Path: Safety & Deception Path

Path: Safety & Deception Path

List of Requirements (outcomes)

- Avoid Deception
    - Deceptive controls
    - Exploitive behaviors
    - Misinformation
    - Preselections
    - Redirection
    - Obscuring primary content
- Citation
- Indicate 3rd party content
- Clear agreement
- Risk statements
- Information privacy
    - Disability information privacy (in tab information privacy)
    - Sensitive information (in tab information privacy)
- Algorithm Accessibility
    - Algorithm bias
    - Social media algorithm
    - Mental health concerns

Exploratory Scratchpads

- Prevent Harm
- For Clear Agreement: Clear Purpose Scratchpad
- Deceptive Patterns Outcomes
- Deceptive Patterns - Functional Needs Subgroup

Documents

Cognitive Accessibility Issue Papers - Online Safety and Wellbeing (Algorithms and Data)

Resources

- COGA 2 Literature Review and update
  Mental Health Literature Review (Responses)
- Proposed pattern and changes for Content-Usable version 3 (pulls our relevant research from mental health lit review spreadsheet)
- Supported Decision Making - Issue Paper (early draft

- Help-the-user-stay-safe-pattern in making content useable (COGA guidance document)
- Cognitive Accessibility Issue Papers - Online Safety and Wellbeing (Algorithms and Data)
- Deceptive Design
- Deceptive Patterns in UX: How to Recognize and Avoid Them - Nielsen Norman
- Series of Medium articles by Nadia Joy Doobal
    - Dark UX Tricks: Avoid Manipulative Patterns
    - Dark UX Patterns: Subtle Manipulations in Digital Design
    - The Hidden Complexity of Dark UX
- The Dark (Patterns) Side of UX Design
- Shining A Light on Dark Patterns (pdf)
- Dark Patterns and User Mental Health: Identifying Theoretical Impacts of Deceptive Design on Vulnerable Demographics
- Mobilizing Research and Regulatory Action on Dark Patterns and Deceptive Design Practices (pdf)
- Dark Patterns and the Emerging Threats of Deceptive Design Practices
- Appropriate Tone: https://www.w3.org/TR/wcag-3.0/#appropriate-tone
- Clear Operation (User Story): https://www.w3.org/TR/coga-usable/#clear-operation-user-story
- Deceptive Patterns Tweets (examples of possible deceptive patterns and anti-patterns - w/some bias)
- Keeping Children Safe Online
- Preventing Online Harm and Abuse
- UK Online Safety Act 2023
- Kids Online Safety Act (proposed, US)
- NDIS Privacy Easy Read
- Personal data (GDPR): https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-information-a-guide/
- Sensitive information / protected characteristics: https://www.lboro.ac.uk/data-privacy/help/comparison/

Method - Disability Related Information

Disability Related Information

Full template (this document comes under part 4: Methods)
Template for Content Creation Process for Migrating WCAG SC (component-based)

Method Instructions
Writing Testable WCAG 3.0 Outcomes

Introduction

Requirement

Disability related information, whether collected directly or through aggregation or pattern recognition, is treated with the same consideration as other Private and Sensitive Information.

Platform

Generic

Whatever laws and policies are applied to other Private and Sensitive Information is also applied to disability related information, including information implied by aggregating or interpreting behavior.

This may include (but is not limited to):

- Notify users when data will be collected, what data is being collected and why it is necessary/how it will be used
- Allow users to request access to the disability related information collected
- Allow users to request right to be forgotten

Technology

- {List of technology(ies)}
    -

Input aspects for testing

1. Identify if disability related information is being collected, either explicitly or through aggregation or pattern recognition
2. Identify the laws, regulations and policies governing data collection and treatment of Private and Sensitive Information
3. Verify that the disability related information is being treated in the same way as other Private and Sensitive Information.

Summary

When disability related information is collected about an individual, the system treats that data the same as all other Personally Identifying Information.

How it solves user need

This SC provides control and autonomy around their disability. It allows them to know what information about heir disability is being collected and ensures the data is collected and presented back in ways that treat the disability related information securely.

When to use

{when the method should or should not be used}

Background

W3C Resources

- {related resources}

Non-W3C Resources

- {related resources}

Accessibility Support

{short paragraph on accessibility support considerations}

Assumptions

- {assumptions}

Examples

- {list of examples, unless using sub-sections, then delete this list}

Passed

{Example Name}

{Use a copy of this section for each example if not using a bullet list of examples}

{explanation}

<

Failed

{Example Name}

{Use a copy of this section for each example if not using a bullet list of examples}

{explanation}

<

Inapplicable

{Example Name}

{Use a copy of this section for each example if not using a bullet list of examples}

{explanation}

Tests

Get Started

{Tips or link to information for beginners in testing.}

Summary

[overview of the test]

Applicability

This outcome applies to any [element names] element that is [condition] and for which one of the following is true:

{excluded, ignored, exception}

[element]

Expectations

[detail of the expectation]

Glossary

[term]

definition

[term]

definition

Guideline: Information Privacy

Guideline : Information provided by a user should be considered private [DRAFT]

Current Applicability Tree

Guideline: Information Privacy - When providing private and sensitive information, users understand:

- That the information requested is private and sensitive,
- How the information requested will be used, and
- The risks involved in providing the information.

For every piece of information that a user enters or interacts with:

1. Is the information private and sensitive?
    a. Yes, information must meet **Access to Information** and **Data Management.** Continue
    b. No, this section is not applicable. End.
2. Is the user made aware and warned of potential risks to privacy?
    a. Yes, **Disability information privacy**, **Acknowledgement of Information Sharing.** Continue.
    b. No. Fail. End.
3. Does the user understand the data and privacy information clearly?
    a. Yes, **Access to Information**. Continue.
4. No, End.
5. Is the information presented on a closed system (ex: kiosk)?
    a. Yes, products must **Protect sensitive information** and Hide information. Continue.
    b. No, the product may Protect sensitive information. Continue.
6. Can the user control the privacy of their data?
    a. Yes, controls must meet **Data Management.** Continue.
7. No. Continue.
8. Is the user entering private and sensitive information that may be disclosed or shared with third parties or algorithms?
    a. Yes, meet **Acknowledgement of information sharing**. Continue.
9. No. Continue.
10. Is disability information directly or indirectly captured?
    a. Yes, **Disability information privacy.** End.
    b. No. End.

Foundational Requirements

1) **Global Privacy Settings -** Privacy settings from the operating system, user agent, and application are honored.

Test:

- Is a global privacy setting available (ex: hide IP address)?
- If available, does the application attempt to or succeed at accessing the information the user attempted to keep private?

Note: Needs additional conversation around use cases where caregivers set these settings or how this disproportionally affects people with disabilities in other way

2) **Access to Information** - Private or sensitive information is available to the person to which it applies (e.g., logging in to personal information, clearance for access to information, downloadable version, persistent way to access information via an icon or button). (e.g. personal medical records/information, account information, etc.)

   Test: The user has a clear path to their private or sensitive information that the system collects and stores.

3) **Notify about sensitive information -** When private or sensitive information is displayed, notify the user and provide a mechanism to hide the information.

   Test: When private or sensitive information is displayed, a notification is provided to the user about the display and a mechanism is available that allows the user to hide the information from observers. The notification and mechanism meets accessibility guidelines including clear language, clear controls and a minimal critical path.

   Possible technique - hide the sensitive information by default and allow user to display

No additional risk - Accessibility accommodations and assistive technology do not expose people with disabilities to additional risk. (Foundational)

4) **Acknowledgement of information sharing** - When private or sensitive disability information will be disclosed or used by third parties or algorithms (including AI), the user is notified and must acknowledge the notification to proceed.

   Test: When private or sensitive information will be shared:

   - a notification is provided to the user,
   - The user must acknowledge the sharing, and
   - The notification and acknowledgment mechanism meet accessibility guidelines.

        - Notification meets accessibility and clear/plain language WCAG 3 guidance
5) **AT Data Collection** - When information about assistive technology use or disability related settings or patterns of behavior are captured, a way is provided for users to turn off the collection or manage the resulting data.

   Test: Ensure users have a way to manage their data and privacy using:

   a) plain language,
   b) clear controls,
   c) warnings about potential risks are provided, and
   d) requires minimal interactions / minimal critical path to make changes.

6) **Disability information privacy -** Disability related vulnerability information is not disclosed to or used by third parties and algorithms (including AI, *"user navigation trackers"* for UX folks to see how people use the page and possibly give AT information to UX teams). This should include implied disability, such as noticing difficulties with numbers, or use of language suggest mental health disability or vulnerability.

Supplemental Requirements

- **Accessible settings** - When the amount of information shared can be adjusted, the method of adjusting the amount of information with a minimal cognitive burden.
    - **Test**:
        - Can information collected/shared can be adjusted?
        - Does the method for adjusting the amount of information shared, follow all clear language requirements and clear path requirements? [list additional supplemental requirements that must be met]
- **Privacy Settings** - Privacy settings do not cause extraneous cognitive load.
    - **Test**:
        - Are privacy settings available?
        - Do privacy settings follow all clear language requirements and clear path requirements? [list additional supplemental requirements that must be met]
- **Appropriate and Safe Content** - Content that may be inappropriate or cause harm to others is identified and a way to avoid it is provided.
    - **Test**:
        -

Supported Decision Making - is supported in a way that provides support while enabling user autonomy Best Practices

- Allow users to request information about the private and sensitive content a platform or algorithm stores or uses regarding themselves.
- Provide a way for users to manage private and sensitive information.
- Post a privacy statement that includes how information is protected and the security processes used by the organization.
- Private and sensitive information should be obfuscated when doing AT data collection.

Assertions

- Private and sensitive information is handled according to [named security procedures] and reviews are conducted
    - Note: The security procedure referenced must state how PII should be handled and warnings given to the user when sharing PII?
    - Internal Verification: The organization follows and conducts verification testing against the named security procedure. The security procedure itself addresses how PII should be handled.
- When considering the safety and security of our users, we considered use cases of people with Diverse Disabilities (diverse range of disabilities include: including individuals with cognitive and learning disabilities and mental health conditions … to be worked on)
- Research is being conducted ongoing for risks to safety, wellbeing, and mental health for users with Diverse Disabilities and when risks are found, all reasonable practical steps identified are taken to mitigate the risk.
- **Safe Content Review** - Content has been reviewed for violence, suicide, and other graphic or troubling content and appropriate warnings are available before accessing the content.
  Note: Troubling content will vary based on culture or individual situations, and reviews should take target audiences into consideration. (Assertion)

History

Exploratory Requirements (Dec 2024/Jan 2025)

Guideline: Security and privacy - Users' safety, security or privacy are not decreased by accessibility measures.

- **Requirement: Clear agreement** - The interface indicates when a user is entering an agreement or submitting data.

- **Requirement: Disability information privacy -** Disability information is not disclosed to or used by third parties and algorithms (including AI).
- **Requirement: Sensitive information -** Prompts to hide and remove sensitive information from observers are available and usable.
- **Requirement: Risk statements -** Clear explanations of the risks and consequences of choices, including use, are stated.

