

Wissenschaftliche Arbeit

Dark Patterns und ihre Auswirkungen auf den Erfolg eines Unternehmens

MxD (2023)

vorgelegt von

David Breyer

eingereicht bei

Mag. Haris Seferagic

Abgabedatum: 19.06.2021

Abstract

Auf der Suche nach Wachstumsmöglichkeiten setzen Technologie-Unternehmen zunehmend auf Big Data, das Sammeln von Daten, um genauere Werbungen zu schalten und somit mehr Geld aus Benutzer*innen zu machen. An diese Daten muss man aber erst einmal herankommen und hier gilt es als Unternehmen eine Entscheidung zu fällen: Wie weit sind wir bereit zu gehen für diese Daten? Nehmen wir was uns gegeben wird oder nehmen wir was wir, auf welche Art auch immer, kriegen können? Viele Unternehmen entscheiden sich für letzteres und verschreiben sich somit den Dark Patterns. Das sind Methoden im User Interface Design um Benutzer*innen auszutricksen und an ihre Daten zu kommen. Sie wirken wie ein genialer Schachzug, verbergen allerdings auch Konsequenzen, die nicht sofort erkennbar sind. Diese Konsequenzen sind vor allem finanzieller Natur, können aber auch die Beziehung zum Kunden nachhaltig beeinflussen. Es wird gezeigt, dass Firmen die auf Dark Patterns setzen, ein Vielfaches des Umsatzes erzielen können, dadurch aber ihre Kunden verärgern und Regierungen zum Handeln animieren. Einige dieser Kunden bringen Klagen ein, die Strafen in Millionen-Höhe nach sich ziehen können und die Regierungen entwerfen Verordnungen die Unternehmen Dark Patterns verbieten sollen. Diese negativen Konsequenzen sind im Moment vernachlässigbar, dürfen aber nicht vollkommen ignoriert werden, da sonst in Zukunft nachhaltige Schäden am Unternehmen entstehen können.

Inhalt

Einleitung.....	4
1. Wortherkunft	5
2. Digital Nudging und Dark Patterns	5
3. Wirkungsmechanismus	6
3.1 Asymmetrische und unvollständige Information	6
3.2 Die Rolle der Heuristik.....	7
3.3 Kognitive- und Verhaltensneigungen.....	8
4. Arten von Dark Patterns	9
4.1 Nagging.....	9
4.2 Obstruction	9
4.3 Sneaking.....	10
4.4 Interface Interference	10
4.5 Forced Action	11
5. Auswirkungen.....	11
5.1 Erosion von Vertrauen	11
5.2 Auswirkungen im Bereich der Ethik.....	13
5.3 Rechtliche Auswirkungen	13
5.4 Finanzielle Auswirkungen	14
6. Fazit	16
Literaturverzeichnis.....	17

Einleitung

Wer heutzutage digitale Services nutzt und das Internet verwendet ist unweigerlich über Begriffe wie „Cookies“, „relevante Werbung“ und „personalisierte Erlebnisse“ gestolpert, oft in Verbindung mit „das Recht zu Privatsphäre“ und „Datenschutz“. Dass diese Begriffe bedeuten, dass das Verhalten eines Benutzers analysiert und verarbeitet wird, um Werbung zu zeigen, ist auch den meisten Menschen bekannt. Welche Daten genau gesammelt werden ist aber schon weitaus weniger offensichtlich. Dass aber die Entscheidung über die Verwendung der Daten nicht zu hundert Prozent bei Benutzer*innen liegt, dürften nur wenige Menschen wissen, denn Unternehmen, die mit den Auswertungen der Daten ihr Geld verdienen, treffen diese Entscheidung schon lange davor für Benutzer*innen. Natürlich hat jeder die Möglichkeit und das Recht die Datensammlung und Verarbeitung abzulehnen, dies tun allerdings nur ein Bruchteil der Menschen.¹ Der Grund für dieses Verhalten liegt vor allem in sogenannten Dark Patterns. Diese beschreiben eine Methodik, eine Art des User Experience Designs, um Benutzer*innen in eine im Vorfeld definierte Richtung zu lenken. Mit welchen Mitteln das geschieht, warum diese spezielle Herangehensweise problematisch ist und was die möglichen Auswirkungen von Dark Patterns sind, ist Gegenstand dieser Arbeit.

¹ Vgl. (Amazee Metrics Ltd., 2021)

1. Wortherkunft

Der Begriff „Dark Patterns“ kommt aus dem Englischen und bedeutet wörtlich übersetzt „Dunkle Muster“. Damit sind Designpraktiken gemeint, die verwendet werden, um Benutzer*innen auszutricksen. Sie werden als dunkel bezeichnet, weil sie für den Benutzer*innen oft nicht erkennbar sind. Der Begriff „Dark Patterns“ wurde das erste Mal von Harry Brignull im Jahr 2010 verwendet.²

