Manipulative Design Patterns in Cookie Notices on Media/News Websites

CMSC 33231: Combating Misleading Online Content (Fall 2023)

Danya Sherbini

1 INTRODUCTION

The concept of consent within the realm of data privacy is murky at best. Manipulative design patterns and other deceptive practices such as dense, lengthy privacy policies prevent users from truly understanding what their choices and trade-offs are with regards to their data privacy. Cookie consent notices are just one piece of the data privacy puzzle. But at the same time, they represent "low-hanging fruit" when it comes to privacy reform measures. Browsers like Safari and Firefox have already limited or banned the use of third-party cookies, and Google has claimed it will be following suit for Chrome (though the timeline for this has been delayed several times). With the introduction of the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA), and subsequent data privacy laws in states like Colorado, Connecticut, Utah, and others, there is potential for more comprehensive consumer privacy protections. As policymakers and other stakeholders attempt to influence state and federal approaches to this issue, a deeper understanding and analysis of these dark patterns is critical. In this project, I examine the cookie consent workflows of 10 news/media websites. I identify manipulative patterns used in these consent workflows and analyze their implications for user autonomy. I also evaluate these consent workflows for legal compliance.

2 BACKGROUND/RELATED WORK

There has been ample research on the topics of data privacy consent, manipulative patterns (commonly called "dark patterns"), and cookie notices. My project draws heavily upon existing literature and applies it to a selection of news/media websites.

2.1 Dark Patterns in Design

In *The Dark (Patterns) Side of UX Design* [2], Gray et al build upon the existing typology of dark patterns developed by Harry Brignull, focusing on five categories: nagging, obstruction, sneaking, interface interference, and forced action. Within each of these categories, they list design "strategies," some of which are pulled from Brignull's work (e.g. "roach motel") and some of which are new. They then use their new typology to perform a content analysis of a collection of exemplars shared by practitioners in order to discuss the ethical concerns of these designs.

2.2 Dark Patterns in Consent Pop-Ups

In *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence* [3], Nouwens et al scrape consent pop-up designs of the five most popular Consent Management Platforms (CMPs) and assess their legal compliance based on three minimum-threshold criteria laid out by GDPR: 1) consent must be explicit 2) accepting all is as easy as rejecting all 3) no pre-ticked boxes. They then run an experiment with 40 participants to examine how the 8 most common interface conditions (i.e., a combination of notification styles, bulk consent button options, and levels of consent granularity) affect user consent. The authors find that notification style (banner or barrier) has no effect, removing the opt-out button from the first page significantly increases consent, and providing more granular controls significantly decreases consent.

Gray et al also examine cookie consent notices in *Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective* [1]. This paper takes an interdisciplinary approach to its analysis of manipulative design choices regarding consent. The authors conduct an interaction criticism, analyzing design examples from different perspectives i.e., the designer, the interface, the user, and the social impact. The paper uses a taxonomy of four higher-level design pattern categories: obstruction, sneaking, forced action, and interface interference. The paper highlights the tensions, trade-offs, and complexities regarding consent and also bridges academic and public policy concerns by addressing possible solutions to ensuring informed user consent, such as standardization, "bright patterns," and educative nudges.

2.3 Alternative Naming Conventions to Dark Patterns

Dark patterns have also been dubbed "deceptive patterns" and "damaging patterns." In *Defining and Identifying Attention Capture Deceptive Designs in Digital Interfaces*, Roffarello et al call out the problematic conflation of "dark" with harm: this association may reinforce the racist heuristic of viewing people with darker skin tones as bad, lesser, or evil [4]. The authors call for a new name and settle on "damaging patterns." They opt not to use "deceptive patterns," first coined by Brignull, because not all the design patterns they examine are deceptive per se, but they all have a damaging effect on user attention capture. Drawing inspiration from Roffarello et al, I choose to use the term "manipulative patterns." Within the context of user consent and data privacy, not all dark patterns are necessarily damaging nor deceptive. However, they do all ultimately manipulate the user in one way or another. Additionally, in my discussion of "bright patterns" (see later section for more details), I opt to use the alternative term "privacy-friendly patterns." The "bright patterns" identified and described in this study may be neutral or pro-privacy, but they do not intentionally attempt to nudge a user towards giving consent. Thus, "privacy-friendly" is a broad enough term to apply to these design patterns.

3 GOALS AND RESEARCH QUESTIONS

The goal of this project is to identify manipulative patterns used in cookie consent workflows on 10 news/media websites, assess their legal compliance with GDPR, and discuss their implications for user autonomy. The research is guided by three key questions:

- **RQ1:** Which manipulative patterns and associated design strategies are present in these cookie consent notices?
- **RQ2:** Are these cookie consent notices legally compliant with GDPR?
- **RQ3:** What is the impact of these designs on user autonomy and choice?