Goal

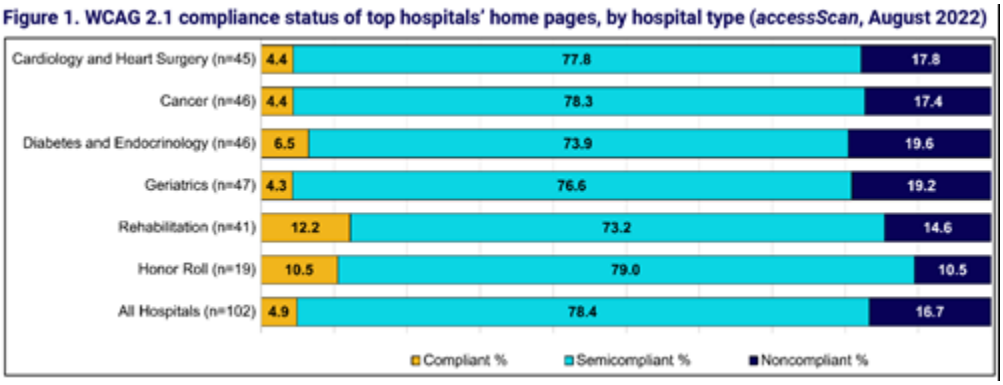
Ensure a user's information is treated as private and secure.

Research

- Web Security and Privacy Technologies - coga issue paper
- People with disability and privacy in precision medicine research: what's at stake? Supriya Lal Kapur, Maya Sabatello (May 2024) Research found that precision medicine research (PMR) is supported by many people with disability, although its vast use of data also raises privacy concerns and is a potential barrier for participation of this population in PMR. The practice of linking or pairing multiple datasets that can result in compromised privacy has received little regulatory attention. This practice is widely documented, with studies showing that statistical models can be built to link together de-identified medical information with personal identifiers. For example, voter registration records and social media posts can successfully identify patients in de-identified electronic health records (EHRs). Studies further found that the risk for compromised privacy remains high even in incomplete, non-clinical datasets where some identifiers are missing.
- Disabled People Need Critical Privacy Protections in ADPPA - Disabled people are one of the most hyper-surveilled communities within the U.S. Public and private entities alike collect enormous amounts of often deeply personal data about our lives and health, for purposes ranging from benign (such as tracking disability-targeted hiring benchmarks) to malicious (such as profiling students as likely future criminals). Algorithm-driven systems now commonly power recruiting and hiring processes, tenant background checks, public benefits applications, and even remote test proctoring, all with outsized impact on people with disabilities.
- FCA Consumer Duty PS22/9 (UK) sets out rules and guidance for a new Consumer Duty that will set higher and clearer standards of consumer protection across financial services and require firms to put their customers' needs first.
- **Information privacy and security as a human right for people with disabilities** J Lazar, B Wentz, M Winckler - **Disability**, Human Rights, and …, 2017 - degruyter.com

    - “People with disabilities often rely on technology devices to compensate for their disabilities. However, this reliance on technical devices may mean that more data are being collected about them than about the typical citizen (without their knowledge), or that they are more susceptible to threats related to privacy and security. Furthermore, if data are collected without an individual’s knowledge that document that an individual has a disability, this information, a violation of his or her privacy, could potentially be used to discriminate against the individual.”
    - Includes section on “Information Privacy for People with Disabilities”
        - Privacy of Disability status
        - Privacy of Geolocation Data
        - Privacy Policies and People with Disabilities
    - People with disabilities do indeed need the same privacy and security protections that all individuals need, and they actually need these privacy and security protections more than the typical user because of their reliance on technology. People with disabilities are likely to have more personal information stored in their accounts or devices than the average citizen does.
- Protection for privacy under the United Nations Convention on the rights of persons with disabilities MC Weber - Laws, 2017 - mdpi.com [Full View]
- Accessible and inclusive cyber security: a nuanced and complex challenge. K Renaud, L Coles-Kemp - SN Computer Science, 2022 - Springer
    - Section on examine the barriers and challenges to developing accessible cyber guidance
- Daniela Napoli. 2018. Developing Accessible and Usable Security (ACCUS) Heuristics. In Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (CHI EA '18). Association for Computing Machinery, New York, NY, USA, Paper SRC16, 1–6. https://doi.org/10.1145/3170427.3180292
- The Critical Role of Web Accessibility in Health Information Access, Understanding, and Use (pdf), Amanda Krupa, MSc (AHIMA Foundation); Jill B. Roark (Consultant), MPH; Kirsten Barrett, PhD (Mathematica) 9/22/2022, updated 11/03/2022, AHIMA Foundation
    - In August 2022, AHIMA Foundation and Mathematica worked together to gather and analyze baseline data on the state of accessibility compliance across the website home pages of top U.S. hospitals. We gathered these data using web accessibility evaluation tools—software programs or online services that help determine if web content meets accessibility guidelines.
    - We found that only 4.9 percent of hospitals on the honor roll or the top hospital lists were WCAG 2.1 compliant. Nearly 80 percent of the hospitals were semi compliant, and 16.7 percent were noncompliant. Rehabilitation hospitals had the most hospitals deemed compliant, at 12.2 percent, and geriatrics hospitals had

the fewest, at 4.3 percent *(Figure 1)*.



- Role of Health Literacy in Health-Related Information-Seeking Behavior Online: Cross-sectional Study, Hee Yun Lee; Seok Won Jin; Carrie Henning-Smith; Jongwook Lee; Jaegoo Lee, 2021
    - Our findings indicate that access to online health-related information is not uniformly distributed throughout the population, which may exacerbate disparities in health and health care. Research, policy, and practice attention are needed to address the disparities in access to health information as well as to ensure the quality of the information and improve health literacy.
    - Although the internet has contributed to enhancing the potential for health information access and use while reducing barriers to obtaining health information in the US general population, not all people have obtained these benefits. For example, gender is a key predictor of use of the internet and online health information behavior [15]. Previous studies have shown that men are less likely than women to use the internet for health information–seeking and to trust online sources [13,16-18]. There remain some groups of people who still experience difficulties in accessing and utilizing health information because of barriers such as a digital gap and limited health literacy [1,19,20].

- Internet Privacy is a Disability Rights Issue Ariana Aboulafia / Jan 19, 2024 - People with disabilities may affirmatively reveal sensitive and private health information to receive an accommodation, including in rideshares and standardized testing. They may also incidentally (and largely unintentionally) share their disability status simply by using assistive or adaptive technology. The “choice” for a person with a disability is to divulge that information, or to either receive an inaccessible version of a service, or to not use that service at all – which impacts that person’s ability to live a full and independent life. Not only do disabled individuals have little control over whether or not to share this information in the first place, they also may have little knowledge as to how that data is processed, stored, and shared after its initial disclosure. For these reasons, advocates for disability rights and disability justice should prioritize the protection of personal and digital privacy as a central issue, and organize towards solutions. Example: ACT test results flagged students’ accommodations on score reports to colleges, sometimes resulting in the student not being accepted.

No disabled person should have to choose between accessing technologies that help them lead fulfilling, self-directed lives and protecting their personal information. And, people with disabilities should be able to benefit from technology without worrying that their health-related data will be used for nefarious or unknown purposes. It is vital that leaders in the disability community embrace internet privacy as a disability rights and justice issue, and support changes in law, regulation, and industry policies that will help protect the data of all individuals, including those with disabilities.

- Information Privacy for Technology Users With Intellectual and Developmental Disabilities: Why Does It Matter? Hajer Chalghoumi,Virginie Cobigo, et al Participants demonstrated awareness of privacy concerns, but not in situations involving the use of technology; their awareness is not transferred to the abstract context of IT use. Privacy breaches were revealed to be a major risk for persons with IDD, who did not seem to understand how their personal information was used. Most protection mechanisms and tools reported were those suggested and implemented by caregivers and close relatives who had a great influence on the participants' attitudes and behaviors toward IT and privacy. Our findings suggest that when using IT, persons with IDD often experience the consequences of a trade-off between autonomy and privacy.
- Protection of Privacy of Information Rights among Young Adults with Developmental Disabilities (Nazilla Khanlou, Anne Mantini, Attia Khan, Katie Degendorfer, Masood Zangeneh) Young adults with developmental disabilities (YADD) and their families are at risk of exploitation in terms of privacy and protection of their personal information (Joffe, 2010). Their increasing dependency on multiple community-based and private agencies creates a scenario where a wide range of personal information is retained and shared through the course of servicing these individuals and their families over time. YADD are vulnerable not only because they are in a sensitive period transitioning into adulthood but also as they have complex developmental needs and may experience difficulties making their own decisions (Dyke et al., 2016). They may also have concurrent health and mental health needs which require support, and even as adults may frequently depend on secondary decision makers to protect their privacy of information rights (Geist, 2016).

Examples

US Trademark Application

Password

Acknowledgement of information sharing

https://www.oneazcu.com/olb-privacy-policy/

Information We Collect

We may collect non-identifying information from visitors to our website. However, visitors to our website remain anonymous. We do not collect identifying information about visitors to our site. We may use standard software to collect non-identifying information about our visitors, such as:

(1) Date and time our site was accessed
(2) The IP address (A numeric address given to servers connected to the Internet)
(3) Web browser used
(4) City, state, and country

We collect non-identifying information for a variety of purposes. We use this information to create summary statistics and to determine the level of interest in information available on our site. Visitors may elect to provide us with personal information via E-mail, online registration forms, or our guest book.

How We Use Information We Collect

This information is used internally, as appropriate, to handle the sender's request. It is not disseminated or sold to other organizations. However, the information we collect from visitors to our website may be released to third parties, shared and/or used to protect against or investigate fraud, if required by law and/or to establish or exercise our legal rights or defend against claims.

Children's Online Privacy Protection Act Information

This website is not directed at children. We do not market to children, nor do we knowingly collect or retain personally identifiable information from children.

Sensitive information

https://www.weber.edu/iso/sensitive-data.html

Sensitive Information

Sensitive Information - Any data, electronic or physical copy, of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on Weber State University interests, the conduct of University programs or the privacy to which individuals are entitled. Examples of such data would include that data protected by the **Government Records Access and Management Act (GRAMA)**, **Family Education Rights and Privacy Act (FERPA)**, **Gramm-Leach-Bliley Act (GLBA)** or other laws governing the use of data or data that has been deemed by the University as requiring protective measures.

Private Information or **Sensitive Information** can be broken into three categories:

High-Risk – Data that could be used to steal an individual's identity or cause harm to the individual, and for which there are legal requirements or industry standards prohibiting or imposing financial penalties for unauthorized disclosure. Data covered by Gramm-Leach Bliley Act (GLBA) and Payment Card Industry (PCI) are in this class.

Restricted – Information assets for which there are legal requirements prohibiting or imposing financial penalties for unauthorized disclosure. Data covered by federal and state legislation, such as **Family Educational Rights and Privacy Act (FERPA)**, Health Insurance Portability and Accountability Act (HIPAA), Government Records Access and Management Act (GRAMA), or the Data Protection Act, are in this class.

Confidential – Data that the University has determined should be protected because it may expose the University to loss if disclosed, but is not protected by federal or state legislation. For example, a user ID in combination with a password is considered to be confidential.

To learn about how to protect sensitive information, go to our **Protecting Sensitive Data** page.

