

# Design for Privacy – mit dem Menschen gestalten.

Michael Bechinie<sup>1</sup>, Markus Murtinger<sup>2</sup>, Manfred Tscheligi<sup>3</sup>

Head of Experience Design, USECON - Experience Design & Consulting<sup>1</sup>

Director Consulting, Sales & Marketing, USECON - Experience Design & Consulting<sup>2</sup>

Geschäftsführung, USECON - Experience Design & Consulting<sup>3</sup>

## Zusammenfassung

Der aktuelle Markt zeigt, dass Kunden attraktive Produkte mit Begriffen wie einfach, klar, intelligent und brauchbar umschreiben. Kurz gesagt: Technologie, die nur „funktioniert“ ist kein Verkaufsargument mehr. Digitale Märkte konkurrieren um Kunden, gerechnet wird mit der „Währung Benutzerdaten“. Um an den größten Anteil des „neuen Geldes“ zu kommen, spekulieren Unternehmen damit wie Menschen „ticken“. „Wir finden nicht heraus, wie Dinge funktionieren. Wir wursteln uns durch“ (S. Krug). Das trifft im Grunde noch immer auf das Interaktionsverhalten von Menschen im Umfeld technischer Anwendungen zu. Speziell bei Design für Privacy und Security geht es um die Herausforderung, Interaktionen mit Produkten und Services zu gestalten, ohne Menschen dabei zu „überlisten“. Der Beitrag fokussiert auf pragmatische Prinzipien und geht zusätzlich auf erste Ergebnisse aus dem EU Forschungsprojekt „Privacy&Us“ ein.

## 1 Unternehmen sind keine Samariter

Ein Blick in die Privacy Policies bekannter Anbieter von Webservices, wie z. B. Facebook, Google etc. genügt um festzustellen, dass die noch immer sehr umfangreichen Texte von Anwälten für Anwälte geschrieben sind. Für Benutzer ist es nach wie vor schwierig die umfangreichen Konsequenzen der Zustimmung abzuschätzen. So bleiben oft nur die Alternativen: (1) „Rasch zum Ende scrollen und einfach zustimmen“ oder (2) das Service nicht zu nutzen. Die meisten Benutzer entscheiden sich wohl für (1) „Scrollen, zustimmen“. Die Beobachtung von Steve Krug „Wir finden nicht heraus, wie Dinge funktionieren. Wir wursteln uns durch“ (Krug, 2014) trifft noch immer auf das Verhalten von Benutzern im Web zu. Als Gestalter von Services, Prozessen, und konkreten Interaktionen mit interaktiven Systemen liegt dort die Herausforderung. Das gilt im Besondern auch bei der Gestaltung im Umfeld von Privatsphäre (Privacy) und Sicherheit gespeicherter Information (Security).

Wenn Benutzer zu Kunden werden, suchen diese nach attraktiven Produkten und Services, die sich im 21. Jahrhundert mit Begriffen wie einfach, klar, intelligent und brauchbar umschreiben lassen. Wenn sich technologische Produkte und Services im Massenmarkt erfolgreich bewegen wollen, müssen Kunden ihre Bedürfnisse erfüllt sehen. Besonders im technologischen Produktumfeld gilt: Technologie, die „nur funktioniert“ ist kein Verkaufsargument mehr, sie muss für Menschen auch passen.

## 2 Benutzer als Ware

Die Bandbreite digitaler B2C Geschäftsmodelle geht von reinen Bezahlservices über Freemium Modelle bis hin zur (vordergründig) kostenfreien Nutzung durch die Endkunden. Im stetig wachsenden Feld der eGovernment und eHealth Services nimmt die Sicherheit von gespeicherter Information (Security) und die Regulierung von Privatsphäre (Privacy) einen noch größeren Stellenwert ein. Die Möglichkeiten reichen vom einfachen Reispass-Antrag über die Verwaltung medizinischer oder sozialversicherungsrelevanter Daten bis zum eVoting. Auch auf der B2B Seite werden inzwischen gesamte Wirtschaftszweige mit Themen wie IoT und Cyber Physikalische Systeme in der Cloud abgebildet. Der Mensch ist auch hier Teil der Kette; Daten von Mitarbeitern sind potentielle Quellen um Unternehmensprozesse zu optimieren.