2. Digital Nudging und Dark Patterns

Nudging ist ein Konzept aus der Verhaltenspsychologie und beschreibt, wie man Kunden*innen oder Benutzer*innen von einer rationalen Entscheidung zu einer irrationalen Entscheidung bewegen kann, indem man sich ihre psychologischen Tendenzen zunutze macht. Dieses Einwirken passiert meistens ohne das Kunden*innen oder Benutzer*innen dies bemerken.³ Im Digitalen Raum, Digital Nudging genannt, wird es immer dann angewendet, wenn Benutzer*innen einer Software oder Website eine Entscheidung treffen oder etwas beurteilen muss.⁴ Dabei wird auf das sogenannte user-centered-design zurückgegriffen (Benutzer-orientiertes Design), welches Methoden und Richtlinien für das Design eines Interfaces vorgibt, um die Intentionen der Benutzer*innen so gut wie möglich vorauszusagen und ihre Wünsche und Bedürfnisse bestmöglich in das Design zu integrieren.⁵ Um die Benutzer*innen anhand dieses Designs zu führen und dessen Verhalten zu beeinflussen werden verschiedene Methoden angewandt. Zum Beispiel können Benutzer*innen zu einer bestimmten Entscheidung bewegt werden, wenn die Information, die Gegenstand einer Auswahlmöglichkeit ist, zu den Wissen passt das die Benutzer*innen bereits besitzt (confirmation-bias). Eine andere Art ist die Tendenz der Menschen zu nutzen, eine kurzfristige Belohnung einer längerfristigen vorzuziehen. Wenn Designer diese und weitere Verhaltensweisen kennen, können sie das Verhalten der Benutzer*innen beeinflussen, um diese zu Entscheidungen zu bewegen die in ihrem Interesse sind.⁶ Wichtig dabei ist, dass die Entscheidungen immer den Benutzer*innen

² Vgl. (Brignull, Expert witness in dark patterns - testimonium.co, 2021)

³ Vgl. (Hartzog, 2018)

⁴ Vgl. (Forbruker Rådet, 2021)

⁵ Vgl. (U.S. General Services Administration , 2021)

⁶ Vgl. (Forbruker Rådet, 2021)

zugute kommen ohne dessen Entscheidungsoptionen zu beschränken.⁷ Designer*innen sollten dabei immer die ethischen Implikationen des Designs im Blick behalten, denn in der Praxis werden Nudges oft missbräuchlich verwendet, um Benutzer*innen zu Entscheidungen zu bewegen die sie unter normalen Umständen nicht getätigt hätten.⁸

Diese missbräuchliche Art von Nudging wird „Dark Patterns“ genannt. Der Begriff „Dark Patterns“ beschreibt das Verwenden des Wissens um die Intention der Benutzer*innen und der menschlichen Verhaltenspsychologie um Benutzer*innen fehlzuleiten, um Entscheidungen zu beeinflussen die nicht im Interesse der Nutzer*innen sind.⁹ Zum Beispiel wird das Wissen, dass die Sicherheit und Privatsphäre der Nutzer*innen selten zu dessen primären Intentionen zählt und deswegen wenig mentale Kapazitäten zur Verfügung stehen um alle möglichen Ausgänge und Konsequenzen der bevorstehenden Entscheidung abzuschätzen, ausgenutzt um mehr Daten mit der Zustimmung der Benutzer*innen zu sammeln als ohne Dark Patterns.¹⁰

3. Wirkungsmechanismus

Wie im vorangegangenen Kapitel bereits erläutert, stützen sich Dark Patterns sowie Nudging auf das Wissen und Ausnutzen der menschlichen Verhaltenspsychologie und Entscheidungsfindung. In diesem Kontext gibt es mehrere bekannte Arten das Verhalten der Nutzer*innen zu lenken, die wichtigsten werde ich anführen. Dies ist in keiner Art und Weise eine vollständige Liste, noch soll es eine sein. Sie dient allein dem generellen Verständnis der Entscheidungsfindung, welche eine integrale Rolle im Bereich der Dark Patterns spielt.

3.1 Asymmetrische und unvollständige Information

Bei asymmetrischer und unvollständiger Information hat eine Partei (die Benutzer*innen) weniger oder schlechteres Wissen, um eine Entscheidung zu treffen als die andere Partei

⁷ Vgl. (Acquisti, et al., 2017)

⁸ Vgl. (Weinmann, Schneider, & vom Brocke, 2021)

⁹ Vgl. (Gray, Kou, Battles, Hoggatt, & Toombs, 2018)

¹⁰Vgl. (Acquisti, et al., 2017)

(zum Beispiel: Webseiten-Betreiber*innen).¹¹ Bansal und Zahedi sprechen vom Trustee (den Benutzer*innen) und dem Trustor (die Partei, der mit der Datensammlung vertraut wird).¹² Die Partei mit mehr oder besserer Information ist im Vorteil. Diese Konstellation ist im Bereich von Informationssicherheit und Privatsphäre die Norm. Hier hat zum Beispiel die Partei, die private Daten über eine andere Partei sammelt, einen Vorteil, indem sie die andere Partei nur bedingt wissen lässt, wofür die Daten gesammelt werden und wofür sie in Zukunft verwendet werden könnten.¹³

