Dark Patterns

Natalie Tork Alinaghipour

Praxisprojekt Wintersemester 2020/2021

Betreuer: Prof. Gerhard Hartmann

19. November 2020

Zusammenfassung

Inhaltsverzeichnis

1 Einleitung

1.1 Problemfeld und Kontext

Bei der Gestaltung von digitalen Systemen spielt die User Experience (UX) eine wichtige Rolle für Online-Marketing und -Vertrieb, da sie maßgeblich zum Erfolg eines Unternehmens beiträgt. UX Design basiert unter anderem auf psychologischen und verhaltensökonomischen Erkenntnissen und hat langfristig zum Ziel, die Erfahrung des Nutzers während der Interaktion eines Produkts zu verbessern. Allerdings können diese Methoden auch dazu missbraucht werden, die menschliche Wahrnehmung und Verhaltensweisen zu beeinflussen, um wirtschaftlich davon zu profitieren. Nutzer können so zu nicht intendierten Taten verleitet und infolgedessen benachteiligen werden. Dies zu bemerken ist für viele schwierig, da der Zweck nicht transparent gemacht wird. Diese Taktiken werden als "Dark Patterns"bezeichnet und werden bereits ethisch erforscht. Heutzutage findet diese Art von manipulativem Design in vielen verschiedenen Bereichen Anwendung, wie in Desktop-, Web- oder Mobilen Applikationen, sowie in Games, Proxemischer Interaktion[1] und Künstlicher Intelligenz.

1.2 Ist-Zustand

Der Begriff *Dark Patterns* wurde von dem UX-Experten Harry Brignull geprägt, als er im Jahr 2010 einen Blog-Beitrag veröffentlichte [1] und kurze Zeit später einen Vortrag auf der UX Brighton Conference hielt. Inzwischen wurden bereits einige Paper über das Thema verfasst, die verschiedene Nutzungskontexte beschreiben. Da demnach viele unterschiedliche Technologien Dark Patterns enthalten, ist der Themenbereich recht unübersichtlich und komplex, wodurch eine ausführliche Recherche notwendig ist.

1.3 Ziel und Lösungsansatz

Das Ziel soll es sein, eine Übersicht in das Themenkomplex Dark Patterns zu bringen, indem diese nach Systemen strukturiert werden. Es soll analysiert werden, welche Dark Patterns zu den jeweiligen Nutzungskontexten existieren und welche versteckten Geschäftsmodelle dahinterstecken. Ebenso gilt es herauszufinden, welche Zielgruppe von diesen Methoden betroffen sind und wer die Stakeholder sind.

1.4 Motivation

Das Thema hat eine hohe gesellschaftliche Relevanz, da heutzutage das Internet für die meisten Menschen in das Leben integriert ist. Alltägliche Aufgaben können dadurch einfacher und schneller bewältigt werden. Jedoch kann die Tatsache, dass viele auf eine gute Usability angewiesen sind, ausgenutzt werden und demnach stellt dies ein mögliches Risiko dar. Zudem hat die Datenschutz-Grundverordnung dazu geführt, dass die Bedingungen der Nutzung bestimmter Dienste zu umfangreich und zu kompliziert formuliert sind, sodass das Lesen

[1] Proxemische Interaktion bedeutet die Verbundenheit und Kommunikation zwischen Geräten und zwischen Mensch und Maschine, sobald diese sich in unmittelbarer Nähe zueinander befinden

unnötig erschwert oder gar unmöglich gemacht wird. Dies hat zur Folge, dass Nutzer wegen Zeit- und Alternativenmangel diesen Bedingungen zustimmen, ohne diese vollständig zu lesen. Aus den oben genannten Gründen weist das Thema auch eine hohe politische Relevanz auf, da es von großer Notwendigkeit ist, Verbraucher:innen durch sinnvolle Maßnahmen vor alldem zu schützen und sie auf Dark Patterns aufmerksam zu machen.

2 Hintergrund

2.1 Über Dark Patterns

2.2 Versteckte Geschäftsmodelle

2.2.1 Stakeholder

2.3 Zielgruppen der Dark Patterns

2.4 Allgemeine Dark Patterns Kategorien nach Gray

Der Ausdruck Dark Patterns stammt von Harry Brignull, der sich noch heute aktiv gegen diese Methoden in digitalen Produkten einsetzt und als Sachverständiger in dem Bereich agiert. Zudem führt er zusammen mit Alexander Darlington[2] die Webseite darkpatterns.org, auf der Brignull die von ihm definierte Taxonomie von Dark Patterns beschreibt, und macht auf dem dazugehörigen Twitter-Account öffentlich auf das Thema aufmerksam [2][3]. Brignull's 12 Typen von Dark Patterns werden von Gray et al. in Kategorien eingeteilt, die die Strategien und Motivation dahinter zusammenfasst [4]. Im Folgenden wird erläutert, was unter den einzelnen Kategorien zu verstehen ist und wie die Taxonomie von Brignull in diese einzuordnen ist. Diese Praktiken finden allgemein in der Gestaltung von digtalen Benutzeroberflächen Anwendung.

2.4.1 Nagging

Während der Interaktion mit dem System wird der Nutzer ein- oder mehrmals entgegen seiner Erwartung umgeleitet und bei der Aufgabenerledigung unterbrochen. Dabei hat die Unterbrechung für den Nutzer keine Relevanz. Diese treten meist in den folgenden Formen auf:

1) Pop-Ups, die den Zugriff auf das Interface sperren,
2) Audionotizen, die zur Ablenkung führen,
3) andere Formen von Aktionen, die den Nutzer von der Erledigung seiner Aufgaben ablenken.

2.4.2 Obstruction

Die Erledigung der Aufgaben wird so erschwert, dass der Nutzer davon abgebracht wird. Ein mögliches Vorkommnis ist, dass der Nutzer in dem Moment,

[2] Alexander Darlington ist im Bereich UX Research bei Aviva in Großbritannien tätig und betreibt Forschung in Ethischem Design.

wo er auf die Barriere stößt, über die Beschränkung der nutzbaren Funktionen benachrichtigt wird. Der Nutzer muss diese Funktionen also erst freischalten.