Ein Standardmodell des digitalen Geschäfts im B2C ist die Erwartung, Webservices kostenfrei nutzen zu können. Kunden wollen für Services, wie z.B. Web Mailer, online Office Anwendungen, Social Media Plattformen etc. kein Geld ausgeben; bis zur kompletten Smart Home Lösung mit einer Vielzahl an Daten, die erfasst und analysiert werden (können). „Bezahlen“ müssen Kunden trotzdem und werden damit zur „Ware Benutzer“. Die Währung in der bezahlt wird ist die Bekanntgabe mehr oder weniger umfangreicher, persönlicher Daten und generierter Inhalte, wie Bilder, Texte, Postings und Nutzungsdaten.

## 3 Verloren in Regularien

Die rechtliche Basis dafür wird durch die Zustimmung der Benutzer zu den Bedingungen des Anbieters geschaffen. In den „Policies“ der Anbieter sind Aspekte der Privatsphäre bzw. des Datenschutzes und meist auch der Nutzungsrechte des Anbieters für benutzergenerierte Inhalte geregelt. Den Services zu Grunde liegende Richtlinien, die Privacy und Security regeln sollen, sind durch die globalisierte Businesswelt für den Anwender vollumfänglich kaum zu durchschauen. Wo liegen meine Daten? Welches Recht gilt? Welche Rechte, aber auch Pflichten habe ich?

Durch die neue EU Datenschutz-Grundverordnung (European Parliament, 2016) sollen ab 2018 personenbezogen Daten besser geschützt werden. Das Verständnis und die konkrete Umsetzung der Verordnung gestalten sich jedoch schwierig. Die EU Datenschutz-Grundverordnung macht an vielen Stellen auch konkrete Vorgaben, z. B. Stelle (42): „[dass] ...eine vom

Verantwortlichen vorformulierte Einwilligungserklärung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden [soll], und sie [...] keine missbräuchlichen Klauseln beinhalten [soll].“ (European Parliament, 2016). Die Verordnung beinhaltet auch Gestaltungs-Hinweise zur Unterstützung der Verständlichkeit, z. B. Stelle (60): „Die betreffenden Informationen können in Kombination mit standardisierten Bildsymbolen bereitgestellt werden, um in leicht wahrnehmbarer, verständlicher und klar nachvollziehbarer Form einen aussagekräftigen Überblick über die beabsichtigte Verarbeitung zu vermitteln.“ (European Parliament, 2016).

## 4 Der Weg aus der Petersilie?

Anbieter machen sich jedoch noch selten Gedanken und die Mühe, Benutzer an diesem wichtigen Punkt zu unterstützen. Provokant behauptet rechnen Unternehmen vielmehr damit, wie Menschen „ticken“ (z. B. lesen Menschen keine langen Texte im Web), um an den größten Anteil des „neuen Geldes“ zu kommen. Für Gestalter interaktiver Systeme gilt es, sowohl zwischen den Interessen der Anbieter bzw. Anwender und etwaigen gesetzlichen Vorgaben die Balance zu finden. Als Gestalter ist es dabei weder das Ziel auf der „Dunklen Seite der Macht“ zu landen, und Menschen mit Design-Patterns zu für sie unvorteilhaften (und für die Anbieter sehr vorteilhaften) Entscheidungen und Aktionen zu „verführen“, noch sie mit völlig korrekten aber umständlichen Design-Patterns „Mitten in die Petersilie“ zu führen. Als Gestalter digitaler Interaktionsprozesse müssen wir uns folgende Fragen stellen:

- Was können wir dazu beitragen, dass sich Anwender an wesentlichen Punkten der Systemnutzung zentrale Fragen stellen und diese nicht als lästig empfinden: Wem gebe ich Zugriff auf welche Daten, wofür, wie lange?
- Von welchen Vorgehensweisen und Richtlinien können wir uns im Gestaltungsprozess leiten lassen, speziell in den Bereichen Privacy (und Security)?

Ein statistisches Abbild der Internetnutzer aus dem Jahr 2017 bietet einen guten Ausgangspunkt für die Begründung von ganz generellen Designentscheidungen für interaktive Anwendungen (Abbildung 1). Rund 50% der Weltbevölkerung sind online, der größte Anteil am Internetverkehr wird von Benutzern mit mobilen Endgeräten generiert. Social Media Services werden von knapp 40% der Weltbevölkerung aktiv genutzt. Andere Zahlen belegen Limitationen, die Menschen stark an der aktiven Internetnutzung hindern. Mehr als 15% haben Defizite in der Alphabetisierung, knapp 4 von 100 Menschen haben Scheinschränkungen und die Hälfte des verfügbaren Inhaltes im Web sind nur in englischer Sprache vorhanden, obwohl Englisch nur von rund 5% der Weltbevölkerung gesprochen wird – ein beträchtliches Missverhältnis.