3.2 Die Rolle der Heuristik

Um eine Entscheidung mit wenig oder unvollständiger Information zu tätigen, müssen Benutzer*innen die Optionen und deren Wahrscheinlichkeiten abwägen. Dieser kognitive Vorgang kann unter Umständen einiges an mentale Kapazitäten abverlangen, vor allem wenn es um Privatsphäre und Informationssicherheit geht. Deshalb fallen die meisten Benutzer*innen auf die Heuristik zurück. Heuristik bezeichnet die Entscheidungsfindung mit begrenzten Informationen und Zeit, eine Abkürzung und Vereinfachung des Entscheidungsprozesses. Man kann es auch als Faustregel verstehen, mit der der Sachverhalt vereinfacht wird, um mit so wenig Aufwand wie möglich zu einer Entscheidung zu kommen. Dabei wird immer auf bereits bestehendes Wissen zurückgegriffen, um daraus die Wahrscheinlichkeiten für bestimmte Ausgänge der Entscheidung zu erwägen. Da aber die meisten Menschen, vor allem im Bereich der Privatsphäre, ein unvollständiges Bild der Lage besitzen, werden die Wahrscheinlichkeiten falsch angenommen. Zum Beispiel kann die Wahrscheinlichkeit, dass die Privatsphäre verletzt wird, als eher unwahrscheinlich wahrgenommen werden, weil die Benutzer*innen selbst nie davon betroffen waren und solche Ereignisse generell nicht direkt zu beobachten sind. Dadurch entsteht der falsche Eindruck, dass solche Ereignisse unwahrscheinlich sind, welcher es erheblich erleichtern, Dark Patterns ohne dem Wissen der Betroffenen anzuwenden. Dieser Fehleinschätzungen können so weit gehen, dass Nutzer*innen einer Website „blind“ vertrauen, da diese von einem Unternehmen betrieben wird, gegenüber denen sie positiv gestimmt sind. Lediglich

¹¹ Vgl. (Acquisti, et al., 2017)

¹² Vgl. (Bansal & Zahedi, 2015)

¹³ Vgl. (Acquisti, et al., 2017)

das Vorhandensein einer Datenschutzerklärung, unabhängig von ihrem tatsächlichen Inhalt, kann Nutzer*innen dazu verleiten der Website Daten anzuvertrauen.¹⁴

3.3 Kognitive- und Verhaltensneigungen

Während die Heuristik vor allem bei komplizierten Entscheidungen zur Anwendung kommt, sind kognitive und Verhaltensneigungen bei jeder Art von Fragestellung zu beobachten. In dem Bereich der Privatsphäre und der Informationssicherheit sind das vor allem Anchoring, Status Quo Bias und Loss Aversion.

Anchoring beschreibt das Nutzer*innen oft Information bedenken, die möglicherweise wenig mit dem eigentlichen Thema zu tun hat, aber dennoch das Fundament der Entscheidungsfindung bilden. Der Entscheidungsprozess wird in dieser Information verankert (eng. to anchor).

Der Status Quo Bias beschreibt das Bestreben der meisten Benutzer*innen immer die voreingestellten Optionen zu übernehmen. Dies wird in dem falschen Glauben getan, dass die voreingestellte Option die rational Beste ist. Oft ist auch das unzureichende Wissen der Nutzer*innen über Risiken im Bereich der Privatsphäre der Faktor warum Benutzer*innen nicht von der voreingestellten Option abweichen.

Loss Aversion bezeichnet das Bestreben der Menschen so wenig wie möglich ihrer Ressourcen zu verlieren. Im Bereich der Privatsphäre bedeutet das, dass die Nutzer*innen abwägen müssen, wie viel ihnen ihre Daten wert sind. Diese Daten sind aber nicht immer gleich viel wert, denn wenn Nutzer*innen das Gefühl haben sie haben die Kontrolle über ihre Privatsphäre sind ihnen ihre Daten um einiges mehr wert, als wenn sie denken, dass sie ihre Daten bereits verloren haben.

¹⁴ Vgl. (Acquisti, et al., 2017)

4. Arten von Dark Patterns

Vorerst muss erwähnt werden, dass es keine einheitlich anerkannte Definition der Arten von Dark Patterns gibt. Die meisten Versuche sie zu kategorisieren beziehen sich auf Harry Brignulls Klassifizierungen, welche 2010 auf dessen Website darkpattern.org veröffentlicht wurden.¹⁵ Darauf aufbauend hat Colin M. Gray et al eine neue Systematik der Dark Patterns entworfen, um sie genereller anwendbar zu machen und die Motivationen der Designer*innen besser einzufangen.¹⁶ Auf diese Klassifizierung bezieht sich dieses Kapitel.

4.1 Nagging

Nagging ist eine immer wiederkehrende Unterbrechung, während der Benutzer*innen seiner primären Intention nachgeht. Diese Unterbrechung hat dabei nichts mit dem zu tun auf das sich die Nutzer*innen fokussiert. Solche Unterbrechungen können durch Pop-Ups, Audio-Einspielungen oder andere Arten die Aufmerksamkeit der Nutzer*innen zu erlangen und abzulenken erwirkt werden. Bei Pop-Ups gibt es oft keine Möglichkeit ein zukünftiges Aufpoppen zu verhindern und die Nutzer*innen werden dazu gedrängt die Option auszuwählen, die für das Unternehmen am besten ist. Da diese immer wieder kehrenden Pop-Ups die Benutzer*innen stören, tendieren sie dazu den einfachsten Weg zu nehmen, um die Störung zu beenden.¹⁷