2.4.2.1 Roach Motel (Brignull)

Führt den Nutzer auf einen langen Pfad und ruft gleichzeitig eine Disorientierung durch unklare Formulierungen hervor. Der Nutzer gerät hier leicht in eine Situation und kommt nur schwer aus dieser Lage heraus. Dies geschieht beim Abonnieren eines Services oder der Registrierung bei einem Service, indem es dem Nutzer schwer oder sogar unmöglich gemacht wird, diesen Service wieder abzubestellen oder das Konto zu löschen.

2.4.2.2 Price Comparison Prevention (Brignull)

Hindert den Nutzer daran, Preise von Produkten und Dienstleistungen zu vergleichen. Dies kann zum Beispiel der Fall sein, wenn es dem Nutzer nicht möglich ist, Produktinformationen zu kopieren, um damit Suchanfragen stellen zu können.

2.4.2.3 Intermediate Currency (Gray et al.)

Der Nutzer wird gezwungen, echtes Geld in eine virtuelle Währung zu investieren, damit er Käufe tätigen kann. Oft kommt dies in Apps vor, die In-App Käufe anbieten.

2.4.3 Sneaking

Relevante Informationen werden vor dem Nutzer versteckt oder verschleiert, oder die Anzeige der Information wird verzögert. Ziel ist es, den Nutzer dazu zu führen, eine Aktion auszuführen, die in der Regel nicht in seinem Interesse ist, wenn er Kenntnis davon hätte. Dazu zählen versteckte Kosten oder unerwünschte Effekte durch die Ausführung einer bestimmten Aktion.

2.4.3.1 Forced Continuity (Brignull)

Wenn ein Nutzer eine Frist versäumt, soll dies ausgenutzt werden. Oft wird der Nutzer hier zur Kasse gebeten werden, wenn ein Service automatisch erneuert wird, weil dieser nicht rechtzeitig vor Ablauf einer Probezeit gekündigt wurde.

2.4.3.2 Hidden Costs (Brignull)

Versteckte Kosten werden erst später offenbart, nachdem ein potentieller Kunde mit einem besonderen Angebot angelockt wurde. Wird dieser beispielsweise kurz vor dem Abschluss eines Bestellvorgangs darauf hingewiesen, dass das Angebot zeitlich begrenzt ist oder diverse Gebühren, Steuern oder hohe Liefergebühren anfallen, so kann das auf dieses Dark Pattern hinweisen.

2.4.3.3 Sneak into Basket (Brignull)

Dem Nutzer wird ohne sein Wissen automatisch ein Artikel in den Warenkorb gelegt, was unbemerkt bleiben kann, wenn der Nutzer seine Einkaufsliste vor der Bestellung nicht überprüft. Oft basieren solche Artikel angeblich auf einer Empfehlung für den Kunden.

2.4.3.4 Bait and Switch (Brignull)

Gewohnte Interaktionselemente einer Applikation führen zu einem unerwarteten und unerwünschten Ergebnis. Für Aufsehen sorgte beispielsweise Microsoft im Jahr 2016, als Nutzer von älteren Windows-Versionen dazu gedrängt wurden, das Betriebssystem auf Windows 10 zu aktualisieren [5]. Ein Schließen der Meldung durch den entsprechenden Button führte zwar zum Schließen des Fensters, allerdings war den Nutzern nicht bewusst, dass sie dabei gegen ein Upgrade auf Windows 10 keinen Widerspruch eingelegt haben. Daraufhin wurde bei diesen Nutzern zu einem von Windows festgelegten Zeitpunkt das Upgrade durchgeführt.

2.4.4 Interface Interference

Sobald bestimmte Aktionen, die überdeckt werden von anderen Aktionen, den Nutzer bei der Erledigung seiner Aufgaben stören oder die Sichtbarkeit von Aktionen oder Informationen beschränken, spricht man von Interface Interference. Gray [4] unterscheidet dabei zwischen *Hidden Information*, *Preselection* und *Aesthetic Manipulation*.

2.4.4.1 Hidden Information

Sorgt dafür, dass wichtige Informationen nur schwer auffindbar und lesbar sind. Demnach bekommt der Nutzer das Gefühl vermittelt, als seien die Informationen für ihn nicht von Bedeutung. Oft sind diese dargestellt als Optionen oder als Kleingedrucktes, verblasster Text oder in Form von schwer verständlichen Geschäfts-bedingungen.

2.4.4.2 Preselection

Eine Option in einem Dialog ist von Anfang an ausgewählt, noch bevor der Nutzer eine eigene Auswahl getroffen hat. Meistens entspricht die Auswahl nicht dem Interesse oder der Absicht des Nutzers, sofern er keine Anpassungen vornimmt. Oft geht er in dem Fall dennoch davon aus, dass die Vorauswahl im besten Interesse des Nutzers ist.

2.4.4.3 Aesthetic Manipulation (Gray et al.)

Die Form der Benutzeroberfläche wird so gestaltet, dass die Aufmerksamkeit des Nutzers auf etwas anderes gelenkt oder dass er von etwas anderem überzeugt wird. Brignull hat dieses Dark Pattern als „Misdirection“ bezeichnet. Darunter fallen die Dark Patterns *Toying with Emotions*, *False Hierarchy*, *Disguised Ad* und *Trick Question*.

Toying with Emotions (Gray et al.) setzt Elemente wie Farben, Sprache oder Schreibstil gezielt dafür ein, Emotionen hervorzurufen, um den Nutzer dazu zu bringen, eine bestimmte Aktion auszuführen. Hier kommen unter anderem niedliche zu viel oder XD oder furchteinflößende Bilder, oder verlockende oder Angst machende Formulierungen zum Einsatz. Zum Beispiel kann es sich bei einem Angebot einer zeitnahen Lieferung nur um eine zeitlich begrenzte Garantie handeln, was den Nutzer unter Druck setzen kann, seinen Einkauf zügig

abzuschließen. Nachforschungen von Gray zeigen allerdings, dass der Timer oft neugestartet wird, nachdem die Zeit um ist.