4 METHODS

4.1 Identifying News/Media Websites

In order to make my project doable in the time allotted, I narrowed the scope of my websites to just news/media sites. Media websites have adopted new business models that monetize user information through the use of tracking cookies. To select my websites of interest, I researched the top news/media websites in the US with the most traffic and settled on a list of 12: New York Times, CNN, MSN, Fox News, New York Post, Google News, People, Washington Post, USA Today, CNBC, Yahoo News, and Forbes. I accessed each website in Google Chrome after clearing all of my cookies and browsing history. Doing this yielded no cookie notices for the vast majority of these websites, so I used a VPN set to the Netherlands. The thought process behind this is that the Netherlands is subject to GDPR, which requires cookie consent. However, the issue with this was that some of the cookie notices appeared in Dutch. To limit having to use a translation app for analysis, I changed the VPN to the UK. Although the UK is not subject to the GDPR, I found that 10 of the 12 websites did have cookie notices. One possible explanation of this is that many of news sites may have a European version of the site domain (ex: eu.usatoday.com) and that they lump the UK together with Europe, thereby de facto subjecting UK users to required cookie consent notices. Fox News and Washington Post were excluded because they still had no cookie notices even with the VPN.

4.2 Data Collection

Screenshots were taken of each step of the cookie consent workflow for each website, following those referenced in Gray et al [1]: initial framing, configuration, and acceptance. The revocation step was not analyzed. A total of 43 screenshots were taken, with a range of 3-6 per website.

4.3 Choosing a Taxonomy

In order to choose a taxonomy relevant to my project, I started with the taxonomy developed by Gray et al [2], which includes five categories of manipulative patterns: nagging, obstruction, sneaking, interface interference, and forced action. A version of this taxonomy is also referenced in *Dark Patterns and the Legal Requirements of Consent Banners* [1]. In its original form, the taxonomy includes both overarching manipulative pattern categories and specific design strategies. This higher degree of specificity was beneficial for my project, enabling my analysis to be more focused.

However, because Gray et al discuss manipulative patterns across a broad range of websites, their taxonomy includes many design strategies that are not relevant to cookie consent pop-ups. So, I narrowed down the list by removing the following: Nagging, Price Comparison Prevention, Intermediate Currency, Forced Continuity, Hidden Costs, Sneak Into Basket, Bait and Switch, Disguised Ad, Social Pyramid, Privacy Zuckering, and Gamification.

Nagging and Privacy Zuckering are arguably relevant to cookie consent but were removed for the following reasons. As discussed in *Dark Patterns and the Legal Requirements of Consent Banners*, the concept of nagging could be relevant if we consider a user's experience with consent banners across the internet. However, these notices don't fall into what we'd traditionally consider nagging (i.e., repeated unrelated interruptions to a user's experience). Meanwhile, per the definition of Privacy Zuckering (tricking users into sharing more information about themselves than they intend to or would agree to) [2], one could argue that all cookie consent notices utilize this strategy and therefore it would not contribute any novel analysis to include this.

Ultimately, this resulted in a taxonomy that is a mix of the narrow and broad definitions used in the two Gray et al papers. The goal in using this adjusted taxonomy is to point to specific elements of the consent notices/workflows that fall under obstruction, sneaking, and forced action, as these do not currently have more specific strategies beneath them, unlike interface interference, which is a more "obvious" category.

Obstruction	**Sneaking**	**Forced Action**	**Interface Interference**
			Hidden Information Pre-selection Aesthetic Manipulation Toying with Emotion False Hierarchy Trick Questions

Table 1: Final taxonomy used

4.4 Detecting Manipulative Patterns

By analyzing the screenshots, each website was coded according to the manipulative patterns detected within its cookie consent workflow. Individual instances of each manipulative pattern were recorded. In other words, multiple instances of one manipulative pattern were possible. Notes were taken to describe each instance of manipulative pattern, and instances were totaled by category and by website. Possible "privacy-friendly patterns," i.e., design patterns that encourage privacy-friendly choices and/or user autonomy, were also identified (if applicable).

4.5 Legal Compliance

I draw upon the minimum criteria for legal compliance used in Nouwens et al [3], which is pulled from the GDPR:

(1) Consent must be explicit
(2) Accepting all is as easy as rejecting all
(3) No pre-ticked boxes

After examining each website's full consent workflow, I coded each one as "compliant" or "not compliant" with each criterion. When unsure, I chose the option for which there is more evidence/support. In order to assess overall compliance, two different

Manipulative Pattern Category	Design Strategy	Definition
Obstruction	-	Making a process more difficult than it needs to be, with the intent of dissuading certain action(s)
Sneaking	-	Attempting to hide, disguise, or delay the divulging of information that is relevant to the user
Forced Action	-	Requiring the user to perform a certain action to access (or continue to access) certain functionality
Interface Interference	-	Manipulation of the user interface that privileges certain actions over others
Interface Interference	Hidden Information	Options or actions relevant to the user but not made immediately or readily accessible
Interface Interference	Pre-selection	An option is pre-selected by default prior to user interaction
Interface Interference	Aesthetic Manipulation	Any manipulation of the user interface that deals more directly with form than function, including design choices that focus the user's attention on one thing to distract them from or convince them of something else
Interface Interference	Toying with Emotion	Any use of language, style, color, or other similar elements to evoke an emotion in order to persuade the user into a particular action
Interface Interference	False Hierarchy	Giving one or more options visual or interactive precedence over others, particularly where items should be in parallel rather than hierarchical
Interface Interference	Trick Questions	Pattern includes a question that appears to be one thing but is actually another, or uses confusing working, double negatives, or otherwise leading language to manipulate user interactions (ex: using check boxes to opt out rather than opt in)

Table 2: Definitions of each manipulative pattern

thresholds were used. Under the first, less severe threshold, a website is deemed compliant if it satisfies at least 2 of the 3 criteria. Under the second, more severe threshold, a website is deemed compliant only if it meets all 3 criteria.