4.2 Obstruction

Obstruction (eng. Behinderung, Hindernis) bezeichnet eine Verkomplizierung eines Prozesses um die Intention der Benutzer*innen so schwer wie möglich zu machen und ihm davon abzubringen seine Intention vollständig durchzuführen. Es ist zum Beispiel viel komplizierter Cookies auf Webseiten abzulehnen als sie zu akzeptieren. Die Aktion, die nicht

¹⁵ Vgl. (Brignull, Dark Patterns - About Us , 2020)

¹⁶ Vgl. (Gray, Kou, Battles, Hoggatt, & Toombs, 2018)

¹⁷ Vgl. (Gray, Kou, Battles, Hoggatt, & Toombs, 2018)

im Sinne des Unternehmens ist, wird hinter unnötig vielen Klicks und User-Interface Leveln versteckt.¹⁸

4.3 Sneaking

Der Begriff „sneaking“ (eng. Schleichen) wird verwendet, wenn eine Applikation oder Webseite absichtlich für die Benutzer*innen wichtige Information versteckt, sozusagen an ihnen vorbei schleicht. Dies kommt oft bei gratis Testversionen vor, wobei die meisten Nutzer*innen übersehen, dass sie eigentlich ein Abonnement abgeschlossen haben und nach Ablauf der Testperiode den vollen Preis automatisch verrechnet bekommen. Eine weitere Art des Sneakings wäre das Verzögern von wichtigen Informationen. Manche Online-Shops verwenden dieses Schema um Kunden*innen zuerst mit günstigen Preisen zu locken und ihnen erst beim Check-Out den vollen Preis, inklusive Lieferkosten und Bearbeitungsgebühren, anzuzeigen.

4.4 Interface Interference

Als Interface Interference (User Interface; eng. Störung, Einmischung) wird jede Art von visueller Hierarchie im User-Interface einer Applikation oder Webseite bezeichnet, die es den Benutzer*innen erschweren sollen, bestimmte Optionen und Information zu finden. Gleichzeitig können andere Optionen hervorgehoben sein, um Benutzer*innen zu diesen zu leiten. Zum Beispiel kann bei mehreren Auswahloptionen bereits eine Option vorgewählt oder bei einem Pop-Up eine Auswahlmöglichkeit farblich hervorgehoben sein. Manche Interfaces zeigen verschiedene Auswahlmöglichkeiten in Schwarz beziehungsweise in Grau an, damit die Nutzer*innen denken, dass die Graue Option nicht verfügbar ist.¹⁹ Auch Werbungen, die als Spiele getarnt sind, zählen zu Interface Interference.²⁰

¹⁸ Vgl. (Gray, Kou, Battles, Hoggatt, & Toombs, 2018)

¹⁹ Vgl. (Gray, Kou, Battles, Hoggatt, & Toombs, 2018)

²⁰ Vgl. (Brignull, Dark Patterns - About Us , 2020)

4.5 Forced Action

Forced Action ist eine häufig vorkommende Methode der Dark Patterns, wobei die Benutzer*innen zu einer Entscheidung gezwungen werden, bevor diese ihrer eigentlichen Intention nachgehen können. Zum Beispiel könnten Benutzer*innen gezwungen werden, eine privatsphärenverletzende Datenschutzerklärung zu akzeptieren, um E-Mail-Benachrichtigungen abzubestellen. Wird die Datenschutzerklärung nicht akzeptiert, können die Nutzer*innen die Benachrichtigungen auch nicht abbestellen.

5. Auswirkungen

Nicht alle Dark Pattern sind gleich „dark“. Dennoch hat jedes Pattern das Potential ein schlechtes User Interface beziehungsweise eine schlechte User Experience zu erwirken.

Die Auswirkungen der Dark Pattern auf ein Unternehmen sind vielschichtig und betreffen verschiedene Bereiche, die in meinen Nachforschungen zusammenhängend erscheinen. Um die Auswirkungen zu quantifizieren, wurden mehrere Datenpunkte rund um bekannte Unternehmen, wie Facebook und Google verwendet. Des Weiteren wurden Statistiken, wissenschaftliche Reports und Artikel herangezogen, um einige Punkte zu stützen. Das Ziel war es, herauszufinden, ob es sich als Unternehmen lohnt auf Dark Patterns zu setzen oder ob negative Konsequenzen überwiegen.

5.1 Erosion von Vertrauen

„ [Trust is a] state of willingness to accept vulnerability based upon positive expectations of the intentions or behavior of the trustee in matters important to the trustor.“²¹

Vorerst muss erwähnt werden, dass für den digitalen Raum andere Maßstäbe gelten als in physischen Kundenbeziehungen. Ein Unternehmen muss bedenken, dass sie als digital agierende Serviceanbieter dem Kunden „Gesichtslos“ und schwer greifbar gegenüberstehen.²² Das bedeutet, dass Vertrauen auf einem schwächeren Fundament aufbaut und leichter zerstört werden kann. Werden Dark Patterns verwendet, erodiert das

²¹ Vgl. S. 62 (Bansal & Zahedi, 2015)

²² Vgl. (Bansal & Zahedi, 2015)

