder nicht zuletzt durch die Einspeisung von Daten in prädiktive Algorithmen, die anschließend zur Vorhersage von Verhaltensmustern größerer Bevölkerungsgruppen verwendet werden können, bloßstellen könnte. Die Gefahr der Preisgabe von Daten, die Dritten gehören - durch die blinde Annahme von Geschäftsbedingungen oder Cookies - und des anschließenden Zugriffs auf die Daten unserer Freunde auf Facebook kann zu beängstigenden Situationen führen, wie wir bereits in der Vergangenheit gesehen haben (z.B. *Cambridge Analytica*). Daher ist die Verantwortung ein wichtiges Thema für Nutzer*innen und Unternehmen.

5 Literaturnachweise

- Barocas, S., & Selbst, A. D. (2018). Big Data's Disparate Impact. *SSRN Electronic Journal*.
<https://doi.org/10.2139/ssrn.2477899>
- Behrendt, H., & Loh, W. (2022). Informed consent and algorithmic discrimination—is giving away your data the new vulnerable? *Review of Social Economy*, 80(1). <https://doi.org/10.1080/00346764.2022.2027506>
- Björnsson, Gunnar. (2019). Collective responsibility and collective obligations without collective moral agents.
- Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns. Proc. Priv. Enhancing Technol.*, 2016(4), 237-254.
- D'Alessandro, B., O'Neil, C., & Lagatta, T. (2017). Conscientious Classification: A Data Scientist's Guide to Discrimination-Aware Classification. *Big Data*, 5(2). <https://doi.org/10.1089/big.2016.0048>
- Eckersley, P. (2010). How unique is your web browser? In Proceedings of the 10th international conference on Privacy enhancing technologies (PETS'10). *Springer-Verlag, Berlin, Heidelberg*, 1–18.
- Favaretto, M., De Clercq, E., & Elger, B. S. (2019). Big Data and discrimination: perils, promises and solutions. A systematic review. *Journal of Big Data*, 6(1). <https://doi.org/10.1186/s40537-019-0177-4>
- Gillis, T. B., & Spiess, J. L. (2019). Big Data and Discrimination. *The University of Chicago Law Review*, 86(2), 459–488.
- Hoepman, J. H. (2014). Privacy design strategies. In IFIP International Information Security Conference (pp. 446-459). *Springer, Berlin, Heidelberg*.
- Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review*.
- Kumar, S., Sharma, P., & Madhusudan (2016). Predictive Analytics: Cloud Computing
- Mishra, N., & Silakrai, S. (2012). Predictive Analytics: A Survey, Trends, Applications, Opportunities & Challenges
- Mühlhoff, R. (2022). Predictive Analytics: Prädiktive Privatheit: Kollektiver Datenschutz im Kontext von Big Data und KI
- Narayanan, A., Mathur, A., Chetty, M., Kshirsagar, M. 2020. Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces. *Queue* 18, 2, Pages 10 (March-April 2020), 26 pages.
<https://doi.org/10.1145/3400899.3400901>
- O'Neil, C. (2017). *Weapons of math destruction*. Penguin Books.

- Ongsulee, P., Chotchaung, V., Bamrunsi, E. & Rodcheewit, T. (2018). "Big Data, Predictive Analytics and Machine Learning," *16th International Conference on ICT and Knowledge Engineering*
- Preibusch, S., Peetz, T., Acar, G., & Berendt, B. (2016). Shopping for privacy: Purchase details leaked to PayPal. *Electronic Commerce Research and Applications*, 15, 52–64.
<https://doi.org/10.1016/j.elerap.2015.11.004>
- Prince, A. E. R., & Schwarcz, D. (2020). Proxy discrimination in the age of artificial intelligence and big data. *Iowa Law Review*.
- Sfetcu, N. Big Data Ethics. *Www.academia.edu*. Retrieved September 1st, 2022, from https://www.academia.edu/42114775/Big_Data_Ethics
- Sfetcu, N. Philosophical Essays. In *www.scribd.com*. Retrieved September 18th, 2022, from <https://www.scribd.com/book/567537100/Philosophical-Essays>
- Squires, G. D. (2003). Racial profiling, insurance style: Insurance redlining and the uneven development of metropolitan areas. *Journal of Urban Affairs*, 25(4). <https://doi.org/10.1111/1467-9906.t01-1-00168>
- Žliobaitė, I., & Custers, B. (2016). Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models. *Artificial Intelligence and Law*, 24(2). <https://doi.org/10.1007/s10506-016-9182-5>