False Hierarchy (Gray et al.) erschwert dem Nutzer während eines Dialogs die Interaktion mit bestimmten Optionen oder bestimmte Optionen werden visuell anders dargestellt und vom Nutzer kaum wahrgenommen. So kann der Nutzer davon ausgehen, dass seine Auswahlmöglichkeiten beschränkt sind oder dass eine bestimmte Option für den Nutzer die bessere ist. Ein Beispiel hierfür ist die Installation von manchen Desktop-Anwendungen, bei der zu Beginn die Optionen einer (empfohlenen) Express-Installation und einer erweiterten, jedoch ausgegrauten Installation aufgelistet werden.

Disguised Ad (Brignull) versteckt eine Werbung hinter einem Navigationselement oder einem Inhalt, die nicht klar als solche gekennzeichnet ist und den Nutzer anlocken soll. Dies kann ein interaktives Spiel, ein Download-Button oder ein anderes hervorstechendes Interaktionselement sein, die den Nutzer dann auf eine andere Seite umleitet.

Trick Question (Brignull) verwendet eine Frage, die doppelte Negation oder missverständliche Formulierungen enthält. Liest der Nutzer sich die Frage nicht gründlich durch, macht die Frage nur den Anschein, als wäre sie das, was der Nutzer erwartet. Mit diesem Trick wird der Nutzer dazu gebracht, mit seiner Auswahl eine Zustimmung zu geben, die nicht in seinem Interesse ist.

2.4.5 Forced Action

Der Nutzer muss eine Aktion ausführen, um (weiterhin) Zugang zu bestimmten Funktionen zu bekommen. Oft ist dies verbunden mit einem Vorgang, der nur dann abgeschlossen werden kann. Die obligatorische Aktion kann auch verschleiert werden als etwas, von dem der Nutzer angeblich profitieren würde. Als Beispiel gibt Gray et al. [4] Windows 10 an, das den Nutzer zwingt, beim Herunterfahren oder Neustarten des Rechners ein Update durchzuführen.

2.4.5.1 Social Pyramid (Gray et al.)

Ein Service kann erst dann (vollumpfänglich) genutzt werden, wenn der Nutzer andere eingeladen hat. Dies kommt oft bei sozialen Anwendungen oder Online-Games vor.
Brignull's *Friend Spam* steht mit diesem Dark Patterns im Zusammenhang. Hierbei wird der Nutzer nach einer Zugriffsberechtigung für sein E-Mail Konto oder sein Konto auf einem Sozialen Netzwerk gefragt, unter dem Vorwand, ihm einen Vorteil zu verschaffen (wie zum Beispiel das Finden von Freunden zur Erweiterung seines Netzwerks bei diesem Service). Allerdings können die Kontaktdaten missbraucht werden, um im Namen des Nutzers Einladungen zu versenden, ohne dass der Nutzer davon Kenntnis hat. Ein bekannt gewordenes Beispiel dafür war LinkedIn, die eine zeitlang von ebendieser Methode Gebrauch gemacht haben, bis sie im Jahr 2015 ein Gerichtsverfahren verloren und diese Methode daraufhin in Kalifornien als illegal erklärt wurde [6].

2.4.5.2 Privacy Zuckering (Brignull)

Der Nutzer wird dazu gebracht, mehr persönliche Informationen als gewollt oder notwendig preiszugeben. Diese Informationen werden dann oft an Dritte verkauft. Erst bei Durchsehen der Geschäftsbedingungen oder der Datenschutzerklärung wird dies dem Nutzer bewusst.

2.4.5.3 Gamification (Gray et al.)

Der Nutzer wird zur wiederholten Nutzung des Services gezwungen, damit er mit bestimmten Funktionen des Services belohnt wird. Solange kann er den Service nicht im vollen Umfang benutzen.

3 Nutzungskontexte von Dark Patterns

Dark Patterns sind inzwischen gut erforscht, und Forschungsteams aus aller Welt verdeutlichen die Relevanz und Risiken für unterschiedliche Nutzungskontexte. Laut Gray et al. existieren verschiedene Dark Patterns Strategien, auf dessen Basis in einem weiteren Paper über 1.200 Online-Shops gefunden werden konnten, die Dark Patterns enthalten [4][7]. In einer weiteren Studie stellte sich heraus, dass mehr als 95% der beliebtesten Android Applikationen Dark Patterns verwenden und konnten nachweisen, dass diese Methoden tatsächlich in der Lage dazu sind, Nutzerverhalten zu manipulieren [8]. Auch in Games konnten solche Strategien verschiedenen, Game-spezifischen Kategorien zugeordnet werden [9]. Ein weiteres Risiko stellen *Privacy Dark Patterns* dar, durch die Nutzer dazu gebracht werden, ihre persönlichen Daten preiszugeben, damit diese von einem Dienstleister gesammelt, gelagert und verarbeitet werden können, ohne dass eine bewusste Zustimmung gegeben wurde [10].
Doch Dark Patterns beschränken sich nicht nur auf Benutzeroberflächen: auch Künstliche Intelligenz hat das Potential, für solche Zwecke missbraucht zu werden. Dazu wurde der Effekt von „Cute Robots“ auf die Preisgabe von emotionalen Daten der Nutzer analysiert [11]. Für Geräte der Proxemischen Interaktion wurde ebenfalls, teilweise anhand von aktuellen und vergangenen Beispielen, Dark Patterns festgelegt und Prognosen angestellt.
Im Folgenden werden verschiedene Nutzungskontexte aufgeführt, in denen Dark Patterns vorkommen. Zum Teil sind die erläuterten Strategien in den von Gray et al. definierten Kategorien wiederzuerkennen, jedoch konnten einige spezifische Dark Patterns gefunden werden, von der nur einzelne Dienste und Technologien betroffen sind.