Vertrauen des Kunden in das Unternehmen kontinuierlich. Da eine Kaufentscheidung erheblich davon beeinflusst wird, wie Kunden*innen ein Unternehmen wahrnehmen, sind sinkende Verkaufszahlen und andere Schäden die Folge.²³ Wird das Vertrauen, dass Unternehmen die Verletzlichkeit der Privatsphäre der Nutzer*innen nicht missbrauchen, zerstört, kann dies außerdem bedeuten, dass die Nutzer in Zukunft weniger oder gar nicht mit dem Unternehmen kooperieren.²⁴ Hier muss angemerkt werden, dass diese Auswirkungen im Wechselspiel mit der vorher erwähnten Loss Aversion stehen. Haben Benutzer*innen bereits das Gefühl, dass sie nicht mehr in Kontrolle ihrer Daten oder ihrer Privatsphäre sind, könnten die Auswirkungen des erodierten Vertrauens erheblich gemildert werden.

Dazu kann erwähnt werden, dass offenbar eine Verbindung zwischen der Wahrnehmung der Kunden*innen gegenüber den Anstrengungen eines Unternehmens im Bereich der Wohltätigkeit und dem Vertrauen in das Produkt besteht. Je „besser“ ein Unternehmen wahrgenommen wird, desto mehr wird dessen Produkten vertraut. Dies kann bedeuten, dass das Verwenden von Dark Patterns unter Umständen mitigiert werden könnte.

Ein weiterer Faktor ist, dass Kunden*innen durch die unerwarteten Konsequenzen ihrer Entscheidungen Frustration aufbauen. Manche Personen könnten hinterfragen, ob sie etwas falsch gemacht haben oder ob das System schuld ist.²⁵ Es könnte passieren, dass dieses Gefühl der Frustration mit dem Produkt beziehungsweise mit dem Unternehmen assoziiert wird. Das würde auf lange Sicht bedeuten, dass das Image des Unternehmens leidet und Kunden*innen nicht mehr bereit sind die Produkte weiter zu verwenden oder auf ein neues Produkt umsteigen. Sollte ein Unternehmen die Strategie des Up-Sellings verwenden, würde dies ein entscheidendes Hindernis darstellen.

All dies trägt dazu bei, dass das Vertrauen in Unternehmen im digitalen Bereich stetig sinkt. Im Jahr 2020 liegt das Vertrauen in diese Unternehmen bei 75%, im Jahr davor noch bei 79%.²⁶

²³ Vgl. (Tian, Hung, & Frumkin, 2020)

²⁴ Vgl. (Bansal & Zahedi, 2015)

²⁵ Vgl. (Gray, Kou, Battles, Hoggatt, & Toombs, 2018)

²⁶ Vgl. (Edelman, 2020)

5.2 Auswirkungen im Bereich der Ethik

Die Erosion des Vertrauens und die damit verbundene Behandlung der Nutzer*innen und Kunden*innen wirft unweigerlich Fragen der Ethik auf. Inwiefern die Praktiken der Dark Patterns ethisch vertretbar sind, wird zunehmend von Organisationen und Regierungen diskutiert. Dies führt dazu, dass Dark Patterns mehr und mehr von der Öffentlichkeit und den Regierungen der Welt als Problem erkannt werden. Ein Weg den Regierungen und Organisation gehen ist, dass sie Versuchen Regeln und Gesetze für das Design von Interfaces und Experiences festzulegen, die die Bewegungsfreiheit von Unternehmen in diesem Bereich einschränken. Im Umkehrschluss bedeutet das, dass Unternehmen mit der Verwendung von stark in die Irre führenden Dark Patterns sich damit möglicherweise selbst Steine in den Weg legen. Während Dark Patterns auf den ersten Blick sehr profitabel wirken, sind die Rückwirkungen von Organisation und Regierungen nicht zu unterschätzen.

5.3 Rechtliche Auswirkungen

Durch das Aufmerksam werden der Regierungen und anderen Organisationen ergeben sich zwei distinktive Auswirkungen im Bereich des Rechts, Klagen gegen das Unternehmen und Gesetze, die das Unternehmen zum Einlenken zwingen sollen.

Klagen gegen Unternehmen aufgrund der Verwendung von Dark Patterns sind selten. Eine der bekanntesten ist eine Klage gegen das professionelle soziale Netzwerk LinkedIn. Dabei wurden Dark Patterns im Zusammenhang mit E-Mail-Benachrichtigungen als illegal unter der Gesetzeslage in Kalifornien gesehen. LinkedIn wurde verurteilt und mit einer Strafe von 13 Millionen US-Dollar belastet. Diese Zahl hätte bei anderem Verfahrensausgang maximal 975 Millionen US-Dollar betragen können.²⁷ Auch Google wurde im Jahr 2020 angeklagt, Benutzer*innen in die Irre geführt zu haben. Das Unternehmen wurde noch nicht verurteilt, wenn würde Google aber eine Strafe von bis zu 5 Milliarden US-Dollar bevorstehen.²⁸

Die Gesetze, die diese Klagen ermöglichen, werden ständig angepasst und erweitert. Kalifornien kann im Bereich der Dark Patterns als Vorreiter gesehen werden, da der Bundesstaat im Jahr 2021 eine neue Verordnung erlassen hat, die das Verwenden von Dark

²⁷ Vgl. (Brownlee, 2021)