6 Anhang

Dies ist eine Liste nützlicher Links und Websites, die wir häufig besucht haben, um allgemeine Informationen zu einer Vielzahl verwandter Themen zu erhalten.

- **Was bedeutet "Datenminimierung" nach EU-Datenschutzrecht?**
<https://medium.com/golden-data/what-is-data-minimization-under-eu-data-protection-law-b0e30fbb856e>)
- **Visualisierung der Länge des Kleingedruckten für 14 beliebte Apps**
<https://www.visualcapitalist.com/terms-of-service-visualizing-the-length-of-internet-agreements/>
- **PayPal-Website**
<https://www.paypal.com/de/home>
- **PayPals YouTube-Kanal:** Ihr YouTube-Kanal soll allen Nutzer*innen (Privatkund*innen, Unternehmen etc.) helfen. Es werden noch einmal alle Vorteile und Funktionen unabhängig von jeglichen Datenschutzfragen/-informationen erwähnt.
<https://www.youtube.com/user/paypalde>
- **Werbespot für Unternehmen:** Der Werbespot richtet sich an Geschäfte/Unternehmen und den intensiven Wettbewerb.
<https://www.youtube.com/watch?v=XqNxLf2XiGg>
- **Privatkunden Werbung:** Die Spots richten sich an Privatkund*innen und zeigen alle Funktionalitäten, Vorteile und neuen Implementierungen von PayPal.
<https://www.youtube.com/watch?v=HFWkRfnb7OA>
<https://www.youtube.com/watch?v=0nnRRe2rPnI>
- Die Widerstandsfähigkeit gegenüber Dark Patterns sollte erhöht werden, indem man mehr über die **Funktionsweise von Privacy Dark Patterns** erfährt (Bösch et al. 2016). Hierfür sind Webseiten wie <https://www.deceptive.design/> sehr zu empfehlen.
- **PayPal, Inc. 2013. Express Checkout User Interface Standards:**
https://www.paypalobjects.com/webstatic/en_US/developer/docs/pdf/pp_ecplacement_guide.pdf
- **Informationen darüber, wie PayPal die großen Datenmengen verwaltet, die es von Nutzer*innen sammelt:**
<https://www.projectpro.io/article/big-data-use-cases-how-paypal-leverages-big-data-analytics/231>

- Abbildung 1 fasst die von Hoepman (2014) definierten **Datenschutzstrategien** zusammen und stellt sie anschließend den abgeleiteten **Dark-Strategien** gegenüber.

Privacy Strategies		Privacy Dark Strategies			
Description	Name	Name	Description	Pattern/Example	Countermeasures
process minimal amount of personal data, just what is needed	Minimize	Maximize	collect, store and process more data than actually needed	Forced Registration = Makes functionalities only available after registration with (often) unnecessary personal data (e.g. birthdates...)	create new account with random data (anonymous one-time-mail address); service BugMeNot = bypassing registrations using an existing account
hide processed personal data from plain view	Hide	Publish	publish personal data don't use mechanisms for authorized access	-	-
process personal data in distributed way to vanish interrelationships	Seperate	Centralize	collect, store and process personal data at a central entity --> make links between users visible	Shadow User Profiles (fits also: Maximize, Perserve) = Collects and keeps records of people that not use the service. Actual users (intentionally) providing personal data enrich the improvement of predictive analytics.	-
process personal data at high level of aggregation , vanish unnecessary data	Aggregate	Perserve	doesn't affect interrelationships between the data sets	Adress Book Leeching (fits also: Maximize) = Imports and stores list, compares it with it's database and suggests connections.	avoid features in which it's unclear how they process the contact lists and deny access unless it's required or in your own interest
inform users whenever personal data is collected and processed	Inform	Obscure	make it hard to get to know if data is collected and processed	Privacy Zuckering = Allows users to adjust the privacy settings which are (intentionally) unnecessary complex and incomprehensive . Often combined with "bad defaults" pattern.	require help of third parties to clarify and get guidance through the preferences
let users have control of the data processing (Hoepman is not aware of any patterns implementing this)	Control	Deny	subjects are denied to control their data and lose control of their data	Immortal Accounts (fits also: obscure) = Requires registration but prevents users from deleting their accounts and their data -> make it unnecessarily complicated or don't provide the option of deletion.	online resources (just-delete.me or accountkiller.com) provide step by step tutorials; use throwaway account with incorrect data
privacy policy compatible with legal requirements should be established and followed	Enforce	Violate	presented privacy polic is violated on intention	-	-
be able to demonstrate usage and compliance of privacy policy and legal requirements	Demonstrate	Fake	pretend to implement strong privacy protection	-	-