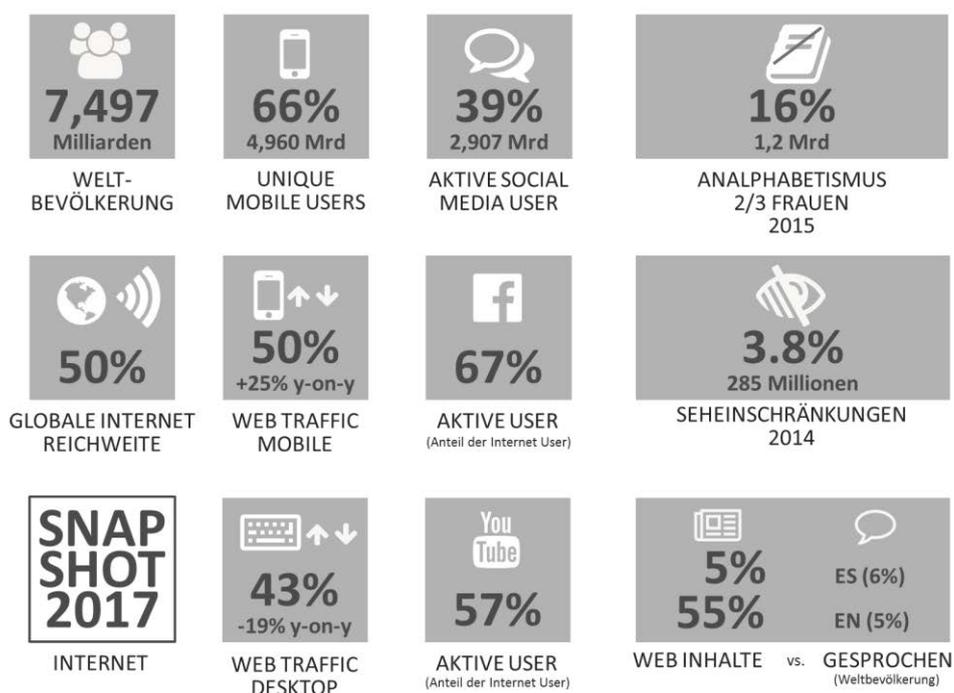


Abbildung 1: Charakterisierung der Internetbevölkerung. Web Inhalte (Dupere, 2015), Internet Statistik (Kemp, 2017), Analphabetismus (WHO, 2015), Seheinschränkungen (WHO, 2014)

Aktuelle Daten zu jährlichen Zuwachsraten von Downloads mobiler Anwendung (Apps) zeigen, dass die Kategorien „Messaging und Social“ mit 44% den Spitzenplatz einnehmen (Statista 2017). Gerade im Messaging wurde die Möglichkeit sich selbst auszudrücken durch die Nutzung mobiler Endgeräte stark gefördert. Die Ausdrucksmöglichkeiten reichen von den durch Apple 2011 eingeführten Emojis bis hin zu den „Lenses“ von Snapchat (Meeker, 2016). Durch verbesserte Kamerahardware aktueller Smartphones und passende Social Media Plattformen hat sich das Volumen geteilter Bilder und Videos in den Jahren 2013 bis 2015 verdreifacht; von rund 1 auf 3 Milliarden Bildern pro Tag (Meeker, 2016). Zusammengefasst ergibt sich folgende Charakterisierung der aktuellen Internet Nutzung:

- Die digitale Kluft nimmt langsam ab, weiterhin gibt es große Hürden in der „leichten und verständlichen“ Nutzung von Webinhalten
- Das Internet ist vorrangig „Mobil und Sozial“
- Englisch dominiert die geschriebenen Inhalte im Internet
- Selbstdarstellung und Kommunikation mit Bildern / Videos haben stark zugenommen

Besonders der letzte Aspekt, liefert einen wesentlichen Anhaltspunkt in Richtung „brauchbares“ Design for Privacy. Der Mensch, als hoch soziales Wesen, definiert sich vielmehr über Konversationen, als über einseitig ausgerichtete Kommunikation ohne „Rückkanal“.