3.1 Shopping Websites

Viele wissenschaftliche Arbeiten haben sich mit der Untersuchung von Marktmanipulation beschäftigt und beschreiben, wie Unternehmen die Beschränkungen der menschlichen Wahrnehmung und die kognitive Verzerrung zu deren Vorteil nutzen können [7][12]. Vor allem im digitalen Bereich sind solche Methoden gut anzuwenden, da es heutzutage möglich ist, Daten über Nutzerverhalten zu erfassen und zu analysieren und somit die Methoden auf Effektivität zu prüfen.

Mathur et al. erläutert, wie verbreitet Dark Patterns in Online-Shops sind und

inwiefern diese Methoden Nutzer beeinflussen und ihnen schaden können. Das Team entwickelte ein Tool, das automatisch Dark Patterns in Online-Shops entdeckt und mithilfe dessen konkrete Ergebnisse und Erkenntnisse ermittelt wurden. Bei der Untersuchung von ungefähr 11.000 beliebten Shopping-Webseiten auf Dark Patterns konnte festgestellt werden, dass 1.254 Webseiten (ca. 11,1%) über 1.800 Dark Patterns enthalten, von denen 183 Webseiten betrügerische Nachrichten verwenden.

Nachfolgend werden die von Mathur et al. festgelegten Kategorien kurz erläutert. Einige Typen von Dark Patterns, die in Online-Shops vorkommen, wurden bereits von Gray et al. beschrieben, demnach werden diese hier nicht näher erklärt.

3.1.1 Sneaking

siehe Kapitel 2.4.3

3.1.1.1 Sneak into Basket

siehe gleichnamigen Abschnitt unter Kapitel 2.4.3

3.1.1.2 Hidden Costs

siehe gleichnamigen Abschnitt unter Kapitel 2.4.3

3.1.1.3 Hidden Subscription (Mathur et al.)

fällt unter die Kategorie *Sneaking* und taucht oft in Verbindung mit *Hard to Cancel* auf.
Der Nutzer wird wiederholt zur Kasse gebeten unter dem Vorwand einer einmaligen Gebühr oder einer Probezeit. Dass das Abonnement laufend erneuert wird, fällt dem Nutzer erst nach Empfangen einer Rechnung auf.

3.1.2 Urgency

Beim Versuch einer KonversionKonversion definieren[3] wird der Kunde dazu gedrängt, eine Kaufentscheidung zu treffen, indem eine Deadline auf Sales oder Schnäppchen gesetzt wird.
Kombiniert mit *Social Proof* und *Scarcity* kann dies potentiell einen FOMO-Effekt[4] auslösen.

3.1.2.1 Countdown Timer

zeigt bei einem Angebot einen Timer an, der aussagt, wie viel Zeit noch verbleibt, bis eine Deadline verstrichen ist. *Deceptive Countdown Timer* sollen den Nutzer eine Deadline vortäuschen und werden aktiviert, sobald die Seite besucht wird. Bei einem erneutem Besuch oder Aktualisieren der Seite wird der Timer erneut gestartet.

[3] Konversion ist...
[4] Fear of Missing Out-Effekt

3.1.2.2 Limited-time Messages

erzeugt durch die Angabe eines ablaufenden oder befristeten Angebots Zeitdruck beim Nutzer, ohne eine konkrete Deadline zu nennen.

3.1.3 Misdirection

Definiert wurde dieses Dark Pattern von Brignull und hat Ähnlichkeit mit Gray's *Interface Interference*. Hierbei werden visuelle, sprachliche und emotionale Signale versendet, um den Nutzer zu einer Entscheidung zu bewegen oder von einer Entscheidung abzuhalten. Bestimmte affektive oder kognitive Eigenschaften des Menschen sollen ausgenutzt werden, ohne tatsächlich die Auswahlmöglichkeiten des Nutzers einzuschränken.

3.1.3.1 Confirmshaming

Der Begriff wurde bereits von Brignull beschrieben und erinnert an Gray's *Toying with Emotions*. Mithilfe von Sprache sollen Emotionen im Nutzer geweckt werden, um den Nutzer von einer Entscheidung abzubringen. Meist geschieht das in Form von Pop-up Dialogen, die den Nutzer mit Rabatten anlocken und zur Eingabe der E-Mail Adresse auffordern. Lehnt der Nutzer das Angebot ab, werden absichtlich Scham-Gefühle oder der Framing-Effekt[5] ausgelöst.

3.1.3.2 Visual Interference

Dieses Dark Pattern ist wiederzuerkennen in Gray's *False Hierarchy*. Durch Stil und visuelle Darstellung wird eine Auswahl auffälliger gestaltet als andere Auswahlmöglichkeiten, sodass der Nutzer eher dazu tendiert, eine bestimmte Auswahl zu treffen.

3.1.3.3 Trick Question

Wie bereits in 2.4.4 im Abschnitt *Interface Interference* erläutert, soll der Nutzer mithilfe von verwirrender Sprache dazu bewegt werden, eine bestimmte Entscheidung oder Auswahl zu treffen. Dies soll verhindern, dass er sich von einem Service (z.B. einem Newsletter) abmeldet. Der Nutzer geht davon aus, dass diese Auswahl seinen Präferenzen entspricht, was sowohl auf den Framing-Effekt, als auch auf den Default-Effekt[6] abzielt.

3.1.3.4 Pressured Selling

setzt den Nutzer unter Druck, eine teurere Version eines Produkts (Upselling) oder verwandte Produkte (Cross-Selling) zu kaufen. Nutzt kognitive Verhaltensweisen des Nutzers aus, wie den Default-Effekt, den Anker-Effekt[7] und das Gefühl von Knappheit, um den Kunden zum Kauf zu bewegen.

[5] Framing-Effekt
[6] Default-Effekt
[7] Anker-Effekt

3.1.4 Social Proof

Nutzer orientieren sich an dem Verhalten anderer Nutzer. Dies wird ausgenutzt, um die Entscheidungsfindung und Käufe der Nutzer zu beschleunigen (Bandwagon[8]-Effekt).

3.1.4.1 Activity Notifications

zeigt die Aktivität anderer Nutzer bei einem Artikel an. Folgende Varianten treten dabei (oft in Kombination) auf:

1) Namen von Nutzern, die dieses Produkt ebenfalls gekauft haben,

2) Wie viele Nutzer dieses Produkt im Einkaufswagen liegen haben,

3) Wie viele Nutzer sich dieses Produkt angeschaut haben.