²⁸ Vgl. (Davis, 2021)

Patterns, die die Fähigkeit der Verbraucher*innen selbst zu entscheiden stark beeinflussen oder untergraben, verbieten. Dies betrifft zwar nicht alle Dark Patterns, aber schränkt Unternehmen dennoch ein.²⁹ Auch in Europa wird Zunehmens auf Dark Patterns geachtet. Frankreichs Datenschutz Kommission hat einen Bericht über die Wichtigkeit von User Interface Design für den Verbraucher veröffentlicht, ähnliche Berichte und Forschungsprojekte kommen aus Deutschland und Großbritannien.³⁰ Noch bedeuten diese Berichte nicht, dass Gesetze verabschiedet werden und Folgen für Unternehmen entstehen, die Aufmerksamkeit ist jedoch auf Dark Patterns gerichtet und Gesetze sind Großteils nur noch eine Frage der Zeit. Der andere Teil, der die Gesetzesverabschiedung beeinflusst, sind die Unternehmen selbst, mithilfe von Lobbying. Google hat im Jahr 2018 21.2 Millionen US-Dollar an Lobbyisten gezahlt, im Jahr 2020 nur mehr 8.8 Millionen US-Dollar.³¹ Es kann angenommen werden, dass die Ausgaben für Lobbying ansteigen werden, sollten Unternehmen weiter auf Dark Patterns setzen wollen. Dies sollte jedoch gut überlegt werden, denn neben den Kosten für das Lobbying müssen die potenziellen Strafen im Hinterkopf behalten werden.

5.4 Finanzielle Auswirkungen

Alle der bereits genannten Punkte wirken sich direkt und indirekt auf die Bilanz eines Unternehmens aus. Um den Strafen, Lobbying Kosten und dem verlorenen Vertrauen zu entkommen könnten Unternehmen Dark Patterns den Rücken kehren. Das Entfernen von Dark Patterns könnte aber zu finanziellen Einbußen führen, da Nutzer*innen die personalisierte Werbung ausschalten, sollten diese eine einfach verfügbare Möglichkeit haben, das zu tun.³² Die mögliche Höhe dieser Einbußen ist von vielen individuellen Faktoren abhängig. Um diese zu veranschaulichen, wurden Google Search, bekannt für weitreichende Datensammlung und daraus resultierender personalisierter Werbung, und DuckDuckGo, bekannt dafür keine Daten zu speichern und Benutzer*innen nicht zu verfolgen, verglichen, um ein Bild der finanziellen Unterschiede der verschiedenen Geschäftsmodelle zu bekommen. Das erste Ziel war es, den Umsatz pro Suche zu

²⁹ Vgl. (Vincent, 2021)

³⁰ Vgl. (Kellogg, 2021)

³¹ Vgl. (Opensecrets, 2021)

³² Vgl. (Laziuk, 2021)

berechnen. Dazu wurden Daten zum Umsatz der Werbung bei Google Search verwendet, welcher 2020 über 104 Milliarden US-Dollar betrug.³³ Die Anzahl der Suchanfragen war 2020 bei circa 2.5 Billionen.³⁴ Dies ergibt einen Umsatz pro Suche bei Google Search von 0.041 US-Dollar. DuckDuckGo fuhr im Jahr 2020 einen Umsatz von 100 Millionen US-Dollar ein.³⁵ Die Zahl der Suchanfragen wird mit 23 Milliarden angegeben.³⁶ Der Umsatz pro Suche beträgt demnach 0.0042 US-Dollar, ein Zehntel dessen von Google.

Um Google Search mit der viel kleineren Suchmaschine DuckDuckGo besser vergleichen zu können, wurde der Umsatz des Jahres 2020 auf die Benutzer*innen-Zahl desselben Jahres heruntergebrochen, um den aussagekräftigeren Umsatz pro Benutzer*in zu errechnen. Die Benutzer*innen-Zahl von DuckDuckGo kann laut DuckDuckGo nur geschätzt werden, da sie keine Daten speichern. DuckDuckGo errechnet einen geschätzten Wert von 80 Millionen Benutzern*innen.³⁷ Dies ergibt einen Umsatz pro Benutzer*in von 1.25 US-Dollar.

Die Benutzer*innen-Zahl von Google Search ist um einiges schwieriger zu definieren, da Google keine Benutzerzahlen veröffentlicht. Um dennoch eine verwertbare Zahl zu bekommen, wurde die Zahl der Google Search Benutzer*innen anhand anderer verwandter Statistiken geschätzt. Zuerst wurde die Zahl der Internetbenutzer*innen weltweit herangezogen³⁸ und mit dem prozentuellen Anteil des Datenverkehrs, der durch Suchmaschinen generiert wird,³⁹ multipliziert. Die resultierende Zahl, die die gesamten Benutzer*innen von Suchmaschinen darstellt, wurde mit dem Marktanteil von Google Search multipliziert, welcher 87.66% beträgt.⁴⁰ Das Ergebnis ist die geschätzte Benutzer*innen-Zahl von Google Search, welche bei 3.94 Milliarden Benutzer*innen liegt. Rechnet man mit dieser Zahl, ergibt sich ein Umsatz pro Benutzer*in von 26.41 US-Dollar. Dieser Wert ist circa 21-mal höher als bei DuckDuckGo. Damit kann angenommen werden, dass die finanziellen Anreize Dark Patterns zu verwenden sehr schwer wiegen.