## 5 Privacy in der Designkrise

Um die Datenbasis für mögliche Design-Ansätze im Bereich Privacy weiter zu verbreitern, ist es hilfreich einen Blick drauf zu werfen, wie es um Einstellungen und Verhalten von Benutzern in Sachen Vertrauen in Anbieter, Erfahrungen mit Cybersecurity und Maßnahmen zur Schutz der Privatsphäre steht. Eine Studie von Pew Research aus 2016 zeigt, dass rund 50% der amerikanischen Bevölkerung weder der Regierung noch den Social Media Anbietern zutrauen, ihre persönlichen Daten entsprechend schützen zu können. 64% der Befragten gaben an, Opfer eines Diebstahls persönlicher Daten gewesen zu sein (z.B. Kreditkartenbetrug, Fremdzugriff auf Emails und Social Media Account, Missbrauch von Sozialversicherungsdaten bzw. Steuerkonto).

Wissen zu unterschiedlichen Konzepten und Begriffen bzw. Maßnahmen, die Benutzer im Umfeld der Datensicherheit ergreifen könnten (z.B. Verschlüsselung von Emails, WLAN Sicherheit, Mehrschritt Authentifizierung) sind teilweise unbekannt bzw. mit falschen Vorstellungen belegt. Benutzer ergreifen laut Studie auch kaum (sichere) Maßnahmen um ihre Passworte zu schützen. Mehr als 85% geben an, sich Passworte zu merken, 50% schreiben diese auf Papier und nur knapp über 10% verwenden ein Passwortmanagement Programm. Schließlich verwenden mehr als 25% der Befragten keinen Screenlock bei ihren Smartphones. Zusammenfassend zeichnet sich ein düsteres, wenn auch realistisches Bild der Internetbenutzer, in Bezug auf die Themen Privacy und Security. Menschen...

- haben geringes Vertrauen in Datensicherheit öffentlicher wie kommerzieller Anbieter,
- haben die eine oder andere Form des Datendiebstahls selbst erlebt,
- haben geringes bzw. falsches Wissen rund um das Thema Cybersecurity und
- sind nachlässig in Sachen Passwortschutz.

Aus den zuvor beschriebenen, unterschiedlichen Charakteristika der Internet Nutzung lässt sich ableiten, dass wir aus Sicht des Experience Designs in einer Designkrise stecken. Aktuelle Designlösungen kommen, wenn es um den Schutz der Privatsphäre im Internet geht, den Menschen nicht entgegen. Meist sind die Lösungen unverständlich und zu kompliziert und (ver)föhren zu, für den Menschen, unvorteilhaften Verhaltensmustern im Internet.

Erschwert wird die Situation auch durch vermeintliche Design-Dilemmas. In letzten 20 Jahren hatten sich die unterschiedlichen Mitspieler der User Experience Community von allen Seiten (IT, wie Design und Business) Gefechte geliefert in denen es sich darum drehte, ob Konzepte mit einander vereinbar sind, oder nicht. Vor 20 Jahren ging es darum, ob Usability technisch schwer umsetzbar ist. Vor 15 Jahren wurde gestritten, ob benutzbare Systeme nur „hässlich“ sein können. Vor 10 Jahren wurde debattiert, dass Usability und Barrierefreiheit einander widersprechen. Um nicht Gefahr zu laufen, einem weiteren Paradigmenstreit zu folgen, ob sich

Privacy (bzw. Security) und Usability mit brauchbaren Designlösungen harmonisieren lassen, ist es notwendig sich auch diesem scheinbaren Design-Dilemma „radikal“ mit dem Human Centred Design Ansatz zu nähern. Sollen Menschen Konsequenzen verstehen und nachvollziehen können, die durch ihre Wahl von Privacy Einstellungen bzw. durch ihre Zustimmung zu Nutzungsbedingungen entstehen, braucht es für die Entwicklung entsprechender Designlösungen auch hier alle Phasen des iterativen Human Centred Design Prozesses (ISO, 2010) bzw. entsprechende Human Computer Interaction (HCI) Maßnahmen (Karat, Brodi, & Karat, 2005):