Dies soll Aufmerksamkeit erzeugen und taucht oft regelmäßig auf, ohne dass sich die numerischen Werte verändern. *Deceptive Activity Notifications* generiert falsche, zufällige Nummern oder verwendet andere täuschende Aussagen durch die Erzeugung fester Werte.

3.1.4.2 Testimonials of Uncertain Origin

listet Nutzer-Empfehlungen und -Bewertungen von einem Produkt auf, bei denen nicht genau nachvollziehbar ist, woher sie stammen oder wie sie erstellt oder mitgeteilt wurden.

3.1.5 Scarcity

Zeigt für ein Produkt eine begrenzte Verfügbarkeit oder eine starke Nachfrage an. So kann der Wert des Produkts aus Sicht des Nutzers und der Wunsch nach ebendiesem Produkt erhöht werden.

3.1.5.1 Low-stock Messages

signalisiert dem Nutzer, dass nur noch eine begrenzte Anzahl eines Produkts verfügbar ist. Dies kann zu Unsicherheit, einem erhöhten Wunsch nach einem Produkt und zu Impulskäufen führen. *Deceptive Low-stock Messages* gibt Auskunft über einen verringerten Vorrat eines Produkts, wobei der angegebene Wert immer wiederkehrt und fest geplant ist. Es kann auch eine zufällige Nummer generiert werden, sobald die Seite neu geladen wird.

3.1.5.2 High-demand Messages

zeigt dem Nutzer die Begehrtheit eines Produkts an. So bekommt er den Eindruck vermittelt, dass das Produkt wahrscheinlich bald ausverkauft sein wird. Manchmal werden diese Werte jedoch willkürlich festgelegt und erscheinen beim Neuladen der Seite oder beim Betrachten eines anderen Produkts immer wieder.

[8] Bandwagon

3.1.5.3 Hard to Cancel (Mathur et al.)

zählt zu *Obstruction* und ähnelt Brignull's Beschreibung von *Roach Motel*.
Dem Nutzer ist nicht bewusst, dass er Mitglied oder Service-Abonnent geworden ist. Oft wird dem Nutzer das Gefühl vermittelt, jederzeit kündigen zu können, jedoch stellt sich dann beim Lesen der Geschäftsbedingungen heraus, dass man dies nur über einen umständlichen Weg, wie einem Anruf beim Kundenservice, bewerkstelligen kann.

3.1.6 Forced Action

siehe 2.4.5 *Forced Action* definiert von Gray et al.

3.1.6.1 Forced Enrollment

Verpflichtet den Nutzer dazu, sich zu Marketing-Kommunikationszwecken (z.B. Newsletter) anzumelden oder ein Konto anzulegen, um ihn zur Preisgabe von Informationen zu verleiten. So muss er mit der Zustimmung der Geschäftsbedingungen auch dem Empfang von Marketing-E-Mails erlauben. Meistens werden dafür Checkboxen verwendet.

3.2 Soziale Netzwerke

3.3 Desktop-Software

3.4 Mobile Anwendungen

Der Großteil der hier vorkommenden Dark Patterns stimmen mit Gray's Kategorien überein. Bei einigen Fällen mussten Geronimo et al. jedoch einschätzen, in welche Kategorie diese hineinpassen [8].
Für einzelne Kategorien werden Beispiele aufgezählt, die in Mobilen Apps Verwendung finden. Nicht berücksichtigt werden konnten allerdings Forced Continuity und Gamification, da Geronimo et al. dafür eine Langzeitstudie hätten durchführen müssen.

3.5 Privacy Dark Patterns

3.5.0.1 Immortal Accounts (Bösch et al.)

Dem Nutzer wird es erschwert oder sogar unmöglich gemacht, sein Konto zu löschen. Zudem kann die Löschung vorgetäuscht werden, während in Wirklichkeit (einige) persönliche Daten behalten werden. Letztendlich können die Barrieren dazu führen, dass der Nutzer sich dagegen entscheidet, sein Konto zu löschen, um sich unnötige Mühen zu ersparen.

3.5.0.2 Hidden Legalese Stipulations

Geschäftsbedingungen sind oft zu lang gestaltet und schwer verständlich formuliert. Aufgrund dessen lesen viele Nutzer diese nicht, wodurch er angreifbar wird, wenn er den Bedingungen dennoch zustimmt. Denn es können Klauseln in den Geschäftsbedingungen versteckt sein und oftmals ohne Vorankündigung verändert werden.

Fall	Unterkategorie	Kategorie
• Ein Pop-up erscheint und unterbricht den Nutzer bei seiner Aufgabe • Pop-up mit Aufforderung zur Bewertung der App		Nagging
• Konto-Löschung nicht möglich • Logout nicht möglich	Roach Motel	Obstruction
• Herauskopieren des Produktnamen beim Shopping nicht möglich	Price Comparison Prevention	
• Mehrere Währungen	Intermediate Currency	
• Ungewollte Artikel werden dem Einkaufswagen hinzugefügt	Sneak into Basket	Sneaking
• Interaktion mit einem App-Feature leitet Nutzer auf Pop-Up mit Hinweis zum Upgrade auf Premium oder auf Android-/iOS-Store um (auch	Bait & Switch	
• Sich bewegende Buttons in der Werbung • Kleines "Schließen"-Button in der Werbung • Anmeldung scheint erforderlich, obwohl die Features der App auch ohne Anmeldung nutzbar sind	Aesthetic Manipulation	Interface Interference
• Geschäftsbedingungen sind klein und/oder in Grau dargestellt	Hidden Information	
• Benachrichtigung (und/oder E-Mails und SMS) ist vorausgewählt • Eine Option ist vorausgewählt • Folgen von Seiten ist voreingestellt • Senden von Nutzungsdaten vorausgewählt (auch *Privacy Zuckering*)	Preselection	
• Countdown-Angebot • Scham-Gefühle auslösen, wenn etwas nicht gemacht wurde	Toying with Emotions	
• Eine von zwei oder mehreren Option sticht deutlicher hervor	False Hierarchy	
• Verwendung doppelter Negation bei Auswahldialog	Trick Question	
• Werbung in Form eines interaktiven Spiels • Werbung oder gesponserter Inhalt, die zum Inhalt zu gehören scheinen • Werbe-Icons/Buttons, die nicht als solche gekennzeichnet sind • Interaktion mit einem App-Feature leitet Nutzer auf Pop-Up mit Hinweis zum Upgrade auf Premium oder auf Android-/iOS-Store um (auch *Bait &*	Disguised Ad	
• Countdown bei Werbeanzeigen • Tägliche/wöchentliche Belohnungen oder Features • Belohnung oder Bonus nach Anmeldung • Countdown bei Belohnungen • Freischalten von Features durch Anschauen von Werbung		Forced Action
• Einladen von Freunden und Belohnungen dafür erhalten	Social Pyramid	
• Dark Patterns bei Privatsphäre-Einstellungen • Senden von Nutzungsdaten vorausgewählt (auch *Preselection*)	Privacy Zuckering	

