Trusted Design Global Case Study: Africa

Tech Hive Advisory

Africa's Deceptive Design Policy Guidelines **3**
Executive Summary 3
Interpretation Section 3
Manifestations of Deceptive Design 3
Applicable Principles 4
User Interface of Digital Products and Services 4
Tracking Technologies Adopted in User Interfaces 5
User Interface for Minors 5
User's Digital Service Profiles 6
Design Impact Assessment 6
Regulatory Oversight 6
Enforcement 6

Trusted Design Global Case Study: Africa

TechHive

At Tech Hive Advisory, we believe that people should have access to a safer digital environment where digital rights and ethical design are prioritised over deceptive design. We believe we can achieve this through awareness creation, advocacy, research, and public action to engage regulators and designers to shape the policy landscape. This year we tasked ourselves with tackling deceptive designs in Africa. Deceptive designs are user interface and design techniques used on websites, mobile applications (Apps), or any other digital medium to manipulate users to do something they did not intend to do in order to benefit the website or App owner. Earlier in the year, we set out to carry out comprehensive research exploring deceptive design use cases in Africa's tech ecosystem, available here. Prior to this, we had put out extensive research on the art of deception by design, available here.

Tech Hive Advisory Contacts:
Adedolapo Adegoroye da@techhiveadvisory.org.ng
Victoria Adaramola va@techhiveadvisory.org.ng

The following is a region-specific discussion of Trusted and Deceptive Design, including exploring relevant issues and recommendations. The perspectives and conclusions presented represent those of the author.

Africa's Deceptive Design Policy Guidelines

Executive Summary

[2 paragraphs]

Interpretation Section

a. Consent
b. Cookies
c. Deceptive design - "Deceptive design" refers to any user interface that undermines, exploits, or undercuts a user's freedom of choice in any way, including subtle omissions, tricks, explicit lies, and nudge techniques, in order to induce a user to do something they did not intend to do.
d. Deleting an account
e. Digital products
f. Freezing an account
g. Lawful basis for processing
h. Informed consent
i. Minors
j. Processing
k. Secure by design
l. User interface
m. Third-party
n. Trackers
o. Web beacons

Manifestations of Deceptive Design

1. The use of the following designs on the user interface of a digital product, website, platform or service shall be regarded as deceptive design;

    a. **Count-down timers:** This form of deceptive design is usually used by e-commerce platforms. It involves using timers to show users that there is a limited period of time for them to make

purchases. This form of deceptive design puts users under pressure to make quick purchases. This form of deceptive design is usually used by e-commerce platforms. In effect, users, due to the fear of missing out, fall for the countdown timers and eventually make a purchase. Aside from count-down timers being deceptive, they put consumers under pressure and mostly do not represent the true position of things.

b. **Pop-ups:** In addition to the use of countdown timers, pop-ups are used to suggest the scarcity of a product or stock to the consumer. Pop-ups display the available stock for a product, thereby creating a sense of scarcity for the product. Like count-down timers, they do not represent the accurate position of things and are sometimes entirely false. The goal of pop-ups is to put consumers under pressure to make a purchase and instil the fear of missing out.

c. **False pricing scheme:** As far as purchases go, prices are a crucial decision-maker. Consumers often weigh their financial capacity or budget against the prices of the goods to decide what to buy. False pricing systems play on the psychology of consumers and trick them into thinking that they are buying a good or getting service at a discounted price. A false Pricing scheme displays two different prices and indicates that the product or service can be purchased at a lesser price when the lesser price is the actual price.

d. **Forceful creation of accounts:** This is a method used by platforms to get users to subscribe to their service and create an account. This involves making users register on the platform before accessing basic services such as inquiries or even gaining access to the platform at all. This form of deceptive design enables platforms and service providers to collect users' data and possibly subject users to unsolicited marketing messages. It is sometimes difficult for users to opt-out of such a system.

e. **Hidden Charges/ information:** This mode of deceptive design is employed either to overcharge customers or to charge extra to access certain services. Service providers and platforms do this by emphasising the main charges and de-emphasising other charges that accrue on the service they render. This form of deceptive design thrives on keeping users ignorant of the breakdown of the service. Hence, they are forced to pay for services they did not freely opt for.
In addition, the service providers tend to misinform the users by hiding some details or misrepresenting the terms and conditions that apply to that service.

f. **Social Proof:** This is a form of manipulation that is used by platforms to persuade users and consumers into patronage. With social proof, platforms and service providers use fictional feedback to describe the experiences of other people that have used the product. This could be in the form of making false comments and recommendations to make intending consumers think that the product or platform is credible.