- Nutzungskontext verstehen und beschreiben
- Nutzungsanforderungen spezifizieren
- Gestaltungslösungen entwerfen
- Gestaltungslösungen aus der Benutzerperspektive evaluieren

## 6 Design mit Hilfe von Heuristiken

Die Ergebnisse eines richtig verstandenen, menschenzentrierten Designprozesses beschränken sich nicht auf kosmetischen Aktionismus. Design soll vielmehr Sinn stiften, besonders wenn es um sensible Bereiche, wie die Privatsphäre von Menschen geht. Das schließt auch Menschen ein, die Schwierigkeiten haben komplexere Inhalte erfassen und verstehen bzw. Konsequenzen ihres Internet-Verhaltens abschätzen zu können. Klaus Krippendorff spricht von einer (notwendigen) semantischen Wende im Design und definiert Design als Prozess der Sinngebung: „Design is making sense of things“ (Krippendorff, 2005). Für die Vermittlung zwischen Artefakt und Mensch sind Interfaces notwendig. Bonsiepe spricht von einem Interface am Schnittpunkt von Benutzer, Aufgabe und Werkzeug (Bonsiepe, 1996). Sinn erhält Design dann, wenn Benutzer in der gestalteten Interaktion die Bedeutung für sich erkennen können. Bedeutung im Zusammenhang mit Privacy heisst auch Konsequenzen des eigenen Handelns abschätzen zu können. Letztlich sollen Benutzer ihr Ziel effektiv, effizient und zufriedenstellend durch die Interaktion erreichen können; Usability muss eine Basisqualität sein, auch im Umfeld von Privacy und Security.

Gute Design Entscheidungen bauen daher auf einem Grundlagenverständnis von menschlichem Verhalten, Wahrnehmungs- und Emotions-Prozessen bzw. anerkannten Designrichtlinien auf. Vorallem bei fachlich komplexen Materien hilft es Menschen, die Entscheidungen treffen müssen (z. B. wenn sie Privacy Einstellungen für genutzte online Services anpassen oder die Konsequenzen einer geänderten Privacy Policy verstehen sollen), wenn das Interaktionsdesign eine „menschliche Passung“ hat. Sowohl Menschen als auch Design arbeiten mit Heuristiken (grobe Annahmen bzw. Erfahrungswerte) um „good enough“ Lösungen zu erreichen.

- *Menschliche Heuristiken*: Verhalten, Emotion, Denkmechanismen für ein Verständnis darüber, warum wir uns „durchwursteln“ anstatt rational und klar vorzugehen.

- *Design Heuristiken*: Prinzipien, die Gestalter bei Fragestellungen im Design der Mensch-System Interaktion unterstützen (z.B. bei Feedback Mechanismen, Visualisierungen, Bezeichnungen etc.)

*Ein Beispiel für eine menschliche Heuristik: Menschen sind hoch soziale Primaten.* Im Laufe der Evolution haben sich nicht nur unsere physischen Merkmale sondern auch unsere psychologisch Mechanismen verändert, und tun dies auch weiterhin. Nach gängigen Theorien zur Evolution menschlichen Verhaltens haben wir Strategien entwickelt unsere genetische Fitness zu optimieren, die auch altruistisches Verhalten mit Fremden miteinschließt. Laut Studien des Primatologen Robert Dunbar (Dunbar, Marriott, & Duncan, 1997) sind wir geradezu „süchtig“ nach sozialen Themen, die den größten Anteil (rund 70%) in täglichen Gesprächen ausmachen, und unser Zusammenleben stark prägen. In diesem Aspekt ergibt sich eine klare Auswirkung auf die Entwicklung von Designlösungen: Menschen sind gut im (wieder) erkennen von Gesprächspartner und erinnern sich an vergangene, soziale Interaktionen. In Folge sind sie empfindlich gegenüber Betrugern und Vertrauen in der Kommunikation stellt einen wesentlichen Faktor stabiler Sozialnetze da. Die Aufmerksamkeit im Designprozess muss daher weg vom einzelnen Artefakt hin zur Konversation verschoben werden. Wenn es um sensible Bereiche, wie die eigene Privatsphäre (Privacy) geht, erwarten Menschen, dass sich z. B. der Social Media Anbieter in einen Gesprächsmodus mit dem Benutzer begibt. Ziel der Konversation muss sein, Vertrauen zwischen den Dialogpartnern schrittweise aufzubauen. Die Entscheidung bei der Freigabe von persönlichen Daten muss dabei in der Hand der Benutzer liegen, bzw. kooperativ „verhandelt“ werden (wenn Du MIR das gibst, bekommst DU das dafür) statt sich Freigaben betrügerisch durch intransparente User Interfaces zu erschleichen.

