No more deceptive designs: dos and don’ts for responsible user experience practices

Digital products, services, and platforms rely on design to build trust with people who are using them. However, as new generations transform personal day-to-day experiences with digital tools, more and more people are impacted by user interface design tactics aimed at influencing one’s decisions. Such design tactics and choices are often referred to as “deceptive designs,” or more commonly, “dark patterns.”[1] By influencing people’s choices, deceptive designs infringe on user autonomy and control.

The use of deceptive designs harms individuals and leads to human and civil rights violations. For example, many people have been forced into giving out their personal data when it is not necessary, in order to use certain services or platforms. Creators of websites and applications, particularly those with e-commerce components, use various deceptive designs to push people into spending more money than they planned. Lots of digital platforms are designed to force people to click through several menus or pages, costing them valuable time to increase “engagement.” When people feel duped by a dark pattern, they may stick with their “decision” out of a sense of shame, embarrassment, or frustration.

To address this problem, a group of designers, researchers, technologists, and civil society members convened at gatherings such as RightsCon, Interaction 22, MozFest, and the Tech Policy Design Lab, developing an ongoing working collaboration to develop a list of dos and don’ts for product design teams. Our working group aims to spark essential changes in product design with recommendations to build trust through design choices that put people first and ensure that they can adequately and autonomously exercise their human and civil rights in the digital world. While we acknowledge this list is not a silver-bullet solution, we

[1] Currently, the issue discussed in this list of recommendations is most commonly known as “dark patterns.” Depending on the context, the issue has also been referred to using terms such as “deceptive designs,” “manipulative designs,” or as a form of “choice architecture,” a term coined by Richard Thaler and Cass Sunstein in their 2008 book *Nudge: Improving Decisions about Health, Wealth, and Happiness.* At the moment, while we are exploring better vocabulary to capture and define the problem across diverse languages, we will use the term “deceptive designs.”. This is subject to change as we update this document.

hope that it serves to advance the rich conversation on deceptive designs happening at the regulatory and technical levels, so that all stakeholders can co-design better digital experiences.

This list of dos and don'ts organizes practices into three categories: **verbal and written language**, **visual design**, and **user research and data collection**. In practice, deceptive interface designs are often not isolated, but rather used in combination with overt data collection and machine learning algorithms, which can exacerbate harms. We encourage companies and their product and design teams to follow these practices as they scope out and implement designs to fulfill product objectives like increasing or retaining subscriptions, increasing conversion rates and encouraging purchases, or gathering personal data.

Key contributors and the working group: Georgia Bullen, Cecilia Maundu, Caroline Sinders, and 30+ designers, researchers, policy experts, technologists, and responsible design advocates.

VERBAL AND WRITTEN LANGUAGE

Written text or audio scripts that come with the interface of a digital product, platform, or service to indicate the functions of the product or instruct people to use it.

Dos:

1. Inform people clearly of their options and the result of these choices.
    a. Add risk and benefits information for the choices people make.
    b. In e-commerce, make it very visible that it's only an option to add additional items before checking out.

2. Create symmetry between options. Allow people to opt-out in any step of their user journey, without using prompts like "yes," "confirm," or "proceed" to distract from opt-outs.

3. Suggest personalizing the reading level to keep writing clear and accessible. Define your audience to ensure that groups that are most at risk can easily understand the content.
    a. Target an elementary reading level for anything related to data.
    b. Use language that can accommodate a wide range of digital literacy.
    c. Write short, concise sentences.
    d. Look to the Web Content Accessibility Guidelines (WCAG) for examples of clear language and content that is readable.
    e. Simplify complex technical information and avoid legal jargon.
    f. Minimize the use of infinite scroll and/or recommendations based on algorithms that prolong, delay, or otherwise influence a person's choices by overwhelming them with information.

4. Use plain language to communicate your privacy policy. Clearly state what the necessity or

utility is to the people of sharing *this specific information.*

   a. Walk people through your data policy when they sign up or start using an app or service.
   b. Indicate what data you collect about them, for what purpose, and how you use and store their data.
   c. Lay out a simple and intuitive process for people to opt-in and then opt-out when they so choose. Clearly state where people have the option to opt in or out.
   d. Be clear and upfront regarding your data retention policy: tell visitors this data will be deleted after X period of time.

5. Be aware of the different possible contexts and meanings words or phrases may have in different cultures, and adjust accordingly for clarity.

6. Pair written language with visuals. Consider an 80% visual to 20% written ratio when presenting new concepts or new information to site visitors or app users.

Don'ts:

1. Don't use confusing or minimizing language to hide from site visitors how you will share their data, such as by using double-negatives or ambiguous descriptions to explain how you collect and use personal data.

2. Don't use broad, vague language to bully people into consent. For example, when people choose to withdraw their consent for use of their data, state clearly how that will impact site services or functionality.

3. Don't use language that creates a false sense of urgency or necessity.
   a. Don't, for example, imply that people will "lose the opportunity of a lifetime" if they don't place an order within a certain time frame.
   b. Don't make payment of optional fees or the sharing of personal information sound like it is mandatory.

4. Don't create guilt. Avoid using language designed to shame people into making certain choices, such as "We are sad to see you go!" when people unsubscribe.

5. Don't require site visitors or app users to explain the choices they've made.

6. Don't provide discriminatory experiences for site visitors or app users based on their personal characteristics.
   a. If, for instance, someone is a reader of a right-to-left language instead of left-to-right, do not make their experience more complicated.
   b. If someone uses accessibility software, they should have a comparable experience to someone who does not.

VISUAL DESIGN

Designs and visual elements aiming to improve the usability and aesthetic appeal of a digital product, platform, or service, including but not limited to image, typography, layout, color, and wireframe.