Applicable Principles

- Accountability
- Transparency
- Necessity
- Secure by Design
- Fairness

User Interface of Digital Products and Services

a. Any use of designs on the user interface of digital products, platforms, and/or services to manipulate users' free choice, autonomy, and decision-making is prohibited.

b. Any digital product, platform, or service's user interface shall not be designed or structured to do any of the following:

   I. obscure, subvert, or impair user autonomy, decision-making, or choice to obtain consent, choice, or user data;
   II. eliminate or restrict the options or choices that should be ordinarily available to a user, such as but not limited to the ability to opt-in and out of services, the ability to accept or reject the use of certain technologies, and the ability to decide on whether or not to provide or refuse to provide personal data;
   III. make choices for users either by pre-selected or pre-ticked options that do not benefit users or make it impossible or difficult for users to opt-out;
   IV. be used to nudge users to select options that are only beneficial to the digital service providers;
   V. use words or descriptions to bully or shame users into making decisions favourable to the digital service provider; or
   VI. manipulate or nudge minors to weaken their privacy settings or provide personal data that is not necessary for the service being used or provided by the minor.

Tracking Technologies Adopted in User Interfaces

a. All tracking technologies, including but not limited to cookies, trackers, web beacons, device graphs, device fingerprinting, or third-party requests deployed on the user interface of digital products to collect, store, profile, and share information about users' activities must only process data in line with the lawful basis for the processing of personal data;

b. Where any of the above tracking technologies are deployed by digital service providers for any form of behavioural or psychological experiment or research based on the activity or data of its users, consent must be obtained from the users who are the object of the behavioural or psychological experiment or research before the commencement of such activities; and

c. Where the lawful basis for processing is consent, the following rules must apply:

   i. The request for consent needs to be clear, in plain language, intelligible and easily understandable;
   ii. Consent needs to be by a positive or affirmative statement or clear act and cannot be pre-selected or pre-assumed;
   iii. Consent needs to be informed and freely given; and
   iv. Consent requests must be specific per purpose and not bundled up with multiple requests.

User Interface for Minors

Where digital services or products are targeted at children or likely to be used by children, the digital service providers must adopt the following rules and strategies for the user interface:

a. Use child-friendly terms and conditions and privacy policies that are easy to understand for kids, and the mechanisms of data processing must be transparent;
b. Processing and collecting children’s personal data must always align with “the best interests of a child”;
c. Only collect and process data that is absolutely necessary for the function of the services being requested and provided by and for the children;
d. Conduct a data protection impact test due to the high risk to children’s data;
e. Adopt age-appropriate designs on the user interface. For the purpose of this section, age-appropriate design alludes to the following requirements:
   i. Employ child rights by design standards such that only the best policies and technologies available are employed for children’s rights and best interests protection in all jurisdictions where their products and services are available;

ii. User interface settings must be high privacy by default, and nudge techniques should not be employed to deceive children into changing those settings;
iii. Processing and collection of children's personal data must always be in line with "the best interests of a child principle"; and
iv. The user interface must be secure by design.

User's Digital Service Profiles

Where a user interface requires the creation of an account before access to services; the following rules must be followed:

a. Users must not be pressured or deceived into providing more information than is necessary during the creation of their accounts. This includes but is not limited to continuously nudging or pushing users through the use of pop-ups, roadblocks and, by being repeatedly asked to provide additional data and offered arguments why they should provide it;
b. Where permissions sought are not necessary to the critical functioning of the user interface, the user interface must disclose along with the request for permission that the request is not necessary for the critical functioning of the user interface;
c. The user interface must make a reasonable effort to accommodate users who do grant access to sensitive permissions, for example, allowing users to manually enter a phone number if they've restricted access to their call logs;
d. Personal data collected during the account creation and during the account lifecycle must only be processed in accordance with the lawful basis for the collection of that personal data; and
e. Users must be allowed to determine the lifecycle of their product by being allowed to delete or freeze their accounts as easily as they were able to create such accounts.

Design Impact Assessment

All user interfaces must be required to go through a design impact assessment to check for the possible existence of elements of manipulative or deceptive techniques leading users to make unintended, unwilling and potentially harmful decisions. For the purpose of this section:

a. the design impact assessment is a process designed to describe and analyse the processing and necessity of the actions required by users or the personal data of users collected.
b. the appropriate legislator, which is the consumer protection commission of each region, will be in charge of creating a template and simple test for digital service providers to enable them to self regulate and carry out individual tests that can inform them of possible elements of manipulative or deceptive techniques.

Regulatory Oversight

For the purpose of this guideline, the consumer protection authority, in collaboration or with consultation with the data protection authority/regulator of each region, will be responsible for playing an active oversight role in ensuring that the use of deceptive design is regulated. The regulators' role will entail the following:

a. Creating a separate complaint handling mechanism for users to report and seek redress for issues particularly relating to or concerning the use of deceptive designs;
b. Investigating user complaints within a stipulated period of time; and
c. Providing feedback and reports to users who have made complaints to the regulators.

Enforcement

Regulators have a prerogative of issuing the first warning to digital service providers upon finding them in contravention of the Guideline; however, where they are repeat offenders, the regulators may either ask the digital

service provider to suspend services for a stipulated period of time or pay a fine or both.