Hiding information

JAWS Feature - Privacy Screen

Privacy Screen

For added security, the Privacy Screen prevents others from seeing what the kiosk user is typing or reading. There are three ways to toggle this feature:

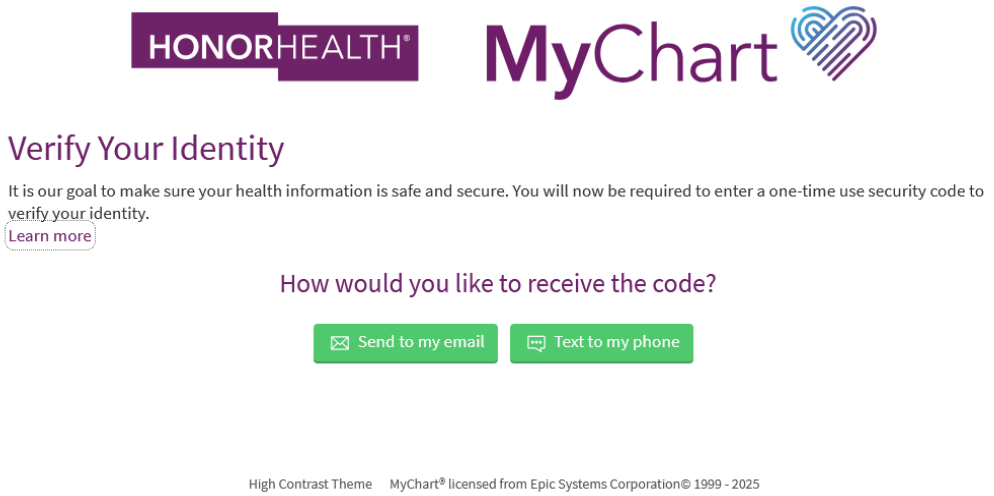
The kiosk user can perform a **One-finger swipe up and left**. The kiosk administrator can also configure this gesture through the JAWS for Kiosk Admin Settings as described in the Customizing Verbosity and Gesture Navigation section.
The Kiosk user can perform a **One-finger swipe down and right** to open the Options dialog and double tap the **Enable Screen Privacy** switch.
Kiosk applications can enable and disable the Privacy Screen using a JAWS for Kiosk SDK method.

For example, a developer can add the following code snippet to a kiosk application to enable the Privacy Screen in JAWS for Kiosk:

```
fun updatePrivacyScreen(isPrivacy: Bool) {
        JAWSKiosk.getSession().setPrivacyScreen(isPrivacy)
}
```

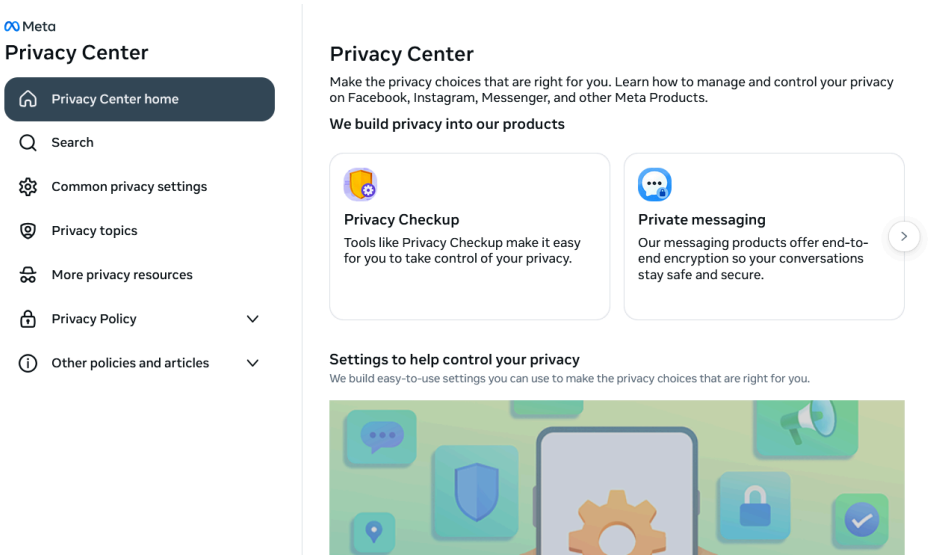
Access to Information

Honor Health - Identity Verification Page



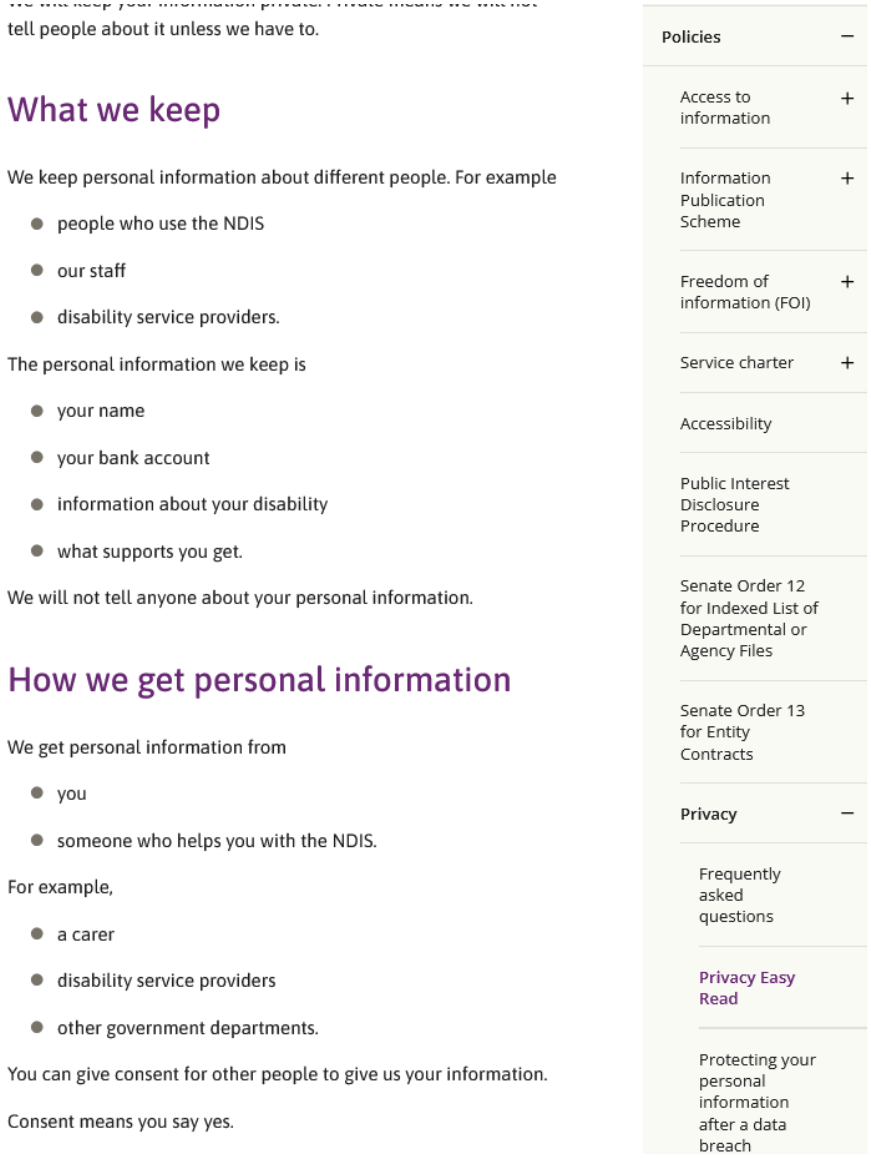
Data Management

Facebook - High cognitive load to use



Disability information privacy

https://www.ndis.gov.au/about-us/policies/privacy/privacy-easy-read



Bad examples

1:
We use cookies and follow our user data policy . Press OK to continue using this site
{ok}

2
Do you agree to our cookie policy and our terms and use of data
Yes / manage data

The manage data option takes you to a long difficult scrollable set of uses. Some people can manage their data but others will not be able to.

What to do

[In as plain-language as possible, outline how you would know if you have met the guideline. E.g. a general test procedure.]

User Need(s)

[List from the scratchpad any that are relevant to this guideline.]

- **User Need:** As a person who is blind, I need features that help me to hide and remove sensitive information from others who may be watching or listening.
- **User Need:** As a person with a mental health, cognitive, or learning disability (maybe any disability), I need protection from predators and information hidden that may identify me as vulnerable (Assertion of Security Process)
- **User Need:** As a person with a mental health disability (maybe all disabilities), I need information about my disability to be protected (Assertion of Security Process)
- **User Need:** As a person with a disability, I need my accessibility preferences, settings and use of assistive technology to be private. (avoid being outed)
- **User Need**: As a user, I understand the risks of sharing my information and am given an opportunity to agree when my medical information is stored, and shared, or presented including implied information such as the name of a medical support app, or web search I am using
- **User Need:** As a person with a mental health, cognitive, or learning disability (maybe any disability), I need content sharing to support SDM (supported decision making) without loss of my autonomy
- **User Need:** As a person with a mental health, cognitive or learning disability I need privacy and data sharing clearly communicated.
- **User Need:** I need optional data to be clearly indicated or not requested.
- **User Need:** I need to safely, privately, and easily access my medical health information
- **User Need:** As a person with a mental health, cognitive, or learning disability (maybe any disability), I need protection from errors and biases in algorithms
- **User Need:** As a person with a disability, I need to control whether content is presented to me because I'm disabled.
- **User Need:** As a person with a mental health disability, I need a way to reduce the negative effects of social media. (safety of what is displayed and knowledge of tracking by social media)
- **User Need:** As a person with a mental health, cognitive, or learning disability (maybe any disability), I need my data to never be used to exploit me

Decision Tree

Guideline: Information Privacy - When providing private and sensitive information, users understand:

- That the information requested is private and sensitive,

- How the information requested will be used, and
- The risks involved in providing the information.

For each request for private and sensitive information:

1. Will information be disclosed or shared with third parties or algorithms?
    - Yes. Use Acknowledgement of information sharing.
    - No, continue.
2. Is the private and sensitive information displayed visibly on the screen and available to assistive technology?
    - Yes. Use Sensitive Information and Hiding Information.
    - No, continue.
3. Is the private and sensitive information safely and easily accessible?
    - Yes, Use Sensitive Information.
    - No, continue.

Suggested Alternative “Applicability” Tree

For each request for private and sensitive information:

1. Does it meet Access to Information?
    a. Yes
    b. No
2. Will information be disclosed or shared with third parties or algorithms?
    a. Yes. Use Acknowledgement of information sharing.
    b. No, continue.
3. Is the private and sensitive information displayed visibly on the screen and available to assistive technology?
    a. Yes, Use Sensitive Information and Hiding Information
    b. No
4. Is the **information** on use of data and privacy information understandable via clear language and minimal critical paths to access?
    a. Yes
    b. No
5. Is the **management** of options and preferences for data and privacy, usable with **a)** clear language and clear controls and **b)** minimal interactions / minimal critical path, for maximum privacy?
    a. Yes
    b. No
6. Are warnings about known potential risks to privacy?

    a. Available in clear language,
    b. Available at the point where a risk may occur, to prevent that risk,
    c. Available to assistive technology.
7. Can sensitive information and posts be fully removed via clear language, clear controls, and assistive technology?
    a. Yes
    b. No

1 April Applicability Tree

1. Is the information that is displayed or to be collected private and sensitive?
    a. Yes, information must meet **Disability Related Information.** Continue
    b. No, this section is not applicable. End.
2. Is a notification about security and privacy provided before the information is displayed or requested?
    a. Yes, notification must meet **Accessible Security and Privacy Notification**. Continue
    b. **No, fail.**
3. Are there prompts to hide sensitive information and effective mechanisms to maintain privacy from observers available?
    a. Yes, prompts must meet **Protect Sensitive Information.** Continue
    b. No, fail.
4. When private or sensitive data is being disclosed to third parties or algorithms, are effective notifications provided that must be acknowledged to proceed?
    a. Yes, notifications must meet **Acknowledgement of Information Sharing**. Continue
    b. **No, fail.**
5. Has explicit permission been granted by the user for information to be disclosed or used by third parties or algorithms, including implied disability?
    a. Yes, disclosure of information must meet **Disability information privacy.**
    b. No, fail.

—

Separate Applicability Trees (4/22/25)

Applicability Tree (Disability Related Information)

1. Is a notification available before **Disability Related Information** is disclosed or shared to third-parties or algorithms?
    a. Yes, notification must meet **Accessible Security and Privacy Notification.** Continue
    b. No, fail.