Dos:

1. Use legible fonts and clear displays when you ask for consent or provide important information.

2. Use opt-ins instead of opt-outs. Don't pre-check the consent box.

3. Develop a recognizable and uniform logo or button to promote awareness of your data use and privacy policy. Keep your privacy statement in a clear, transparent, comprehensible, and easily accessible manner, especially for information aimed at kids.

4. When you offer choices, treat options equally by creating a symmetrical design. Avoid discrimination with color, font, and styling treatments.
   a. "Yes" and "no" options should be the same size, using the same font and color, with the same level of readability.
   b. Ensure the options are displayed as simple in all environments, including devices, operating systems, and browsing tools, or apps. Choices should be distinct.
   c. Bring attention to the part of the interface where visitors have to make a choice (instead of minimizing it or making it invisible).

5. Follow the WCAG standards to ensure accessible color contrast, visual displays, and accessibility compliance. People with cognitive disabilities should be able to understand what they're consenting to.

6. Be aware of the cultural significance of specific colors, shapes, or other indicators that may prompt people to make specific choices, and adjust accordingly to prevent manipulation.

7. Ensure that action buttons or banners don't take up half of the screen or hide important information, including in designs for mobile devices. Follow the WCAG for specific examples.

8. Ensure that the privacy-protective path is nor more arduous than the non-privacy protective path. One way to measure this is to count how many clicks or taps it takes for individuals to proceed in their privacy-enhanced paths, compared to going against their own privacy interests.

9. Provide aid or support in the interface design for deleting personal accounts / data, and adjusting privacy and security settings.

Don'ts:

1. Don't make it difficult for people to reject certain choices or opt-out entirely.
   a. Don't make it easier to consent to data collection than to reject it.
   b. Don't make the process for unsubscribing significantly harder or longer than the process for subscribing, such as making the option for unsubscription hard to find.
   c. Don't automatically set up recurring purchases.
   d. Don't bury the tools for people to accomplish the goal of deleting accounts or restricting access to their personal data.

2. Don’t confuse people about the choices they need to make by creating perplexing navigation or too many click-throughs.
    a. Don’t take site visitors or app users off-course with crowded visuals or other kinds of distractions.

3. Don’t hide important information or options from people.
    a. Don’t, for instance, bury key information that affects an individual’s personal data or opt-out process in the long scrolls of a privacy / personal data policy.
    b. Don’t hide or minimize an action that is important for decision-making, such as by using subtle hyperlinks instead of obvious buttons.
    c. Don’t use small fonts that make it hard to read.
    d. In e-commerce, don’t pre-add items to a shopping basket or otherwise include purchases in a sneaky way.

4. Don’t design a component or interaction that entraps people by exploiting a mistake, such as people clicking on the wrong item or option.
    a. Don’t place an item deliberately in an area that people are likely to hit by mistake.
    b. Don’t use colors to trick people into making mistakes or selecting options that are against their own best interest, such as using green in contexts where “green” means “go” and “red” means “stop.”

USER RESEARCH AND DATA COLLECTION

Information collection and study of the potential people who will be using a digital product, platform, or service, with the aim to understand them and provide insights to optimize the product design.

Dos:

1. Product teams often rely on user data, such as crash data, to improve their products. Yet use of the data can entail privacy risks. Communicate those risks clearly and openly. Make potential harm visible.

2. Favor building site visitors’ or app users’ trust over exploitation and short-term profits.

3. Advocate for security best practices such as following privacy-by-design and privacy-by-default principles that protect people’s digital rights.

4. Create an independent mechanism for oversight of your user research.
    a. Consider building an independent board with civil society and academic organizations to review your site’s balance of meeting research objectives with robust public disclosures of the risks/benefits for participants.

5. Conduct user tests with people in marginalized groups to ensure you don't harm those already underserved. At the same time, treat participants with respect. If a group would be harmed simply by participating in your research, do not include that group, or change your parameters.

6. Ensure your company provides discussion space and transparency for product decisions.

7. Question the kind of relationship you want your brand, service, or business to build with your users, customers, or community, and make choices that will enhance, not undermine, trust.

8. Consider researching and sharing data with company leadership to show how rights-protecting design decisions could increase the company's value, enhance your brand's image, and deepen customer loyalty.

9. If you're proposing a change in order to protect people that could change the norm of your company's business practices, consider asking for permission to do a pilot test, an A/B test, a temporary release, or another form of research to demonstrate the value of the change.

10. Stay updated on laws and policies that impact product design and implementation, such as privacy, data protection, consumer rights, and human rights in general. Advocate for going beyond mere compliance.

11. Devote extra attention and resources to your request for consent.
    a. Ask for consent when site visitors or app users are engaged in a task or view that is related to what you are asking for.
    b. Approach respectfully with an on-screen nudge instead of disrupting an important workflow or process. Give people the option to decide later.
    c. Consider a process that lets people choose what data they want to share.
    d. Test to see whether your visitors or users may want to temporarily disable data collection. If that's a common desire, give them an easy way to opt out for a period of time.

Don'ts:

1. Don't accept all product feature requests without challenging them. Question those that favor short-term business returns over building long-term trust in your products.

2. Don't use price optimization based on people's income levels or other characteristics as a means to enable price differentiation or other forms of discrimination.

3. Don't base your research or product decisions on assumptions about your visitors and users. Interrogate your reasoning and work to ensure you do not deepen existing bias or entrench structural discrimination.

4. Don't forget you have a voice. All companies have a duty to respect human rights. Don't hesitate to speak up if you think your product or company is complicit in rights violations. Advocate for building human rights considerations into all corporate practices, including product design.

We welcome your feedback and commentary. If you have any suggestions regarding this tipsheet, or have questions, please contact Sage Cheng at sage@accessnow.org and Willmary Escoto at willmary@accessnow.org.