*Ein weiteres Beispiel einer menschliche Heuristik: Menschen werden, wenn sie Entscheidungen treffen immer von Emotionen geleitet.* Je nach Theorie können das sein:

- *Affektbedingte Basiskreisläufe* wie z.B. SPIEL, PANIK, ANGST, WUT, PFLEGE, LUST oder SUCHEN (Panksepp & Biven, 2012)
- *Kernaffekte*, die als unreflektierte neurophysiologische Zustände empfunden werden, und sich zwischen angenehm / unangenehm bzw. aktiviert / inaktiviert bewegen (Russell, 2003)

Erst in zweiter Linie kommt ein weiteres System bei der Entscheidungsfindung zum Zug, das uns dabei unterstützt kontrolliert und bewusst zu handeln bzw. regelbasiert und schlussfolgernd vorzugehen. Die beiden Systeme sind besser bekannt als: System 1 (automatisch, schnell) und System 2 (reflektierend, langsam). Das Grundproblem, das sich daraus ableiten lässt, haben Daniel Kahneman und Amos Tversky in vielfachen Studien beschrieben (Kahneman, 2011): Menschen haben zu großes Vertrauen in ihr eigenes Urteilsvermögen. Die Folgen sind, dass Menschen schwierige Fragen durch leichte ersetzen, voreilige Schlussfolgerungen aufgrund unvollständiger Informationen ziehen, Probleme isoliert betrachten bzw. durch „framing“ Entscheidungen stark beeinflusst werden können. Auch in diesem Aspekt ergibt sich eine klare Auswirkung auf die Entwicklungen von Designlösungen: Komplexe Sachverhalte wie sie bei Einstellung von Privacy Optionen oder Policies bzw. deren Konsequenzen vorkommen, werden vorerst von System 1 und dann von 2 „bearbeitet“ und letztendlich unzureichend vom Benutzer entschieden. Neutraler Boden ist in diesem Bereich schwer

zu finden, der die Interessen des Anbieters (Geschäft machen) mit denen des Benutzers (Privatsphäre bewahren) ausreichend balanciert. Zumindest „faire“ Grundeinstellungen muss ein Benutzer jedoch erwarten können, bzw. ein Mindestmaß an Nachvollziehbarkeit der Konsequenzen, wenn die Einstellungen geändert werden. An diesem Punkt wird die heikle Aufgabe des Gestalters besonders klar, nicht auf die „Dunkle Seite der Macht“ zu wechseln und nur System 1 anzusprechen, was klar zum Vorteil des Anbieters ausgehen würde.

Weitere Hilfestellung findet der Gestalter bei generellen Usability Prinzipien, wie z. B. bei den für UX Professionals hinreichend bekannten Design Heuristiken (Nielsen, 1994) und auch den Design Guidelines, die auf der Kenntnis kognitiver Psychologie (Wahrnehmung, Gedächtnis, Lernen, etc.) aufbauen (Johnson, 2014). Stellvertretend sei vor allem auf zwei Heuristiken verwiesen, die für die Thematik Design for Privacy besonders wichtig erscheinen:

- *Übereinstimmung des Systems mit der realen Nutzerwelt*: Das System sollte die Sprache des Nutzers verwenden, mit Wörtern, Phrasen und Konzepten ähnlich denen der Nutzer, anstelle von systemorientierten Bezeichnungen. Folge den Gepflogenheiten der „realen Welt“ und stelle Informationen als natürlich / logische Abfolge dar.
- *Kontrolle und Freiheitsgrad für Benutzer*: Nutzer verwenden Systemfunktionen oft irrtümlich und benötigen daher einen klar erkennbaren „Notausgang“, um den ungewollten Stand ohne einen erweiterten Dialog verlassen zu können.

Beide Heuristiken geben Gestaltern gute Anhaltspunkte, Charakteristiken menschlichen Verhaltens und Handelns in Designlösungen zu berücksichtigen: das mentale Modell der Benutzer, was ein Anbieter mit meinen freigegeben Daten darf und nicht darf, welche Abhängigkeiten bzw. Zusammenhänge bestehen, muss sich im Design widerspiegeln und der Benutzer muss die Möglichkeit haben die Kontrolle zu behalten.