2. When **Disability Related Information** is being disclosed to third-parties and algorithms, are effective notifications provided that must be acknowledged to proceed?
    a. Yes, notification must meet **Acknowledgement of Information Sharing**. Continue
    b. No, fail.
3. Are there prompts to hide **Disability Related Information** and effective mechanisms to maintain privacy from observers available?
    a. Yes, prompts must meet **Protect Sensitive Information.** Continue
    b. No, fail.
4. Are there effective mechanisms available to users to manage or delete **Disability Related Information** to protect users? (e.g., mental health, cognitive, learning, etc.)
    a. Yes, effective mechanisms must meet:
        i. Protect Sensitive Information.
        ii. Data Management
    b. No, fail.

Applicability Tree (Accessible Security and Privacy Notification)

1. Is a notification about security and privacy provided before the information is displayed or requested?
    a. Yes, notification must meet **Accessible Security and Privacy Notification**. Continue
    b. **No, fail.**
2. Are notifications available to users accessible through assistive technologies?
    a. Yes, notification must meet **Accessible Security and Privacy Notification**. Continue
    b. **No, fail.**
3. Are notifications available in clear and plain language? (e.g., Terms of Service, Code of Conduct, etc.)
    a. Yes, notification must meet **Accessible Security and Privacy Notification**. Continue
    b. **No, fail.**

~~Applicability Tree (Access to Information)~~

~~1. Is sensitive and private information available safely and privately to the user?~~
    ~~a. Yes, information must meet **Access to Information**. Continue~~
    ~~**b. No, fail.**~~
~~2. Is a notification about security and privacy provided before the information is displayed or requested?~~
    ~~a. Yes, notification must meet **Accessible Security and Privacy Notification**. Continue~~
    ~~b. **No, fail.**~~

3. ~~Are there prompts to hide sensitive information and effective mechanisms to maintain privacy from observers available?~~
    a. ~~Yes, prompts must meet **Protect Sensitive Information.** Continue~~
    b. ~~No, fail.~~
4. ~~Can sensitive and private disability information or data be manageable by users?~~
    a. ~~Yes, data management must meet:~~
        i. **~~Disability Related Information,~~**
        ii. **~~Access to Information,~~**
        iii. **~~Protect Sensitive Information.~~**
    b. ~~No, fail.~~

Applicability Tree (Protect Sensitive Information)

1. Are there prompts to hide sensitive information and effective mechanisms to maintain privacy from observers available?
    a. Yes, prompts must meet **Protect Sensitive Information.** Continue
    b. No, fail.
2.

Applicability Tree (Acknowledgement of Information Sharing)

1. When private or sensitive data is being disclosed to third parties or algorithms, are effective notifications provided that must be acknowledged to proceed?
    a. Yes, notifications must meet **Acknowledgement of Information Sharing**. Continue
    b. **No, fail.**
2.

Applicability Tree (Data Management)

1. Can sensitive and private disability information or data be manageable by users?
    a. Yes, data management must meet:
        i. Disability Related Information
        ii. Access to Information
        iii. Protect Sensitive Information
    b. No, fail.

Applicability Tree (Disability Information Privacy)

1. Has explicit permission been granted by the user for information to be disclosed or used by third parties or algorithms, including implied disability?
    a. Yes, disclosure of information must meet **Disability information privacy.**
    b. No, fail.
2.

Foundational Requirements

Disability Related Information - Disability related information, whether collected directly or in aggregate, is treated with the same consideration as other Private and Sensitive Information.

Accessible Security and Privacy Notification - Information provided about private and sensitive information must be available in a plain language version and to assistive technology.

Access to Information - Disability information or otherwise, is available safely and privately to the person to which it applies.

Protect Sensitive Information - Prompts to hide or reveal sensitive information from observers are available and provides an effective way to do so.

Acknowledgement of information sharing - When private or sensitive disability information will be disclosed or used by third parties or algorithms, the user is notified in an accessible message that must be acknowledged to proceed.

Data Management - Disability information can be managed in ways by users that are covered by **Disability Related Information, Access to Information, Protect Sensitive Information.**

Disability information privacy - Disability information is not disclosed to or used by third parties and algorithms, which includes implied disability.

Guideline: Algorithm Accessibility

Guideline: Users are not disadvantaged or harmed by algorithms.

- Algorithm bias - Algorithms (including AI) used are not biased against people with disabilities.
- Social media algorithm - A mechanism is available to understand and control social media algorithms.
- Mental health concerns - From fast subgroup - Linked to document

Foundational Requirements

Tools to create LLMs and other AI meet accessibility requirements.

Supplemental Requirements

None

Assertions

Disability Inclusive Data Sets
Data sets have been trained using representative and unbiased disability related information that is proportional to the general population.

Algorithms avoid causing harm
Usability testing and ethics reviews have been conducted to minimize the possibility that algorithms cause harm to people with disabilities.

Exploratory Requirements (Dec 2024/Jan 2025)

Guideline: Previous: Users are not disadvantaged by algorithms.

Suggested: Users are not disadvantaged or harmed by algorithms.

Goal

Ensure algorithms are not biased against disabled people

Research

- Notes from my discussions with many professional Mental Health people Licensed Clinical Social Workers, Licensed Professional Clinicians, etc. (CONTENT WARNING: examples of how algorithms affect teens and children - Conversations with LCSW/LPCs
- Cognitive Accessibility Issue Papers - Online Safety and Wellbeing (Algorithms and Data)

Examples

What to do

[In as plain-language as possible, outline how you would know if you have met the guideline. E.g. a general test procedure.]

User Need(s)

[List from the scratchpad any that are relevant to this guideline.]

Decision “Applicability” Tree

History:

Best Practices

Assertions

Guideline: Avoid Deception

Guideline: Avoid Deception

Users do not encounter deception when completing tasks, unless essential to the task.

Foundational Requirements

- **No misleading wording** - Controls do not include double negatives, false statements, or other misleading wording.
- **Artificial pressure** - Process completion does not include artificial time limits

  Note: Implying to a user that they will lose a benefit if they don't act immediately is an artificial time limit (example: lose coupon code if you don't give email immediately)

  - **Test**:
    - Check if there is a process
    - Check if the process has a time limit
    - Check that the time limit is not fake
- **No Misinformation** - Processes can be completed without navigating misinformation.
  - **Test**:
    - Check if there is a process
    - Check that the process does not include misinformation
    - Check that the process does not include redirection
- **No Hidden Preselections** - During process completion, preselected options that impact finance, privacy or safety are visibly and programmatically available to the user by default. Exception: The user selected these options previously in the process.
  - **Test:**
    - Check that there is a process (No, pass; Yes, keep going)
    - Check that the process includes preselected options that impacts the users' finances, privacy, or safety (No, pass; Yes, keep going)

        - Check that the preselections are visible without expanding content or navigating outside of the process (No, Fail; Yes, Pass)
        - Check that the preselections are programmatically available (No, Fail; Yes, Pass)
- **No Sneaking [Needs More Research]** - When completing a process, all financial, privacy or safety related information and choices that are provided to the user [balance between towards the start and help walking through decisions].
    - **Test**:
        - Check that there is a process that affects finances, privacy or safety (No, pass; Yes, keep going)
        - Check that all information and choices about the impact to finances, privacy or safety are available before the user makes decisions. (Yes, Pass; No, Fail)
- **No Redirection [Need More Research]** - A mechanism is available to alert users they are exiting the site. Users are notified before they exit a site.
    - Test:
        - Check that there is a link, button or other component causes the user to exit a set of webpages
        - Check that the user is notified as part of the component (ex: external link icon) or before they exit the site (pop up window).
- **No Interference/Obstruction -** Interactive controls that impact finances, privacy or safety or move users to another site are visible and available - does not overlay a control with a different purpose causing the user to click it by accident and without knowledge.
- **Changes in Agreement** - A user is notified before any change in terms of agreement to a continuing process, service, or task, and is given the opportunity to provide consent to continue.
    - **Test:**
        - Check that there is a continuing process, service or task where there is a change in the terms of agreement
        - Check that the user is given an opportunity to consent to the change and the user may exit the agreement.
    - **Best Practice:** Notify a user before a change in agreement terms (ex: moving from free trial to subscription price, change in price on

an ongoing order, etc.) and include instructions for how to cancel the subscription/order/etc.

Supplemental Requirements

- **No emotionally misleading designs** - Systems do not threaten individuals or restate decisions in a degrading way.
- **Misdirection** - Systems do not draw users attention away from information that impacts finances, privacy or safety by visually emphasizing other information.
- **No nagging** [Needs more Research]- Once a user declines a request, the system does not ask again.
    - **Test**:
        - Check if the system asks the user to do anything such as sign up, log in, disable ad blockers, turn on their camera, etc.?
        - Check that once the user has stated they do not want to take that action, does the computer continue to ask?

Assertions

- User testing with people with cognitive disabilities is used to confirm that deceptive patterns are not used.
- Check interface against common deceptive patterns
- Usability testing has been conducted with people with cognitive and mental health related disabilities to assure the process does not cause unnecessary anxiety and stress.

Questions:

- Is there a way to make Obstruction into a requirement? (steps/barriers between intent and completion)
- Is there a way to make tricking users into revealing more PII than they intended into a requirement?

Research

- Cognitive Accessibility Issue Papers - Online Safety and Wellbeing (Algorithms an…
- COGA 2 Literature Review and update
  Mental Health Literature Review (Responses)
- Proposed pattern and changes for Content-Usable version 3 (pulls our relevant research from mental health lit review spreadsheet)
- Supported Decision Making - Issue Paper (early draft
- Help-the-user-stay-safe-pattern in making content useable (COGA guidance document)
- Cognitive Accessibility Issue Papers - Online Safety and Wellbeing (Algorithms and Data)
- Deceptive Design
- Deceptive Patterns in UX: How to Recognize and Avoid Them - Nielsen Norman
- Series of Medium articles by Nadia Joy Doobal
  - Dark UX Tricks: Avoid Manipulative Patterns
  - Dark UX Patterns: Subtle Manipulations in Digital Design
  - The Hidden Complexity of Dark UX
- The Dark (Patterns) Side of UX Design
- Shining A Light on Dark Patterns (pdf)
- Dark Patterns and User Mental Health: Identifying Theoretical Impacts of Deceptive Design on Vulnerable Demographics
- Mobilizing Research and Regulatory Action on Dark Patterns and Deceptive Design Practices (pdf)
- Dark Patterns and the Emerging Threats of Deceptive Design Practices
- Appropriate Tone: https://www.w3.org/TR/wcag-3.0/#appropriate-tone
- Clear Operation (User Story): https://www.w3.org/TR/coga-usable/#clear-operation-user-story
- Deceptive Patterns Tweets (examples of possible deceptive patterns and anti-patterns - w/some bias)
- Keeping Children Safe Online
- Preventing Online Harm and Abuse
- UK Online Safety Act 2023
- Kids Online Safety Act (proposed, US)
- NDIS Privacy Easy Read

Research

- Deceptive controls
- Exploitive behaviors
- Misinformation
- Preselections
- Redirection

- Obscuring primary content

- **Misleading Button Labels:** Some websites or applications can use deceptive button labels to make users perform unintended actions. For instance, a “Free Download” button may actually redirect users to a paid subscription.
- **Hidden Opt-Out Settings:** Many services allow users to automatically accept certain settings. However, changing or disabling these settings can be challenging for users.
- **Complex Opt-In and Opt-Out Options:** Some services may use complex approval or cancellation buttons to persuade users to accept or cancel an unwanted condition. Users may be at risk of performing an unwanted action.

https://medium.com/design-bootcamp/deceptive-ui-examples-of-misleading-user-interface-designs-19676a5163a1

Guideline: Citations and 3rd Party Content

Guideline: Citations and 3rd Party Content

NOTE: These need more research before we write standards for them.