Abbildung 1: Vergleich der Datenschutzstrategien von Hoepman (2014) und der nachgebauten Dark Privacy Strategies von Bösch et al. (2016). (Tabelle in Anlehnung an bestehende Tabelle von Bösch et al. (2016))

- In Abbildung 2 ordnet Hoepman (2014) seine Strategien rechtlichen Grundsätzen zu, die mit den (damals) bestehenden Datenschutzgesetzen übereinstimmen.

	Purpose limitation	Data minimisation	Data quality	Transparency	Data subject rights	The right to be forgotten	Adequate protection	Data portability	Data breach notification	(Provable) Compliance
MINIMISE	o	+								
HIDE		+					o			
SEPARATE	o						o			
AGGREGATE	o	+								
INFORM				+	+				+	
CONTROL			o		+			+		
ENFORCE	+	+				+	+			o
DEMONSTRATE										+

Legend: +: covers principle to a large extent. o: covers principle to some extent.

Abbildung 2: Die acht Strategien zum Schutz der Privatsphäre, die den bestehenden Rechtsgrundsätzen zugeordnet sind, nach Hoepman (2014), S. 457.

- In Abbildung 3 stellt Hoepman (2014) seine Datenschutzstrategien in einem Datenbankschema dar, um ihr Zusammenspiel zu visualisieren.

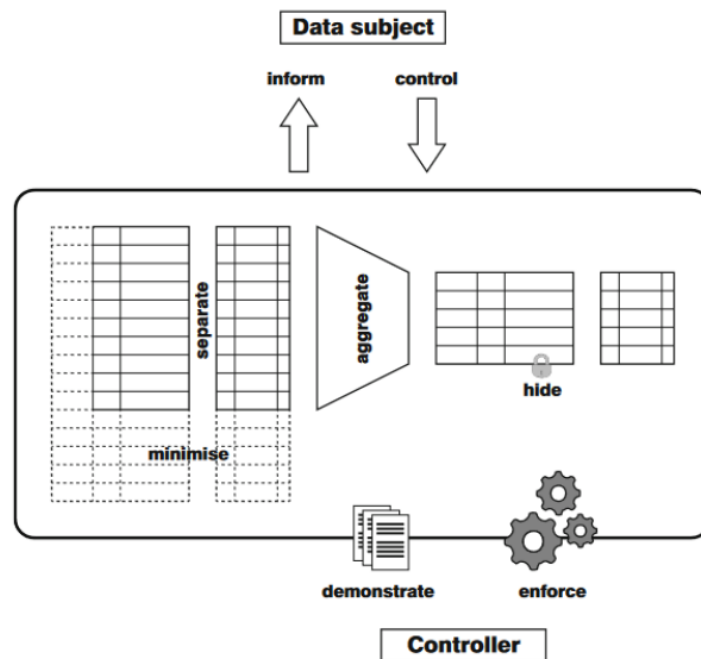


Abbildung 3: Schema der acht Datenschutzstrategien nach Hoepman (2014), S. 457.