## 7 Forschung hilft der Praxis

Technische Aspekte von Privacy und Security sind vielfach Gegenstand sowohl akademischer als auch industrieller Forschungsprojekte. Seit ca 10 Jahren hat sich jedoch eine wachsende Community etabliert, die vorallem Forschungsfragen an den Schnittpunkten Usability, Design und Privacy bearbeitet. Ein aktuelles EU Projekt, „Privacy&Us“ (Innovative Training Network), an dem die Autoren beteiligt sind, untersucht in 13 Dissertationsprojekten unterschiedlichste Aspekte von Privacy und Usability. Durch die Vielfalt der untersuchten Themengebiete ergibt sich die Möglichkeit Erkenntnisse aus unterschiedlichsten Bereich zu konsolidieren. Die Projekte untersuchen Themen wie: Usable Transparency Enhancing Tools (TETs), Beeinflussung persönlicher Einstellungen zu Privacy, NFC Zahlungsmethoden, Smartphone Ökosysteme, IoT, Sealed Cloud Anwendungen, Entscheidungsprozessen von Benutzern, Personal Genomic Testing, Healthcare Data, Verhaltensökonomische Aspekte oder Authentifizierung von Transaktionen. Die Projekte werden dabei in enger Kooperation zwischen Universitäten, Interessensvertretungen und Unternehmen durchgeführt. Erste, vorläufige Ergebnisse zeigen:

- alle Projekte bzw. Researcher profitieren vom Austausch zwischen „academics und business“ wenn es um die Erforschung von Privacy, Design und Usability geht
- der Human Centred Design (HCD) Prozess bietet auch in diesem Forschungsfeld ein ideales Rahmenwerk für die Bearbeitung angewandter Forschungsfragen
- die Entwicklung und empirische Validierung von Vorhersagemodellen für Privacy bezogenes Benutzerverhalten bietet eine gute theoretische Grundlage für die Entwicklung modellbasierter Guidelines die Gestalter unterstützen sollen
- klassische Design Heuristiken bieten nachwievor ein gutes Rahmenmodell für die Entwicklung Privacy bezogener high-level User Interface Requirements in ganz unterschiedlichen Anwendungsfeldern

## 8 Design for Privacy: Vier Imperative

Design for Privacy soll als Design mit dem Menschen und nicht für den Menschen verstanden werden, in dem der Mensch nicht als Objekt sondern als Mitgestalter gesehen wird. Als starke Design Leitlinien können zusammenfassend folgende, vier Imperative formuliert werden:

- *Methodischer Imperativ*: Folge deinen Benutzern, nicht der Theorie über DIE Benutzer, um sie zu verstehen.<sup>1</sup>
- *Design Imperativ*: Definiere WAS Menschen erwarten und benötigen; abhängig von der Situation, dem WANN und WARUM.
- *Semantischer Imperativ*: Gestalte mit dem Menschen, nicht für den Menschen, um „Sinn zu konstituieren.“<sup>2</sup>
- *Ethischer Imperativ*: Stelle solche Interaktions-Lösungen zur Verfügung die die Entscheidungsmöglichkeiten für Menschen erhöhen.<sup>3</sup>

## Danksagung

Die Erstellung dieses Beitrags wurde durch Fördermittel des H2020 Forschungs- und Innovationsprogramms der Europäischen Union unterstützt: Marie Skłodowska-Curie Innovative Training Networks „Privacy&Us“ (grant agreement No 675730) [http://cordis.europa.eu/project/rcn/198304\\_en.html](http://cordis.europa.eu/project/rcn/198304_en.html)

---

<sup>1</sup> Nach William Charlesworth „Follow the duck, not the theory of the duck.“ (Lafreniere, 2002)

<sup>2</sup> Nach Klaus Krippendorff (Krippendorff, 2005)

<sup>3</sup> Nach Heinz von Förster (von Foerster, 2001) „On Constructing Reality“