Foundational Requirements

Supplemental Requirements

Questions:

Research

- Series of Medium articles by Nadia Joy Doobal
    - Dark UX Tricks: Avoid Manipulative Patterns
    - Dark UX Patterns: Subtle Manipulations in Digital Design
    - The Hidden Complexity of Dark UX

Prevent Harm Scratchpad

Outcome: Visually and programmatically cite the source of the interface and primary content

- **User Need:** As a person with a cognitive disability, I need to understand where content comes from and how well I can trust it

Outcome: Visually and programmatically indicate the existence and source of all third party content (AI, Advertising, etc).

    - **User Need:** As a person with low vision, I need it to be visually clear which actions are disguised advertisements trying to get me to follow a different path rather than the action that I need to use in order to complete a task.

Guideline: Clear Agreement and Risk Statement

Guideline: Clear Agreement and Risk Statement

Users understand the benefits, risks and consequences of options they select.

Foundational Requirements

- **Agreement Indicated**: The interface indicates the legal, financial, privacy or security related consequences, before a user enters a legal, financial, privacy, or security related agreement.
    - Test
        - Check if a user is entering legal, financial, privacy, or security related agreements.
        - Check that the user is notified about the agreement before finalizing the agreement.
- **Comparable risk**: When people with disabilities are required to use alternative or additional processes or content not used by people without disabilities, use of the alternative does not expose them to additional risk.
    - Test
        - Check if people with disabilities are required to use an alternative or additional process
        - Check that the alternative does not expose them to additional legal, financial, privacy or security risks

Supplemental Requirements

- **Risk Statements**: The interface states the benefits, risks and potential consequences of choices.
- ~~**Correct Mistakes**: A process and instructions are available for users to correct mistakes.~~

Questions:

Research

- Making Content Usable

Clear Agreement: The interface indicates when a user is entering an agreement or submitting data.

Risk Statements: Clear explanations of the risks and consequences of choices, including use, are stated.

Definitions

- Financial
    - (Cambridge) -**relating to money or how money is managed**
    - Likely use the normal definition for this term
- Legal
    - **legal commitments**
        - transactions where the person incurs a legally binding obligation or benefit (WCAG 2.2)

- Privacy
    - that affect private and sensitive information (see shared glossary)
- Safety
    - Accidental harm
    - Individual's health (Physical safety)
- Security
    - International harm
    - IT - protection against intentional attacks and unintended vulnerabilities
    - Information/data

Digital Accessibility Framework

- For systems that collect private information, people with disabilities may need the system to protect their privacy, even when they are not doing things that other users might be expected to do to guard their own privacy.

- People may need to be able to use products without the fear of negative consequences if they make mistakes.
- People may need the system to provide an appropriate level of safety (including physical safety, and safety of my data, finances, legally, etc.).
- For systems that collect private information, people with disabilities may need the system to maintain my privacy and provide them the same amount of control of their personal information/privacy as other users.
- For systems that include hazards, people may need the hazards to be obvious, easy to avoid, and difficult to trigger.
- For systems that collect private information, people need positive assurance that sensitive information they enter, such as password or national ID, is not displayed on the screen.
- For system the presents content and other stimuli, people may need alternative versions of content that do not rely on a specific sense to avoid injury.

Guideline: Obstruction

Guideline: No Obstruction

User interface components and navigation must be operable and must be presentable to users in ways they can perceive without obstruction.

Foundational Requirements

- **No Obstructions** - Content that is essential for a user's task or understanding is not permanently covered by non-dismissible or non-movable elements.
    - **TEST**
        - Does the overlay obscure or obstruct a task or content? (No, pass; Yes, stop/fail)
        - Is the overlay dismissable or moveable for task completion or not to hinder visual elements? (No, stop; Yes, pass)
- **Clearly Dismissable Content Overlays** - When content temporarily overlays other content, it must be clearly dismissible or movable via standard interaction methods and its presence does not disrupt critical screen reader announcements or keyboard focus.
    - **TEST**
        - Does the content overlay obscure or obstruct a task or content? (No, pass; Yes, stop/fail)
        - Is the content overlay dismissable or moveable for task completion or not to hinder visual elements? (No, fail; Yes, pass)
- **No Audio/Video Content That Obscures** - Audio or video content that covers other content should have clearly visible and immediately accessible controls to pause, stop, or dismiss.

If any audio on a web page plays automatically for more than 3 seconds, either a mechanism is available to pause or stop the audio, or a mechanism is available to control audio volume independently from the overall system volume level.

    - **TEST**
        - Does the audio/video component ~~that is interactive~~ cover or obscure other content? (No, keep going. Yes, fail)

        - Does the audio/video component have a visible mechanism to pause, stop, or dismiss the audio/video? (No, fail. Yes, keep going)
        - Does the audio/video component have visible and accessible controls to pause, stop, or dismiss the video? (No, fail. Yes, pass.)
- **Disabled Controls** - The presence and appearance should not impede a user's overall operation of the system by causing confusion, frustration, and forced to guess why something isn't working, wasting cognitive effort.
    - **TEST**
        - Are the controls clear to the user visually and use clear labeling? (No, fail. Yes, keep going.)
        - Is there assistance via helper text or prompts to guide a user to use the controls without impeding the operation? (No, fail. Yes, pass.)
        -

Supplemental Requirements

- **Stable Layout** - Content should not shift or reflow in a way that causes users to lose their place or makes previously visible content inaccessible without explicit user action. (anti-pattern)
- **Consistent Positioning of Persistent Elements** - If elements are designed to be persistent (e.g., sticky headers/footers), their position should be predictable and not overlap with primary content in a way that makes it unreadable or unusable. (deceptive pattern/anti-pattern)
- **Avoid Unnecessary Zooming** - Obstruction can occur if content forces excessive horizontal scrolling or requires constant zooming to view due to poor responsiveness or fixed layouts that don't adapt to different screen sizes. (anti-pattern)
- **Contextual Explanation for Disabled State** - If a control is disabled, there must be clear, concise, and immediately perceivable information explaining why it is disabled and what actions the user needs to take to enable it. (deceptive pattern/anti-pattern)
- **Implicit Misdirection:** The design should avoid scenarios where disabling a control implicitly suggests a false pathway or intentionally hides the correct one. (deceptive pattern)

- **Clear Error Identification and Description** - If a user attempts to complete a task and a control is disabled due to an error, the error must be clearly identified and described, in text, telling the user how to fix it. (deceptive pattern/anti-pattern)
- **No Infinite Scrolling** - Obstruction can occur if content forces excessive scrolling, creating an infinite scroll to keep the user engaged. (deceptive pattern/anti-pattern)

Best Practices:

- **Critical Content and Controls are always unobstructed**
- **Focus Indicators and Interaction are always visible and clear**
- **Content order and reading order are maintained**
- **Semantic Structure and Programmatic Access are Not Compromised**

Questions:

- Where is the overlap re: other guidelines and does the overlap apply in this guideline?

Research:

- Obstruction - Deceptive Design by Harry Brignull
- FTC v. Amazon.com Inc.
- State of Arizona, ex rel. Mark Brnovich, Attorney General v. Google, LLC
- Roach Motel Dark Pattern: Understanding Its Impact on Users
- STATEMENT OF COMMISSIONER ROHIT CHOPRA Regarding Dark Patterns in the Matter of Age of Learning, Inc.
- Chapter 13: Introducing the Mathur et al. taxonomy by Harry Brignull
- Chapter 19: Obstruction - Deceptive Patterns by Harry Brignull
- Amazon: How to cancel Audible subscription?
- StubHub: Dark patterns in event ticket sales
- Roach Motel on Dark Patterns
- Hard to cancel - Deceptive Patterns by Harry Brignull

- Mathur, Arunesh & Mayer, Jonathan & Kshirsagar, Mihir. (2021). What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods. 10.48550/arXiv.2101.04843.

Definitions:

-

Levels of Conformance (Draft - Subject to further WCAG 3.0 modeling)

- **Bronze:** Basic prevention of severe and frequent obstructions.
- **Silver:** Addresses common obstruction scenarios and provides mechanisms for users to manage less severe obstructions.
- **Gold:** Ensures a highly predictable and obstruction-free experience, with user control over all dynamic elements.

To Do

To Do List

Define Diverse Disabilities (diverse range of disabilities include: including individuals with cognitive and learning disabilities and mental health conditions … to be worked on)

Work with, browsers, platforms APA, ADAPT and COGA on global privacy settings such that When a global setting on privacy is available , sites and apps can use it. . The application can let the user override the global setting, and an icon or other unobtrusive method can alert the user that the global setting is being used. (note that the platform could use this to identify bad actors and warn other users)

Meeting Minutes

Meeting Minutes

Participants

Todd Libby (Facilitator)
Lisa Seeman-Horwitz
Mary Jo Mueller
Rachael Montgomery
Azlan Cuttilan
Jaunita Flessas

21 January 2025

- **Participants: Todd, Rachael, Mary Jo, Azlan**
- Todd kindly facilitating
- Second Meeting on Tuesdays at 10 Eastern (directly before AG)
- Began compiling resources
- Start with grouping of:
    - Disability information privacy
    - Sensitive information
    - Risk statements

28 January 2025 (10:00)

- **Participants: ?**
- Decided to focus on information privacy
- Began collecting research on accessibility and information privacy

4 February 2025

- **Pre-AG Meeting:** Continued work on sensitive information and disability information privacy
    - **Participants: Todd, Lisa, Rachael, Mary Jo**
    - User needs added
    - Get Lisa up-to-speed with what we have been working on and the structure to what we are doing.
- **AG Breakout room:**
    - **Participants: Todd, Rachael, Mary Jo**
    - Discussion of the line between accessibility and security
        - Security requires the information be secure
        - Accessibility requires the user understand when their information is not secure/private and what they need to do to protect it

11 February 2025

- **Pre-AG Meeting:** Continued with work on the sensitive information and disability information privacy
    - **Participants: Todd, Rachael, Azlan, Jaunita**
    - Worked through some user needs wording
    - Decision tree material added
    - Foundational and Supplemental requirements added
    - Best Practices added
    - Assertions list underway
- **AG Breakout room:**
    - **Participants: Todd, Rachael, Azlan, Jaunita**
    - More discussion on user needs and the wording
        - Placement on which requirements fall under which categories
        - Wording the requirement(s)
        - Discussions on tone (if tone or language is harmful or inappropriate in certain situations)
            - disability privacy information and how that is impacted by UX tooling
            - data management
            - and access to information.

18 February 2025

- **Pre-AG Meeting:**
    - **Participants: Todd, Lisa, Rachael**
    - More work in the Decision Tree
        - Wording around requirements
        - Consolidate list of user needs
        - Discussions on what can be added or reworked with Lisa.

- **AG Breakout Room:**
    - **Participants: Todd, Rachael, Mary Jo**
    - Appropriate tone fits here or in Plain Language?

25 February 2025

- **Pre-AG Meeting:**
    - **Participants: Todd, Azlan**
    - Worked on examples and discussed good examples to showcase.

- **AG Breakout Room:**
    - **Participants: ??**

4 March 2025

- **Pre-AG Meeting:**
    - **Participants: Todd, Lisa, Azlan, Rachael**
    - Finding more bad examples of information privacy
    - Alternative decision tree work

- **AG Breakout Room:**
    - **Participants: Todd, Azlan, Rachael**
    - Take 3 Alternative tree work

11 March 2025

- No meeting (CSUN)

18 March 2025

- **Pre-AG Meeting:**
    - **Participants: Todd,**
    - More work on Take 3 Alternative tree

- **AG Breakout Room:**
    - **Participants: Todd,**
    - Researching bad examples of privacy information anti-patterns.