Abbildung 1: Meine Grafik

3.5.0.3 Bad Defaults

Standard-Optionen werden so gesetzt, dass der Nutzer dazu angeregt werden soll, seine persönlichen Informationen mit dem Service zu teilen. Die meisten Menschen haben keine Zeit, um alle Konfigurationen zur Privatsphäre durchzugehen und an seine Bedürfnisse anzupassen. Infolgedessen geben Nutzer oft mehr über sich preis, als sie beabsichtigen, wie Informationen über den Online-Status, Teile des Nutzerprofils oder Seitenbesuche. Dieses Dark Pattern wird meistens verwendet auf Web- und mobilen Applikationen, vor allem in Sozialen Netzwerken.

3.5.0.4 Privacy Zuckering

siehe *Forced Action* in Abschnitt 2.4.5

3.5.0.5 Address Book Leeching

Der Nutzer wird nach Zugriffsrechten auf sein Adressbuch gefragt, damit er sich mit seinen Kontakten verbinden kann. Jedoch werden die Kontaktdaten intern gespeichert und für die Weiterverarbeitung genutzt, ohne dass der Nutzer darüber in Kenntnis gesetzt wird. Die Kontakte erhalten Einladungen oder Werbung, die oft im Namen des Nutzers versendet werden. Die Daten können auch genutzt werden, Profile zu erstellen und Individuen zu tracken.
Dieses Dark Pattern hängt mit Brignull's *Friend Spam* zusammen. erläutern?

3.5.0.6 Shadow User Profiles

Daten über unregistrierte Personen können ohne ihre Zustimmung und ihr Wissen gesammelt und aufgezeichnet werden. Diese Informationen erhält der Dienstleister von importierten Adressbüchern registrierter Nutzer (z.B. via *Address Book Leeching*), Metadaten oder Erwähnungen und können dazu genutzt werden, um Algorithmen zu verbessern, wie die Empfehlung von Kontakten oder Ad Targeting.

3.6 Games

3.6.0.1 Temporal Dark Patterns

Grinding

Playing by Appointment

3.6.0.2 Monetary Dark Patterns

Pay to Skip

Pre-Delivered Content

Monetized Rivalries

3.6.0.3 Social Capital-Based Dark Patterns

Social Pyramid Schemes

Impersonation

3.7 Proxemische Interaktions-Systeme

Die Proxemik ist ein Forschungsgebiet, Der Begriff der *Proxemik* wurde vom Anthropologen Edward T. Hall im Jahr 1960 vorgestellt und umfasst die Theorie über non-verbale Kommunikationswege, die erklärt, wie Menschen ihre Umgebung wahrnehmen und nutzen, um Kommunikationsziele zu erreichen [13]. Der Theorie zufolge ist die physische Distanz zu anderen abhängig davon, in welcher Beziehung die Kommunikationspartner zueinander stehen. S. Greenberg hat den Begriff der *Proxemischen Interaktion* wie folgt definiert [14]:

> *[...] Diese Erwartungshaltung des Menschen kann gegenüber der Proxemik für Interaktionsdesign genutzt werden, um die Interaktion zwischen Mensch und [digitalen] Geräten in einer Ubicomp-Umgebung Schönere Bezeichnung finden oder Definition formulieren zu beeinflussen. So wie die Menschen zunehmendes Engagement und Intimität erwarten, wenn sie auf andere zugehen, so sollten sie es auch als natürlich empfinden, dass die Konnektivität und Interaktionsmöglichkeiten zunehmen, wenn sie selbst und ihre Geräte sich in unmittelbarer Nähe zueinander befinden. Dies wird als Proxemische Interaktion bezeichnet.*

Greenberg et al. erstellten eine Prognose, wie diese Technologie potentiell missbraucht werden könnte [15]. Nachfolgend wird diese zusammenfassend erläutert.

3.7.1 The Captive Audience

Eine Technologie wird im Raum strategisch platziert und nutzt die Gelegenheit der „Gefangenschaft“ von Personen zu eigenen Zwecken aus, die an einem bestimmten Ort ein Ziel erreichen möchten, welches eine gewisse Zeit in Anspruch nimmt. So müssen Menschen beim Aufsuchen eines Ortes zur Durchführung einer Routine hinnehmen, dass das System eine unaufgeforderte und möglicherweise ungewollte Aktion ausführt.
Beispiele umfassen unter anderem Spiegelflächen-Werbung in öffentlichen Toiletten [16] und öffentliche Werbeflächen. Ein weiteres Beispiel ist ein Projekt der Werbeagentur BBDO und dem Sender Sky Go, die einen Prototypen entwickelten, das über hochfrequentige Vibrationen Audio-Werbung für Pendler abspielt, sobald diese ihren Kopf an das Zugfenster lehnen [17].