## Literaturverzeichnis

- Bonsiepe, G. (1996). *Interface. Design neu begreifen* (1st ed.). Mannheim: Bollmann.
- Dunbar, R. I. M., Marriott, A., & Duncan, N. D. C. (1997). Human conversational behavior. *Human Nature*, 8(3), 231–246. <https://doi.org/10.1007/BF02912493>
- Dupere, K. (2015). English is strangling other languages on the Internet. Retrieved July 6, 2017, from <http://mashable.com/2015/12/12/english-strangling-internet-languages/#erf8O5ADUEqm>
- European Parliament. (2016). General Data Protection Regulation (Datenschutz-Grundverordnung). *Official Journal of the European Union*, 11(April), 1–260. Retrieved from <http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/de/pdf>
- ISO. (2010). *DIN-EN/ISO 9241:210 Prozess zur Gestaltung gebrauchstauglicher interaktiver Systeme*. ISO.
- Johnson, J. (2014). *Designing with the Mind in Mind* (2nd ed.). Waltham: Morgan Kaufmann.
- Kahneman, D. (2011). *Thinking, Fast and Slow* (1st ed.). New York, NY, USA: Farrar, Straus and Giroux.
- Karat, C. M., Brodi, C., & Karat, J. (2005). Usability Design and Evaluation for Privacy and Security Solutions. In *Security and Usability - Designing Secure Systems that People Can Use* (pp. 47–74).
- Kemp, S. (2017). *Q2 2017 GLOBAL DIGITAL STATSHOT*.
- Krippendorff, K. (2005). *The Semantic Turn: A New Foundation for Design*. CRC Press.
- Krug, S. (2014). *Don't Make Me Think - A Common Sense Approach To Web Usability* (3rd ed.). New Riders Press.
- Lafreniere, P. (2002). Follow the Duck, Not Your Theory of the Duck. *Human Ethology Bulletin*, 17(2), 9–12.
- Meeker, M. (2016). *Internet Trends 2016 - Code Conference*. Retrieved from <http://www.kpcb.com/InternetTrends>
- Nielsen, J. (1994). Heuristic Evaluation. In *Usability Inspection Methods* (pp. 25–62). <https://doi.org/10.1089/tmj.2010.0114>
- Panksepp, J., & Biven, L. (2012). *The Archaeology of Mind*. W. W. Norton & Company.
- Russell, J. A. (2003). Core affect and the psychological construction of emotion. *Psychological Review*, 110(1), 145–72. <https://doi.org/10.1037/0033-295X.110.1.145>
- von Foerster, H. (2001). *Understanding Understanding Essays on Cybernetics and Cognition*. New York, NY, USA: Spinger.
- WHO. (2014). Visual impairment and blindness. Retrieved July 6, 2017, from <http://www.who.int/mediacentre/factsheets/fs282/en/>

WHO. (2015). *World health statistics 2015*. [https://doi.org/ISBN 978 92 4 156525 7](https://doi.org/ISBN%20978%2092%204%20156525%207)

## Autoren



**Bechinie, Michael (bechinie@usecon.com)**

Studium der Anthropologie (Universität Wien). Head of Experience Design bei der USECON GmbH. Mehr als 15 Jahre Erfahrung im Bereich Usability / User Experience / User Interface Design. Themen: Management, Durchführung von Experience Design Projekten im Umfeld B2C, B2B Anwendung, User Interface Style Guide Entwicklung, Usability Trainings. Support von Bachelor, Master und PhD Arbeiten im Usability Umfeld.



**Murtinger, Markus (murtinger@usecon.com)**

Studium der Betriebswirtschaft (Wirtschaftsuniversität Wien) mit dem Fokus Entrepreneurship & Innovation, Marketing sowie Tourismus & Freizeitforschung. Director Consulting, Sales & Marketing bei der USECON GmbH. Mehr als 10 Jahre Erfahrung im Bereich Usability & User Experience. Themen: strategisches User Experience Management sowie Customer Experience & User Innovation.



**Tscheligi, Manfred (tscheligi@usecon.com)**

Doktorat der Sozial- und Wirtschaftswissenschaften. Gründer, Eigentümer und Geschäftsführer der USECON GmbH. Gründer und Leiter des Forschungszentrums CURE. Leiter des Center for Human-Computer Interaction an der Universität Salzburg. Leiter des Centers for Technology Experience am Austrian Institute for Technology in Wien. Mehr als 25 Jahre Erfahrung im Bereich Usability / User Experience und Human Computer Interaction (HCI). Themen: Erforschung der Interaktion zwischen Mensch und Maschine.