25 March 2025

- **Pre-AG Meeting:**
    - **Participants: Todd, Azlan**
    - Reorganized Current Applicability Tree, definitions linked to Shared Glossary
    - Prepare for next guideline (Algorithm Accessibility)

- **AG Breakout Room:**
    - **Participants: Todd, Rachael**
    - Edit and finish Current Applicability Tree - Information Privacy
    - Begin work on Algorithm Accessibility

1 April 2025

- **Pre-AG Meeting:**
    - **Participants: Rachael, Todd, Azlan**
    - Definitions linked to Shared Glossary for Private & Sensitive Information
    - Writing Methods underway

- **AG Breakout Room:**
    - **Participants: Rachael, Todd, Azlan**

    - Methods work

8 April 2025

- **Pre-AG Meeting:**
    - **Participants: Rachael, Azlan**
    -

- **AG Breakout Room:**
    - **Participants: Rachael, Azlan**
    - Help from members of other subgroups

15 April 2025

- **Pre-AG Meeting:**
    - **Participants: Todd, Azlan**
    - Worked on a couple more items in the decision tree
    - Bring Todd up-to-speed from last week.

- **AG Breakout Room:**
    - **Participants: Todd (½ meeting), Azlan, Mary Jo, Juanita Flessas**
    - Worked on Applicability Tree items

22 April 2025

- **Pre-AG Meeting:**
    - **Participants: Todd**
    - Access to Information and Data Management applicability tree work.
    - Read Github repo from Harm From Motion Subgroup to see if we needed to pull anything from that repo
        - Todd read through the repository and did not see anything that was consistent with use in this subgroup from the Harm From Motion subgroup.
        - Todd split up categories and made separate applicability tree

- **AG Breakout Room:**
    - **Participants: Todd, Rachael**
    - Decided on async work best for group, when we can get together we can
    - Update from Todd to rachael
    - Todd's email may be going into spam folders if group members could check so that communication from Todd is not missed.

Survey Questions (Safety & Deception Outcomes)

Deceptive Patterns Objections Items for discussion

All these I (Todd Libby) feel have safety issues which are in the Conformance Summer 2025 Slides (Level Exercise), all are likely to prevent task completion even with AT support, All have impact and maybe universal applicability. I would also call on subgroup members to weigh-in as well. rachaellbradley@gmail.com azlan.cuttilan@gmail.com

How do we make them testable is the one hurdle that I feel that is possibly what needs to be overcome but these are crucial to accessibility on some level.

Unnecessary steps (Supplemental)

1. *Roach motel example/forced continuity:* The steps that a user has to go through to unsubscribe from a newsletter or service because the organization wants to keep them as a customer/follower. e.g., Deactivating an account and having to fill out a reason and submitting that form. Unsubscribing from a newsletter and having to contact support or email support.
   "Unnecessary" can be termed as: "*Unnecessary steps are steps that are added in the process of the user being able to quickly and efficiently perform a task (such as unsubscribing, canceling, confirmshaming, or forced continuity when they are not notified of a trial ending)."*
   Unnecessary covers tactics that obscure cancellation options, auto-renew without clear consent, or make cancellation/deletion of accounts difficult for users regardless of ability.
   Usually the roach motel and forced continuity go hand-in-hand and have a huge impact on accessibility.
   - The NY Times had a process when the user wanted to cancel but the page to cancel from offered up an "are you sure" guilt trip and a button taking the user back to their account and then if the user still wanted to cancel, the user would have to contact Customer Care, which operated during certain hours of the day.
   - Facebook still has extra steps that the user has to perform to deactivate an account which is still not entirely deactivated and even after the 30/60/90 days of the account being inactive, one can go in and reactivate the account.
   - Amazon had a four-step process to cancel an account (and still it is a rigamarole) for users that no longer wanted to use or needed to use the service.
   - FTC's "Click to Cancel" rule was a start but that did not cover international entities and the Click to Cancel rule has been voided due to lobbying. Citing the Amazon example, not only was it not enforced, but the scope of the rule was too broad.

References:
https://www.nixonpeabody.com/insights/articles/2025/08/27/click-to-cancel-vacated-whats-next-for-businesses

Respondents to address: jrawe@understood.org alastair.campbell@thisisgain.com : wilco.fiers@deque.com gundula.niemann@sap.com cpandhi@paciellogroup.com bruce@bailey4.us

Julie: Unnecessary would apply to steps that take the user off a path that they were originally intended to maintain. Julie wants to cancel her account but has to take an added three steps because the company keeps asking her in a multi-step form if she is sure she wants to delete her account.

Bruce: I don't see how all users would desire added steps in a process to complete a set path to cancel an account or unsubscribe from a newsletter. An actionable measurement I can think of is setting a baseline of what a reasonable, non-deceptive flow would require. What is that number being the argument? The answer should be one to get to the unsub/delete page, two to click, and perhaps three to acknowledge the action and that is it.

Wilco: I don't think flows such as Amazon, Facebook, Instagram, or any other similar company with an extended number of clicks to wear and tire a person out could ever be considered necessary. Neither have the hundreds of people I have surveyed either.

There are plenty of cases where organizations take advantage of this deceptive pattern to wear people out so they quit and stay with their subscription or keep their account active. This is not about the legality or regulation, it is about the user deciding what is necessary and putting that power into their hands through accessibility.

Gundula: I have started with this definition as a base, "*Unnecessary steps are steps that are added in the process of the user being able to quickly and efficiently perform a task (such as unsubscribing, canceling, confirmshaming, or forced continuity when they are not notified of a trial ending).*"

Alastair: Unnecessary to the user as I mentioned to Wilco's argument.

I am fine with supplemental. It should not be tossed away because it is something that causes harm. Stress, anxiety, and that could lead to something more.

No misleading wording (Foundational)

The argument that double negatives are essential for a specific tone or to convey a nuanced meaning is often a matter of stylistic choice, not necessity. In most cases, a double negative can be rephrased as a positive statement without losing meaning, and in doing so, the message becomes more accessible.

While it's true that purely automated tools can't perfectly test for the nuance of misleading wording, a combination of methods can be used to evaluate and ensure compliance. WCAG 3 proposes a more holistic, outcome-based approach, moving beyond simple pass/fail criteria.

- **Qualitative and Quantitative Testing:** Guidelines can be created with a scoring system based on a combination of automated checks (e.g., flagging sentences that contain "not" and "un-") and qualitative human-based testing. Qualitative tests would involve having a diverse group of users, including those with cognitive disabilities, read and interact with the content to identify and score areas of confusion or deception.
- **Usability Testing:** Observing how users interact with a site is the most effective way to identify misleading wording. If users are consistently clicking the wrong button, entering incorrect information, or abandoning a process, it's a strong indicator that the language is not clear or is intentionally deceptive.

Impeding on a writer's style is a common argument (labels, headings) against many guidelines. Accessibility standards are not meant to stifle creativity but rather to ensure that essential information is conveyed clearly. We are aiming to address this by focusing on ***outcomes*** rather than prescribing rigid methods.

A writer is still free to use creative or complex language for non-critical content, like marketing copy or blog posts. The guidelines would be most critical for transactional and functional content, e.g., forms, error messages, and navigation instructions, where clarity is paramount to the user's ability to complete a task. The goal is to prioritize clarity and functionality where it matters most, without dictating a writer's style.

Defining specific issues or examples is what is done regularly by the W3C. We have a glossary of terms, we have a shared glossary we are working on and writing. If we are creating a glossary of terms, then definitions regarding what is misleading should be debated and agreed upon in the W3C. We did this with the whole "view/component/etc." debate.

1. *Trick wording examples:*
    - From 2010 to 2013, low-cost airline Ryanair used the trick wording deceptive pattern. During the flight booking process, Ryanair presented users with the instruction "Please select a country of residence" written prominently on a dropdown menu. If read on its own, users were likely to just select their country of residence from the dropdown and continue with their booking process. However, in doing so they would have inadvertently purchased travel insurance.
      https://www.deceptive.design/types/trick-wording
      For a user to choose not to purchase travel insurance, they were required to open the dropdown and scroll down to the label "No travel insurance required" which was nonsensically listed between two countries: Latvia and Lithuania. Ryanair combined trick wording with the visual interference deceptive pattern to confuse and misdirect users.
      Trick wording and visual interference are also an example of more than one deceptive pattern being used in harmony to deceive a user.
    - Credit Karma was fined for using false "pre-approved" claims, to entice consumers into applying for credit card offers they often did not qualify for.
      https://www.deceptive.design/cases/in-the-matter-of-credit-karma

- TikTok was fined by the Dutch DPA for violating GDPR Article 12(1) by providing its privacy policy solely in English to Dutch users, many of whom are children under the age of 16.
  https://www.deceptive.design/cases/tiktok-s-ex-officio-investigation-by-dutch-dpa
- Example: *"Would you prefer not to opt out of email notifications?"*
  This convoluted phrasing forces users into mental gymnastics to determine their desired action. A better approach is to simplify and clarify the language, such as: *"Sign me up for email notifications"* or *"No, I don't want updates."*
- Example: *"Don't allow us to not collect your data?"*
  Double negatives confuse users and increase the likelihood of unintended selections. Replace them with straightforward phrasing, like: *"Allow us to collect your data: Yes/No."*
- Example: *"Click OK to continue"* (with hidden terms in fine print).
  Businesses should avoid masking consent or terms in ambiguous prompts. Instead, explicitly communicate what the user is agreeing to, such as, "Click *OK to agree to share your data with third parties."*

Julie: I think this would be an assertion because I know of no tests for this.

Bruce/Wilco: The argument that double negatives are essential for a specific tone or to convey a nuanced meaning is often a matter of stylistic choice, not necessity. In most cases, a double negative can be rephrased as a positive statement without losing meaning, and in doing so, the message becomes more accessible.

The ACT example is an example of how it works for an organization that is not trying to mislead or deceive people. In the cases of a deceptive pattern, this is all about misleading people and tricking people to possibly make a financial decision they may not be able to make confidently or may not be able to afford at all when hidden costs come into play.

Again, turning a double negative into a positive statement can make the wording more accessible and does not limit free speech at all, it removes the opportunity for organizations to deceive users.

I don't see a tool for making a website accessible as far as automatic scanning. Yet we rely on those tools to do some of the heavy lifting. Whether it is Axe, WAVE, Accessibility Insights, IBM Equal Access, ARC, Playwright, Jest, or any other automatic checker, there is never one "right" tool for the job because they all differ in results here and there.

Gundula: Misleading: "*The use of language to intentionally confuse, deceive, or manipulate a user into taking an action they didn't intend to."*

Alastair: I don't think this impedes any sort of writing style other than someone trying to deceive a person for financial gain using deceptive patterns. A schoolteacher updating something in a CMS is on the other end of the spectrum, as opposed to someone creating copy to confuse, deceive, and lie to someone for financial gain.

I agree with Rachael this should be Foundational but I'm fine with supplemental level here also.