3.7.2 The Attention Grabber

Ein strategisch in der Öffentlichkeit platziertes, proxemisch-sensibles System erzeugt Aufmerksamkeit, nachdem es ins Blickfeld einer vorbeilaufenden Person kommt. Es soll den Passanten in einen Kunden verwandeln.
Proximity Marketing, wie Apple's iBeacon oder Samsung Proximity, ist ein Beispiel dafür [18] [19]. Hier werden Kunden in der Nähe via Smartphone-Benachrichtigung Informationen zugesendet, wie Produkt-Vorschläge oder Angebote.

3.7.3 Bait and Switch

Das System lockt einen Betrachter mit begehrenswerten Angeboten oder interessanten Informationen, sobald dieser allerdings darauf aufmerksam wird und sich der Anzeige nähert, verändert sich die Werbung. Daraufhin kann ihm ein Angebot angezeigt werden, das im Bezug auf Preis und Qualität nicht seinen Erwartungen entspricht, weil das zuvor angezeigte Produkt nicht mehr verfügbar ist. Es kann auch zur Darstellung von unerwarteter Werbung genutzt werden. Genauso ist es möglich, den Passanten nach einer Registrierung bei einem ungewollten Service zu fragen, damit er die Interaktion fortführen kann, was mit eventuellen Sicherheitsrisiken verbunden ist.
Amnesty International platzierte 2009 eine Werbung an einer Bushaltestelle, die mithilfe von Eye Tracking erkennen konnte, wann ein Wartender auf die

Anzeige schaut und kurz darauf wurde das Bild verändert. Zunächst wurde ein Bild angezeigt, die Häusliche Gewalt darstellte, und sobald man hinsah, zeigte das Bild ein vermeintlich glückliches Pärchen. Dies sollte auf Häusliche Gewalt aufmerksam machen mit dem Slogan „Es passiert, wenn niemand hinsieht." [20]
Ein anderes, aktuelles Beispiel ist Öffentliches WLAN, wie am Bahnhof oder in Flughäfen. Personen werden mit angeblicher kostenloser WLAN-Verbindung angeworben, jedoch stellt sich erst später heraus, dass der Service erst nach einer Registrierung nutzbar ist. Nach erfolgreicher Verbindung ist die Surfgeschwindigkeit dann allerdings zu langsam und der Nutzer zieht möglicherweise ein Upgrade auf ein Premium-Angebot mit einer schnelleren Surfgeschwindigkeit in Erwägung.

3.7.4 Making Personal Information Public

Sobald eine Person einen bestimmten Bereich betritt, werden seine persönlichen Informationen öffentlich sichtbar gemacht. So können persönliche Informationen, wie Kalender-Einträge, Benachrichtigungen oder Direktnachrichten, auf Geräten in der Nähe angezeigt werden, z.B. auf öffentlichen „Ambient Displays". Diese Systeme haben eigentlich die Absicht, hilfreich zu sein, jedoch können Außenstehende diese persönlichen Informationen einsehen.
In 2009 wagte eine niederländische Werbeagentur eine Guerilla-Marketing Aktion an einer Bushaltestelle von Fitness First in Rotterdam: Ein Gewichtssensor wurde in einer Sitzbank eingebaut und zeigte das Gewicht einer Person auf einem öffentlichen Display an, sobald diese Platz nahm [21].

3.7.5 We Never Forget

Ein System identifiziert proxemische Interaktionen, weil eine permanente, fortbestehende (und ungewollte) Beziehung besteht. Der Verlauf von vergangenen proxemischen Interaktionen wird gespeichert, welcher dazu verwendet werden kann, Verbindungen wiederherzustellen, einen Informationsaustausch durchzuführen, und/oder um vorherige Kontexte wiederherzustellen (z.B. die Anzeige der letzten angezeigten Informationen).
Ein typisches Vorkommnis sind WiFi Hotspots, mit der sich mobile Geräte verbinden können. Möglicherweise möchten Nutzer es bei einer einmaligen Nutzung, und trotzdem kommt es zu einer erneuten, automatischen Verbindung mit dem Service. Dies kann auch die Sicherheit des Nutzers gefährden, wenn beispielsweise jemand ein gestohlenes Handy verwendet und die Anmeldedaten des (ehemaligen) Nutzers missbraucht.

3.7.6 Disguised Data Collection

Zur Verfügung gestellte Informationen eines bestimmten Services wird missbraucht, um Nutzerprofile mit Informationen anzureichern, ohne dass der Nutzer seine Zustimmung abgibt. Systeme, die proxemische Beziehungen nachverfolgen können, haben somit Zugang zu zahlreichen Daten über das Verhalten seiner Nutzer. Diese Infos können von Marketing-Abteilungen potentiell dazu genutzt werden, um Personen zu orten und zu verfolgen und dadurch herauszufinden, wie effektiv Marketing-Aktionen sind. Diese Technologie kann möglich gemacht werden mit bspw. RFID-Chips, Rundfunk-Mobiltelefone und Smart Cards. Viele öffentliche Displays arbeiten bereits mit Computervision, um proxemische

Interaktionen nachzuverfolgen, demnach können Bildaufnahmen analysiert und Personen dadurch identifiziert werden. Zudem können kostenlose WiFi-Dienste aufspüren, an welchem Standort bzw. in welchem Geschäft sich eine Person befindet, indem die Signalstärke und die IP-Adresse des Geräts innerhalb eines Geschäfts gelesen wird.
Kombiniert mit anderen Daten-Ansammlungen, z.B. dem proxemischen Interaktionsverlauf (*We Never Forget*), kann ein noch ausführlicheres Profil erstellt werden.

3.7.7 The Social Network of Proxemic Contacts or Unintended Relationships

Das System verfolgt die proxemischen Beziehungen des Nutzers zu anderen und konstruiert auf dessen Basis ein soziales Netzwerk. Dabei geht es davon aus, dass der Nutzer in einer sozialen Beziehung zu diesen Personen steht, auch wenn dies nicht der Fall ist.
Mit den Daten könnten Marketer beispielsweise Zielgruppen durch demographische Merkmale erkennen. Die Techniken, die in *Disguised Data Collection* beschrieben wurden, können auch dazu genutzt werden, soziale Beziehungen abzuschätzen, indem bspw. physische Distanz oder gemeinsame Interessen analysiert werden.