³³ Vgl. (Statista, 2021)

³⁴ Vgl. (Petrov, 2021)

³⁵ Vgl. (Steinberg, 2021)

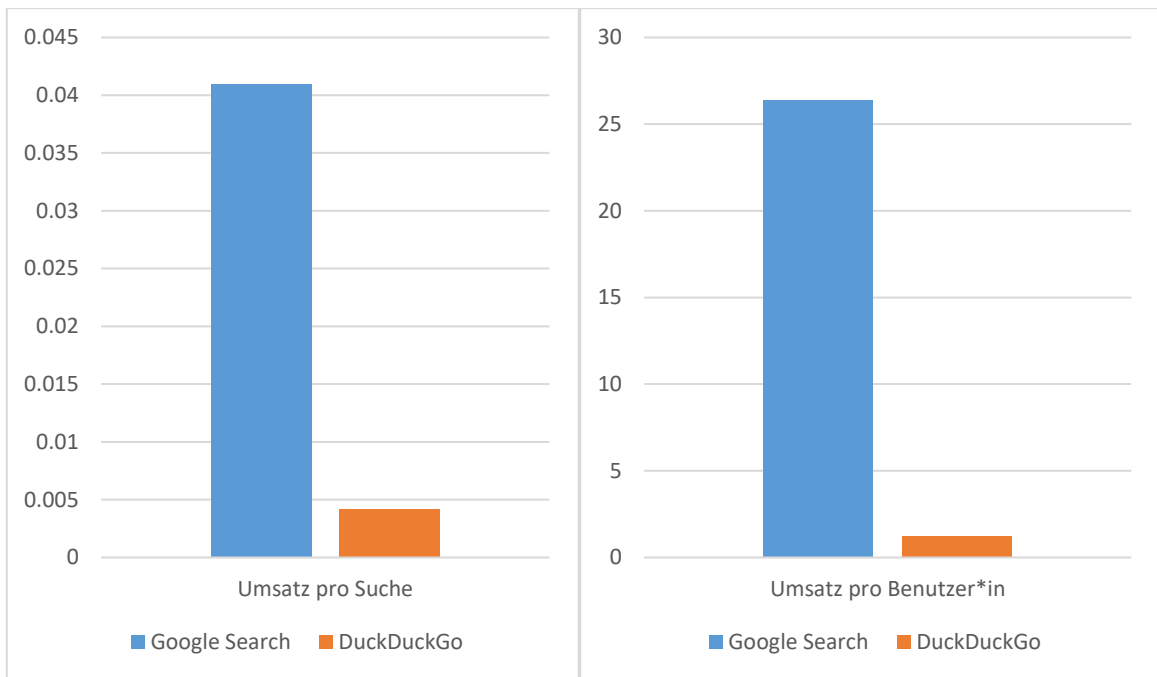
³⁶ Vgl. (DuckDuckGo, 2021)

³⁷ Vgl. (DuckDuckGo, 2021)

³⁸ Vgl. (Statista, 2021)

³⁹ Vgl. (99firms, 2021)

⁴⁰ Vgl. (Statista, 2021)



6. Fazit

Die Auswirkungen von Dark Patterns sind vielschichtig und für jedes Unternehmen unterschiedlich. Dennoch ist das Ergebnis dieser Untersuchung klar: Die Auswirkungen von Dark Patterns sind vor allem finanzieller Natur. Dark Patterns ermöglichen es einem Unternehmen durch die Ausnutzung menschlichen Verhaltens mehr Daten zu sammeln und ein Vielfaches des Umsatzes zu generieren, den es ohne Dark Pattern einfahren würde. Zum Zeitpunkt des Verfassens dieses Fazits überwiegen die finanziellen Vorteile von Dark Pattern den Nachteilen bei weitem. Seltene Klagen, in Relation zum Umsatz gesehen geringe Strafen und schleppende oder nicht vorhandene Gesetzesänderungen begünstigen das Verwenden von Dark Pattern. Das Kundenvertrauen ist das einzige, dass ein Unternehmen auf lange Sicht schaden könnte. Gleichzeitig sehen aber viele Kunden dieses Verhalten als notwendiges Übel, da aus ihrer Sicht die Vorteile, und nicht die Risiken, überwiegen.⁴¹ In Zukunft werden Dark Pattern aber immer kostspieliger und öffentlich sichtbarer werden, was zu ernsthaften Kundenverlusten und Image Schäden führen könnte.

Deswegen sollten Unternehmen schon heute damit beginnen, über das Entfernen von Dark Patterns aus ihren Praktiken nachzudenken.