No artificial pressure (Foundational)

1. *Fake urgency:*
    - The Shopify app "Hurrify" could be used to create various fake urgency messages, one of which was a fake countdown timer. A user typically saw a site that uses the Hurrify countdown timer. It's very prominent, animated and claims that the sale will end once the timer hits zero. However, the admin interface for sellers has (they are still in business) a default configuration to *"Run the campaign all over again"* which means that the counter simply resets when it reaches zero. Which is commonplace for a lot of these timers that are used to promote fake urgency to sell. Hurrify has been banned from the Shopify app store.
    - Ticketmaster uses a 15 minute countdown timer to rush the user into a decision before they have to start the process all over again from the start of the ticket transaction if they do not make a decision quick enough.
    - Vermont held AdoreMe liable for hidden subscriptions, misrepresenting time-limited discounts, and obstructing subscription cancellations. https://www.deceptive.design/cases/in-the-matter-of-adoreme-inc
    - Nintendo faces a class action lawsuit over allegedly compelling players to make in-game purchases by creating hurdles for non-buyers and employing fake limited-time offers. https://www.deceptive.design/cases/n-a-through-his-guardian-v-nintendo-of-america

Julie:

> **Essential** - A countdown to a live webinar, livestream, conference start time or seasonal event like a holiday sale. Ticket or seat reservations (contingent on progression-based), shipping deadlines or online exam timers.
>
> **Artificial** - "Flash sale" timers that never expire, Scarcity timers (Hurry, only 2 left!), cart expiration timers to force users to end the checkout process and spend money, repeating or rolling timers for discounts which are used prominently.

Wilco: A lot of these timers, especially when it comes to less than reputable organizations are most of the time, artificial and deceptive (cite the Shopify plugin case). Even the more prominent companies (read Nintendo or Ticketmaster cases) use or used these patterns to their advantage financially. This is trying to close that loophole as much as possible.

Gundula: Anything that would have to do with security, like a quiz or test for an employee who is taking a security course during their onboarding at a new job, would be considered essential. Artificial time limits are the target here, the timers and the deception to force a user to spend time and money for financial gain which has to do with the user's security, not the organization.

Alastair: I still think this can work and be accessible as there are accessible examples we see. The incentive is to minimize impact and the impact on mental health (stress, anxiety, etc.). Artificial pressure is a risk that the work in deceptive patterns and making UX usable and accessible are trying to address.

Charu:

Artificial time: *“Timers that create a sense of false urgency. preying on a user's fear of missing out to rush them into a decision. The time limit is not real and serves only to manipulate the user.”*

I agree with Chuck that this should be Foundational level.

_____

With the deceptive patterns, I hoped we could bring forth guidelines to WCAG 3 that promoted the “solve for some, extend to all” approach accessibility has for everyone.

While we cannot ensure the safety of people with disabilities, the guidelines promote the idea of “making the digital spaces PWD visit accessible and accessible for all.” approach. So too does this work, which extends beyond the constraints of the 2.x set of guidelines.

I encourage everyone to browse through and read the Deceptive Design website https://deceptive.design to not only get more familiarized with these deceptive patterns, but the legal cases that are in the past and ongoing. I think having a broader aspect and outlook to this work is crucial in understanding more of the work and research behind this by many people and the Safety & Deception subgroup.

Email’s sent out 9/11/2025

Julie Rawe:

Hi Julie, apologies for the delay in response. I figured you were speaking on your behalf and not COGA, so thank you for clarifying that.

I think a joint meeting between us and COGA would be great and I believe both Rachael and Azlan do too. We meet one hour before the AG meeting on Tuesdays.

I can email the subgroup and see if they would like to join in on the COGA meeting. I think that may work better, but I will ask first.

I can then go over the items you responded to in the meeting and get your group members to weigh-in on what we are trying to do. Which is, I feel very strongly about leaving these in WCAG 3

and not tossing them aside, no matter if they are best practice, assertion, or Supplemental/Foundational.

Bruce Bailey:

Hi Bruce,

I wanted to reach out and respond to your comments on the survey here: https://www.w3.org/wbs/35422/requirement_levels/results and address your concerns and see if we could talk through this in some form.

This might be a lot, so I will try to keep this as brief as I possibly can.

Unnecessary Steps (https://www.w3.org/wbs/35422/requirement_levels/results/#xq9):

You wrote: *"I would remove this as it seems desirable for all users, and I can't conceive how to test it. I agree that unnecessary steps have disproportionate impact to PWD and users of AT, but how would that be measured in an actionable way?"*

I don't know how to test for this either but I also haven't found time to sit down and actually think about this yet or take this back to the group yet as well. My intent on bringing this to WCAG 3 was the research I have done between cognitive load and click rates.

I think this is something that I'd also bring to COGA to see if they have done anything with this or not. We are planning a joint meeting at some point.

My definition I would bring to people is,

"*Unnecessary steps are steps that are added in the process of the user being able to quickly and efficiently perform a task." (Such as unsubscribing, canceling, confirmshaming, or forced continuity when they are not notified of a trial ending)*

I am fine with this being "Supplemental" or whatever term we will use, if there is a measurable way found to test for this. Otherwise, I am going back-and-forth between assertion and best practice.

No misleading wording (https://www.w3.org/wbs/35422/requirement_levels/results/#xq10):

You wrote: *"I would not have double negatives in same category as "false". Never no double negatives is too strict, but might be supplemental. False or misleading wording better addressed by other regulation."*

The wording isn't grouped into "false" as much as it is grouped into "deceptive" which the work done by many have categorized these patterns as deceptive. The people that make the marketing that uses double negatives would probably not care but that's not an assumption I'd bet on.

I do, however, feel that double negatives are essential for a specific tone or to convey a nuanced meaning which are often a matter of stylistic choice, not necessity. In most cases, a double negative can be rephrased as a positive statement without losing meaning, and in doing so, the message becomes more accessible.

"Would you prefer not to opt out of email notifications?" can be better framed as, *“Sign me up for email notifications”* or *“No, I don’t want updates.”* Or, *“Don’t allow us to not collect your data?”* can easily be written straightforward as, *“Allow us to collect your data: Yes/No.”*

Also covered are

“Click OK to continue” (with hidden terms in fine print) but instead, explicitly communicate what the user is agreeing to, such as, “Click *OK to agree to share your data with third parties.”*

Other than the legal cases that are currently in courts around the world, I don't see any other regulation and have seen none that address these types of deceptive patterns. Testing for this is also a question I have as to "how do we test for this?" which is something I want to research more of.

I know that there is a lot of research to do with the testability of these things on our level and would like to have these remain in our work towards WCAG 3. I think these are crucial to preventing harm and a lot of these are intertwined which fills holes in the gaps that the current guidelines have in them on the usability/UX front.

Thanks and I look forward to your thoughts.

Wilco Fiers:

HI Wilco,

I wanted to reach out and respond to your comments on the survey here: https://www.w3.org/wbs/35422/requirement_levels/results and address your concerns and see if we could talk through this in some form.

This might be a lot, so I will try to keep this as brief as I possibly can.

Unnecessary Steps (https://www.w3.org/wbs/35422/requirement_levels/results/#xq9):

You wrote: *"I don't see how an outcome like this could ever work. There is no objective way of deciding what is and isn't necessary. There are all sorts of motivations that drive people / organizations to ask for stuff. Some legal, some policy, some to get a more complete picture in my data. Who gets to decide what is necessary?"*

My definition I would bring to people is,

“Unnecessary steps are steps that are added in the process of the user being able to quickly and efficiently perform a task." (Such as unsubscribing, canceling, confirmshaming, or forced continuity when they are not notified of a trial ending)

I think there is an objective way to look at these patterns because in legal circles, the courts US/International are looking at these. A lot of these. In the EU, with the Consumer Rights Directive (CRD) and the Unfair Commercial Practices Directive (UCPD), as well as the Digital Services Act (DSA).

The FTC here in the US was doing a lot of work with this during the Biden administration, but as we know, things have changed dramatically here, so the future is uncertain. We had the "Click-to-Cancel" rule that was about to take effect but days before that, it was squashed due to lobbying by organizations that thought it was too broad or strict (meaning they could not make money off keeping people deceived and stuck in a subscription or being an account holder).

I'm not saying the W3C be the deciders of what is and what is necessary, rather I am asking that we include this so that people think about these things before they create these deceptive patterns.

We already have the courts deciding what is unnecessary, whether that is enforced or not remains to be seen.

No misleading wording (https://www.w3.org/wbs/35422/requirement_levels/results/#xq10):

You wrote: *"Double negatives are quite different from false statements and misleading wording.*

On double negatives; while a I appreciate the problem these might create, they are often necessary. ACT has lots of them for example. "Not empty" for example is a very common one. We use that because it is the clearest way we could come up with to express that concept. Avoiding double negatives is a good idea, prohibiting double negatives is definitely not.

As for false statements and misleading wording, I don't think that belongs in WCAG. Accessibility is about access to information and functionality. While people with disabilities can be more vulnerable to false and misleading information, I don't believe WCAG is the right tool for tackling that particular problem. There are consumer protection and disability rights laws around the world for that. This outcome seems like it would limit free speech, which seems like a highly problematic thing for AGWG to attempt."

I agree that double negatives are not like misleading wording or false statements.

I do, however, feel that double negatives are essential for a specific tone or to convey a nuanced meaning which are often a matter of stylistic choice, not necessity. In most cases, a double negative can be rephrased as a positive statement without losing meaning, and in doing so, the message becomes more accessible.

"Would you prefer not to opt out of email notifications?" can be better framed as, *“Sign me up for email notifications”* or *“No, I don’t want updates.”* Or, *“Don’t allow us to not collect your data?”* can easily be written straightforward as, *“Allow us to collect your data: Yes/No.”*

Examples also include,

“Click OK to continue” (with hidden terms in fine print) but instead, explicitly communicate what the user is agreeing to, such as, “Click *OK to agree to share your data with third parties.”*

Your example of the usage of double negative with the ACT, while I understand that I have to argue that the ACT is not trying to deceive people to maintain an account with the ACT, or keep someone in a subscription to the ACT. In short, the ACT doesn't use double negative to trick or deceive people for financial gain.

It is not as much prohibiting double negatives as much as it is promoting using positive statements to make messages more accessible on the cognitive side as well as all-around.

As for false statements and misleading wording, I again point to promoting the use of positive writing to make things more accessible. I think the argument of free speech does not apply here at all, that is an entirely different subject.

The rights and laws around the world are there, but are they being enforced? Somewhat. Legal cases I have researched are finally addressing that over the past few years, but governing bodies as far as I know aren't really putting a clamp on the deceptive practice. That might be an oversight on my part because I live in a country that is chock full of these patterns, I don't know.

As for WCAG being the "right tool" I don't think there is a right tool for anything really. Even in an accessibility audit, is Axe the right tool? Is ARC or WAVE? Playwright or Jest? I think we can set a standard here though and not make it as much as a tool, but rather a foundation for mitigating deceptive patterns like these.

I agree with Rachael that this should be on the Foundational level, but I am not opposed to it being Supplemental.

No artificial pressure (https://www.w3.org/wbs/35422/requirement_levels/results/#xq11):

You wrote: *"I don't think this works. The most common problem of these is organizations freezing a price for you for a certain time, and telling you when this time expires to pressure you to decide fast. That time limit is not artificial. The price COULD change after the time expires. The loophole in this outcome is large enough to let just about any site that does this pass anyway."*

I have many examples and there are a lot of examples how artificial these timers can be. One in particular was the Shopify app “Hurrify” could be used to create various fake urgency messages, one of which was a fake countdown timer. An admin could go in, and restart the timer. The app is not in

Shopify's app store any longer, but they do still have the app available through the company that makes it.

Nintendo was sued for creating fake limited-time offers so that players would make in-game purchases (allegedly). I have split what is essential and what is artificial into a couple groups using a few examples to start with:

Essential - A countdown to a live webinar, livestream, conference start time or seasonal event like a holiday sale. Ticket or seat reservations (contingent on progression-based), shipping deadlines or online exam timers.

Artificial - “Flash sale” timers that never expire, Scarcity timers (Hurry, only 2 left!), cart expiration timers to force users to end the checkout process and spend money, repeating or rolling timers for discounts which are used prominently.

I hope this could close the loophole as much as possible and agree with Chuck that this should be on the Foundational level, but again, I am okay with it being Supplemental as well.