3.7.8 The Milk Factor

Ein proxemisches System zwingt eine Person, durch einen bestimmten Ort zu gehen oder diesen aufzusuchen, um einen Service zu erhalten.
Ähnlich wie in Supermärkten, wo Produkte strategisch platziert sind, um die Sichtbarkeit von bestimmten, promoteten Gegenständen und somit Impulskäufe zu erhöhen, können proxemische Interaktionen dafür sorgen, dass in Zonen bestimmte Funktionalitäten unzugänglich sind, damit Menschen sich zu bestimmten Orten begeben.
In Japan etwa gibt es Getränkeautomaten, die, wenn man weit weg steht, Werbebilder zeigen, angepasst an die aktuelle Jahreszeit, Temparatur und Tageszeit. Erst, wenn man sich dem Automaten nähert, kann man erkennen, welche Getränke angeboten werden. Demographische und Verkaufs-Daten werden ohne Einwilligung auf dem Firmenserver hochgeladen und für Analysen und zu Marketing-Zwecken verwendet.

3.8 Künstliche Intelligenz

3.8.1 Home Robots

4 Schluss

4.1 Ausblick

4.2 Fazit

Literatur

[1] Harry Brignull. *Dark Patterns - Dirty Tricks Designers Use to Make People Do Stuff*. 2010. URL: https://90percentofeverything.com/2010/07/08/dark-patterns-dirty-tricks-designers-use-to-make-people-do-stuff/.

[2] Harry Brignull und Alexander Darlington. *Dark Patterns - Types of Dark Pattern*. Zuletzt besucht am 15.11.2020. 2010. URL: https://darkpatterns.org/types-of-dark-pattern.html.

[3] Harry Brignull. *Dark Patterns / Twitter*. Zuletzt besucht am 15.11.2020. URL: https://twitter.com/darkpatterns.

[4] Colin M. Gray u. a. "The Dark (Patterns) Side of UX Design". In: *CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* 534 (2018). DOI: 10.1145/3173574.3174108.

[5] Paul Thurrott. *Upgradegate: Microsoft's Upgrade Deceptions Are Undermining Windows 10*. Zuletzt besucht am 15.11.2020. 2016. URL: https://www.thurrott.com/windows/windows-10/67367/upgradegate-microsofts-upgrade-deceptions-undermining-windows-10.

[6] Harry Brignull und Alexander Darlington. *Dark Patterns - Friend Spam - A Type of Dark Pattern*. Zuletzt besucht am 16.11.2020. 2010. URL: https://darkpatterns.org/types-of-dark-pattern/friend-spam.html.

[7] Arunesh Mathur u. a. "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites". In: *Proc. ACM Hum.-Comput. Interact.* 1.CSCW (2019). DOI: 10.1145/3359183.

[8] Linda Di Geronimo u. a. "UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception". In: *CHI '20: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* CSCW (2020). DOI: 10.1145/3313831.3376600.

[9] José P. Zagal, Staffan Björk und Chris Lewis. "Dark Patterns in the Design of Games". In: *Foundations of Digital Games 2013* (2013).

[10] Christoph Bösch u. a. "Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns". In: *Proceedings on Privacy Enhancing Technologies 2016* (2016). DOI: 10.1515/popets-2016-0038.

[11] Dr. Cherie Lacey und Dr. Catherine Caudwell. "Cuteness as a 'Dark Pattern' in Home Robots". In: IEEE Press, 2019, S. 374–381. DOI: 10.1109/HRI.2019.8673274.

[12] Arvind Narayanan u. a. *Dark Patterns - Past, Present, and Future | September 2020 | Communications of the ACM*. Zuletzt besucht am 18.11.2020. 2020. URL: https://cacm.acm.org/magazines/2020/9/246937-dark-patterns/fulltext.

[13] Communication Studies. *Proxemics - Communication Studies*. Zuletzt besucht am 19.11.2020. 2013. URL: https://www.communicationstudies.com/communication-theories/proxemics.

[14] Nicolai Marquardt und Saul Greenberg. *Proxemic Interactions: From Theory to Practice - Synthesis Lectures on Human-Centered Informatics*. 2015. DOI: 10.2200/S00619ED1V01Y201502HCI025.

[15] Saul Greenberg u. a. "Dark Patterns in Proxemic Interactions: A Critical Perspective". In: Association for Computing Machinery, 2014. DOI: 10.1145/2598510.2598541.

[16] Deal Runner. *Novo-Ad Mirror*. Zuletzt besucht am 19.11.2020. 2015. URL: https://www.youtube.com/watch?v=nTZ13rwdFYQ.

[17] Jörg Breithut. *DER SPIEGEL - Spiegel Netzwelt - Sprechende Fenster wecken schlafende Pendler*. Zuletzt besucht am 19.11.2020. 2013. URL: https://www.spiegel.de/netzwelt/gadgets/sprechende-zugfenster-diese-werbung-weckt-schlafende-pendler-a-909619.html.

[18] Jose Vilches. *Techspot - Apple's iBeacon location-aware shopping goes live in over 250 stores*. Zuletzt besucht am 19.11.2020. 2013. URL: https://www.techspot.com/news/54932-apples-ibeacon-location-aware-shopping-goes-live-in-over-250-stores.html.

[19] Shawn Knight. *Techspot - Proximity is Samsung's version of Apple's iBeacon marketing platform*. Zuletzt besucht am 19.11.2020. 2014. URL: https://www.techspot.com/news/58799-proximity-samsung-version-apple-ibeacon-marketing-platform.html.

[20] Marco Settembrini di Novetre. *Frankfurter Allgemeine - Deus Ex Machina - Guck mal, wer da guckt*. Zuletzt besucht am 19.11.2020. 2012. URL: https://blogs.faz.net/deus/2012/12/11/guck-mal-wer-da-guckt-961/.

[21] Charlie Sorrel. *Weight-Revealing Billboard Shames Fatties into Joining Gym*. Zuletzt besucht am 19.11.2020. 2009. URL: https://www.wired.com/2009/03/weight-revealin/.