⁴¹ (Mildner & Savino, 2021)

Literaturverzeichnis

- Amazee Metrics Ltd. (2021, 05 24). *76% Ignore Cookie Banners – The User Behavior After 30 Days of GDPR*. Retrieved from Amazee Metrics: www.amazeemetrics.com
- Brignull, H. (2021, 05 24). *Expert witness in dark patterns - testimonium.co*. Retrieved from testimonium.co: testimonium.co
- Brignull, H. (2010). *Dark Patterns - UX Brighthon 2010* [Recorded by H. Brignull]. Brighton, East Sussex, United Kingdom.
- Hartzog, W. (2018). *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Cambridge: Havard University Press.
- Weinmann, M., Schneider, C., & vom Brocke, J. (2021, 04 21). *Springer Link*. Retrieved from Digital Nudging | Springer Link: <https://link.springer.com/article/10.1007/s12599-016-0453-1>
- Forbruker Rådet. (2021, 04 20). *forbrukerrådet*. Retrieved from <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf>
- Johnson, E. J., & Goldstein, D. (2021, 05 25). *SSRN*. Retrieved from Do Defaults Safe Lives? by Eric J. Johnson and Daniel G. Goldstein :: SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1324774
- U.S. General Services Administration . (2021, 05 27). *User-Centered Design Basics | usability.gov*. Retrieved from [usability.gov](https://www.usability.gov/what-and-why/user-centered-design.html): <https://www.usability.gov/what-and-why/user-centered-design.html>
- Acquisti, A., Adjerid, I., Belabako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., . . . Wilson, S. (2017). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys*, 44:1 - 44:41.
- Bansal, G., & Zahedi, F. M. (2015). Trust violation and repair: The information privacy perspective. *Decision Support Systems*, 62-77.
- Brignull, H. (2020, 05 20). *Dark Patterns - About Us* . Retrieved from Dark Patterns: www.darkpatterns.org
- Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018, 04 21-26). *ACM Digital Library*. Retrieved from *The Dark (Patterns) Side of UX Design*: <https://dl.acm.org/doi/pdf/10.1145/3173574.3174108>
- Tian, Y., Hung, C., & Frumkin, P. (2020). An experimental test of the impact of corporate social responsibility on consumers' purchasing behavior: The mediation role of trust. *Corporate Social Responsibility and Environmental Management*, 2972-2982.
- Laziuk, E. (2021, 07 10). *96% of US users opt out of app tracking in iOS 14.5, analytics find*. Retrieved from [flurry.com](https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/): <https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparency-worldwide-us-daily-latest-update/>
- Edelman. (2020). *Edelman Trust Barometer 2020*. Edelman.
- Statista. (2021, 06 20). *Google: ad revenue 2001-2018 | Statista*. Retrieved from [statista.com](https://www.statista.com/statistics/266249/advertising-revenue-of-google/): <https://www.statista.com/statistics/266249/advertising-revenue-of-google/>

- Petrov, C. (2021, 06 20). *The most Fascinating Google Search Statistics*. Retrieved from techjury.net: <https://techjury.net/blog/google-search-statistics/#gref>
- Steinberg, D. (2021, 06 20). *The World is Worried About Data Privacy. Is DuckDuckGo the Answer?* Retrieved from Pillymag.com: <https://www.phillymag.com/news/2021/02/20/duckduckgo-data-privacy-paoli/>
- DuckDuckGo. (2021, 06 20). *DuckDuckGo Traffic*. Retrieved from duckduckgo.com: <https://duckduckgo.com/traffic>
- DuckDuckGo. (2021, 06 20). *How Many People Use DuckDuckGo?* Retrieved from spreadprivacy.com: <https://spreadprivacy.com/how-many-people-use-duckduckgo/>
- Statista. (2021, 06 20). *Worldwide Internet Users by Region 2020*. Retrieved from Statista.com: <https://www.statista.com/statistics/265147/number-of-worldwide-internet-users-by-region/>
- 99firms. (2021, 06 20). *Search Engine Statistics 2021 - 99firms*. Retrieved from 99firms.com: <https://99firms.com/blog/search-engine-statistics/>
- Statista. (2021, 06 20). *Search engine market share worldwide | statista*. Retrieved from statista.com: <https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines/>
- Brownlee, J. (2021, 06 21). *After Lawsuit Settlement, LinkedIn's Dishonest Design Is Now A \$13 Mil.* Retrieved from fastcompany.com: <https://www.fastcompany.com/3051906/after-lawsuit-settlement-linkedins-dishonest-design-is-now-a-13-million-problem>
- Davis, J. (2021, 06 21). *Google to face \$5bn privacy lawsuit as consumer craving for secrecy increases*. Retrieved from telecoms.com: <https://telecoms.com/504758/google-to-face-5bn-privacy-lawsuit-as-consumer-craving-for-secrecy-increases/>
- Vincent, J. (2021, 06 02). *California bans 'dark patterns' that trick users into giving away their personal data - The Verge*. Retrieved from theverge.com: <https://www.theverge.com/2021/3/16/22333506/california-bans-dark-patterns-opt-out-selling-data>
- Kellogg, S. (2021, 07 15). *How US, EU approach regulating 'dark patterns'*. Retrieved from iapp.org: <https://iapp.org/news/a/ongoing-dark-pattern-regulation/>
- Opensecrets. (2021, 06 22). *Alphabet Inc. Lobbying Profile* • opensecrets.org. Retrieved from opensecrets.org: <https://www.opensecrets.org/federal-lobbying/clients/summary?cycle=2020&id=D000067823>
- Mildner, T., & Savino, G.-L. (2021). *Ethical User Interfaces: Exploring the Effects of Dark Patterns on Facebook*. Bremen: University Of Bremen.