I know that there is a lot of research to do and would like to have these remain in our work towards WCAG 3. I think these are crucial to preventing harm and a lot of these are intertwined which fills holes in the gaps that the current guidelines have in them on the usability/UX front.

Thanks and I look forward to your thoughts.

Gundula Niemann:

Hi Gundula,

I wanted to reach out and respond to your comments on the survey here: https://www.w3.org/wbs/35422/requirement_levels/results and address your concerns and see if we could talk through this in some form.

This might be a lot, so I will try to keep this as brief as I possibly can.

Unnecessary Steps (https://www.w3.org/wbs/35422/requirement_levels/results/#xq9):

You wrote: *"The term "unneccessary" needs a clear definition and might still lead to strange results"*

My definition I would bring to the group is,

“Unnecessary steps are steps that are added in the process of the user being able to quickly and efficiently perform a task." (Such as unsubscribing, canceling, confirmshaming, or forced continuity when they are not notified of a trial ending)

This is a starting point and I would go over this definition with the Safety & Deception group in our next meeting to see if we could refine this.

I believe that to cut down on cognitive load, steps can be termed "unnecessary" which are found in these deceptive patterns and practices, as well as normal flows such as the one Amazon has used and currently uses to this day to minimize clicks and cognitive overload or repetitive strain for people with motor skill issues.

I can see this even being beneficial for users of assistive technologies.

No misleading wording (https://www.w3.org/wbs/35422/requirement_levels/results/#xq10):

You wrote: *"The term "mispleading" needs a clear definition, and whether wording is clear or not might depend on the context and target user base."*

I have as a starting point, “*The use of language to intentionally confuse, deceive, or manipulate a user into taking an action they didn't intend to.”*

I will bring this back to the Safety & Deception group as a starting point where we can refine this definition as needed. I believe wording can be made better by taking double negatives for instance and turning them into positive statements that can make them more accessible.

Some examples of misleading are, *"Would you prefer not to opt out of email notifications?”* can be better framed as, *“Sign me up for email notifications”* or *“No, I don’t want updates.”* Or, *“Don’t allow us to not collect your data?”* can easily be written straightforward as, *“Allow us to collect your data: Yes/No.”*

Examples also include,

“Click OK to continue” (with hidden terms in fine print) but instead, explicitly communicate what the user is agreeing to, such as, “Click *OK to agree to share your data with third parties.”*

I agree with Rachael that this should be on the Foundational level, but I am not opposed to it being Supplemental.

No artificial pressure (https://www.w3.org/wbs/35422/requirement_levels/results/#xq11):

You wrote: *"When is a time limit "artificial"? Not having any time limit might cause other issues, like security issues. I'd rework this."*

I have split what is essential and what is artificial into a couple groups using a few examples to start with:

Essential - A countdown to a live webinar, live-stream, conference start time or seasonal event like a holiday sale. Ticket or seat reservations (contingent on progression-based), shipping deadlines or online exam timers.If a timer is essential to a security risk, then it belongs here, but if used as a deceptive pattern, it would be classified as "artificial" as defined below.

Artificial - “Flash sale” timers that never expire, Scarcity timers (Hurry, only 2 left!), cart expiration timers to force users to end the checkout process and spend money, repeating or rolling timers for discounts which are used prominently.

I agree with Chuck that this should be on the Foundational level, but again, I am okay with it being Supplemental as well.

I know that there is a lot of research to do and would like to have these remain in our work towards WCAG 3. I think these are crucial to preventing harm and a lot of these are intertwined which fills holes in the gaps that the current guidelines have in them on the usability/UX front.

Thanks and I look forward to your thoughts.

Alastair Campbell:

Hi Alastair,

I wanted to reach out and respond to your comments on the survey here: https://www.w3.org/wbs/35422/requirement_levels/results and address your concerns and see if we could talk through this in some form.

This might be a lot, so I will try to keep this as brief as I possibly can.

Unnecessary Steps (https://www.w3.org/wbs/35422/requirement_levels/results/#xq9):

You wrote: *"Unnecessary to whom? Anything that that is more subjective moves into supplemental for me, possibly best-practice."*

My definition I would bring to the group is,

“Unnecessary steps are steps that are added in the process of the user being able to quickly and efficiently perform a task." (Such as unsubscribing, canceling, confirmshaming, or forced continuity when they are not notified of a trial ending)

This is a starting point and I would go over this definition with the Safety & Deception group in our next meeting to see if we could refine this.

I believe that to cut down on cognitive load, steps can be termed "unnecessary" which are found in these deceptive patterns and practices, as well as normal flows such as the one Amazon has used

and currently uses to this day to minimize clicks and cognitive overload or repetitive strain for people with motor skill issues.

I can see this even being beneficial for users of assistive technologies.

I am fine with this being Supplemental, best practice, yes but I think it fits more in the realm of Supplemental.

No misleading wording (https://www.w3.org/wbs/35422/requirement_levels/results/#xq10): AC

You wrote: *"If there were user-agent methods of achieving this it could be foundational, otherwise it's impinging on people's writing style, and easily tripped by less expert authors. E.g. the school teacher updating something in a CMS."*

I have as a starting point, "*The use of language to intentionally confuse, deceive, or manipulate a user into taking an action they didn't intend to.*"

I will bring this back to the Safety & Deception group as a starting point where we can refine this definition as needed. I believe wording can be made better by taking double negatives for instance and turning them into positive statements that can make them more accessible.

Some examples of misleading are, *"Would you prefer not to opt out of email notifications?"* can be better framed as, *"Sign me up for email notifications"* or *"No, I don't want updates."* Or, *"Don't allow us to not collect your data?"* can easily be written straightforward as, *"Allow us to collect your data: Yes/No."*

Examples also include,

"Click OK to continue" (with hidden terms in fine print) but instead, explicitly communicate what the user is agreeing to, such as, "Click *OK to agree to share your data with third parties."*

I believe this does not fit in with your example as a teacher is not actively looking to deceive students for financial gain. I don't believe this impedes on anyone's writing style other than the people that are writing these in a deceptive manner.

I don't feel that less expert authors would necessarily be affected by this because a blog author, for instance, is in most cases, not necessarily looking to deceive readers for financial gain. Not to say that possibility is not there at all because I can think of instances where it could apply like with content creators that aren't really acting with ethics in mind, but I do agree with you for the most part on this.

I agree with Rachael that this should be on the Foundational level, but I am not opposed to it being Supplemental.

No artificial pressure (https://www.w3.org/wbs/35422/requirement_levels/results/#xq11): AC

You wrote: *"If there were user-agent methods of achieving this it could be foundational, e.g. pop-up/ad blockers. Or even if things could be marked-up as non-critical to the task. The incentives are opposing each other though, so seems unlikely to work."*

I have split what is essential and what is artificial into a couple groups using a few examples to start with:

Essential - A countdown to a live webinar, live-stream, conference start time or seasonal event like a holiday sale. Ticket or seat reservations (contingent on progression-based), shipping deadlines or online exam timers.If a timer is essential to a security risk, then it belongs here, but if used as a deceptive pattern, it would be classified as "artificial" as defined below.

Artificial - “Flash sale” timers that never expire, Scarcity timers (Hurry, only 2 left!), cart expiration timers to force users to end the checkout process and spend money, repeating or rolling timers for discounts which are used prominently.

I agree with Chuck that this should be on the Foundational level, but again, I am okay with it being Supplemental as well but I lean more towards Foundational.

I know that there is a lot of research to do and would like to have these remain in our work towards WCAG 3. I think these are crucial to preventing harm and a lot of these are intertwined which fills holes in the gaps that the current guidelines have in them on the usability/UX front.

Thanks and I look forward to your thoughts.

Charu Pandhi:

Hi Charu,

I wanted to reach out and respond to your comments on the survey here: https://www.w3.org/wbs/35422/requirement_levels/results and address your concerns and see if we could talk through this in some form.

This might be a lot, so I will try to keep this as brief as I possibly can.

Unnecessary Steps (https://www.w3.org/wbs/35422/requirement_levels/results/#xq9):

You wrote: *"Can we define 'Unnecessary'?"*

My definition I would bring to the group is,

“Unnecessary steps are steps that are added in the process of the user being able to quickly and efficiently perform a task." (Such as unsubscribing, canceling, confirmshaming, or forced continuity when they are not notified of a trial ending)

This is a starting point and I would go over this definition with the Safety & Deception group in our next meeting to see if we could refine this.

I believe that to cut down on cognitive load, steps can be termed "unnecessary" which are found in these deceptive patterns and practices, as well as normal flows such as the one Amazon has used and currently uses to this day to minimize clicks and cognitive overload or repetitive strain for people with motor skill issues.

I can see this even being beneficial for users of assistive technologies.

No artificial pressure (https://www.w3.org/wbs/35422/requirement_levels/results/#xq11):

You wrote: *"Can we clarify 'Artificial time limits'?"*

Definition of 'Artificial': *“Timers that create a sense of false urgency. preying on a user's fear of missing out to rush them into a decision. The time limit is not real and serves only to manipulate the user.”*

I have split what is essential and what is artificial into a couple groups using a few examples to start with:

Essential - A countdown to a live webinar, live-stream, conference start time or seasonal event like a holiday sale. Ticket or seat reservations (contingent on progression-based), shipping deadlines or online exam timers.If a timer is essential to a security risk, then it belongs here, but if used as a deceptive pattern, it would be classified as "artificial" as defined below.

Artificial - “Flash sale” timers that never expire, Scarcity timers (Hurry, only 2 left!), cart expiration timers to force users to end the checkout process and spend money, repeating or rolling timers for discounts which are used prominently.

I agree with Chuck that this should be on the Foundational level, but again, I am okay with it being Supplemental as well.

I know that there is a lot of research to do and would like to have these remain in our work towards WCAG 3. I think these are crucial to preventing harm and a lot of these are intertwined which fills holes in the gaps that the current guidelines have in them on the usability/UX front.

Thanks and I look forward to your thoughts.

For Editor's Meeting

Revised Versions from Last Draft

Revised Guidelines, Etc

- **Unnecessary steps** - Unnecessary steps and inputs in a workflow are not included or are indicated visually and programmatically and a mechanism is provided to skip past the steps. (Supplemental)
- **Avoid misleading wording** - Content does not include double negatives or false statements. (Foundational)
- **Clear messaging** - Conduct a usability test that includes participants with cognitive disabilities and/or mental health based disabilities to evaluate content for misleading wording, artificial pressure, misdirection, and other deceptive practices. (Assertions)
- **Artificial Pressure** - Process completion does not include artificial time limits. (Foundational)
- **Changes in agreement -** Changes in terms of agreement to a continuing process, service, or task are conveyed to users and an opportunity to consent is given. (Assertion)
- **No hidden preselections -** Preselected options that impact finance, privacy, or safety are visibly and programmatically available by default, except when the user selected these options previously in the process. (Foundational)

Definitions

- **Unnecessary** - Optional pages, fields, components, information, or behaviors. When removed, neither the organization nor the user are prevented from completing the task or workflow. When removed, the task can still be completed.
- **Misleading wording:** Misleading: "*The use of language to intentionally confuse, deceive, or manipulate a user into taking an action they didn't intend to.*"
- **Double negative** - a positive statement in which two negative elements are used to produce the positive force, (Oxford languages)
- **Artificial time**: *"Timers that create a sense of false urgency, that preys on a user's fear of missing out to rush them into a decision. The time limit is not real and serves only to manipulate the user." This is in contrast to essential time limits tied to a time constrained event such as* a live webinar, livestream, or conference start time; a seasonal event like a holiday sale; ticket or seat reservations; shipping deadlines; or online exam timers.
- **Misdirection** - Content designed to draw attention away from information that impacts finances, privacy, or safety by visually emphasizing other information.