5 FINDINGS

5.1 Scale of Manipulative Patterns

A total of 55 instances of manipulative patterns were identified across the 10 news websites. Of the four manipulative pattern categories, interface interference had the most unique instances identified, for a total of 24 out of the 55. This is followed by sneaking, obstruction, and forced action with 17, 9, and 4 instances respectively. Of the 24 instances of interface interference, 9 were identified as hidden information, 8 as false hierarchy, and 6 as aesthetic manipulation. Only one instance of pre-selection and one instance of toying with emotion were found. No instances of trick questions were found among the cookie consent flows. (An example of a trick question within the context of cookie consent notices would have been using a checkbox to opt out rather than to opt in; no design choices like these were identified).

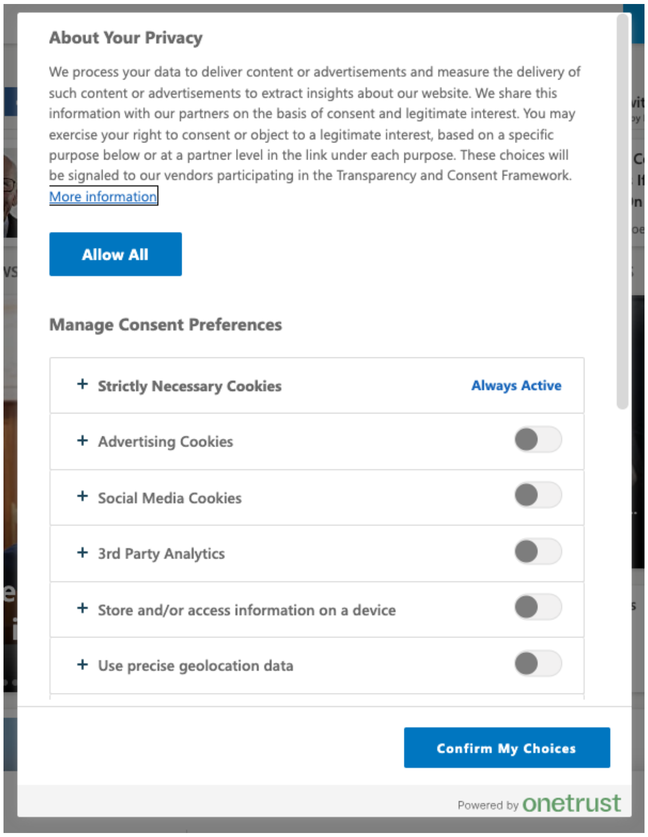
Of the 10 websites examined, 6 had cookie banners at the bottom of the page, 2 had tracking/consent walls [2] that blocked access to the website and only offered the user the option to accept, and 2 had pop-ups that blocked access to the website but gave users the option between accept or reject.

5.2 Manipulative Pattern Analysis

Obstruction. 9 of the 10 websites had cookie consent workflows that utilized some form of obstruction. The most obvious perpetrators are the tracking walls and pop-up notices: these types of consent notices make using a website more difficult for users by blocking their access until they make a choice. But even the consent flows that began with banners used obstructing design tactics. In nearly all of these cases, the "manage choices" or "cookie settings" page had a labyrinth-like set-up of information, making the process of consenting more difficult than it needs to be. The sheer amount of information, coupled with the multiple layers of information, has the intent of pushing users to click the "Accept All" all button (in the cases where an "Accept All" button is present on the cookie settings page; there were a couple of instances in which it was not).

Sneaking. Every website had at least one instance of sneaking. There were two primary manifestations of sneaking in the cookie consent workflows examined. The first was the use of drop-down toggles or sidebar panels to delay or hide certain information on the cookie settings pages. These design choices force users to click a + or ∨ button to expand a subsection of the page. In the case of the sidebar panel design, users must click each panel to reveal that section's information. These design strategies act as an additional barrier to accessing information about how cookies are used. Of the consent workflows that contained some form of cookie settings page, information was broken into as little as 4 subsections and as many as 16. The second primary form of sneaking—and perhaps the most nefarious—was a lack of clear and transparent default settings. For the optional cookie consent banner in particular, it was not clear what happens if a user does not engage with the banner and make a choice regarding their consent.

Forced Action. This manipulative pattern came into play for the tracking walls and mandatory pop-ups. These two types of consent

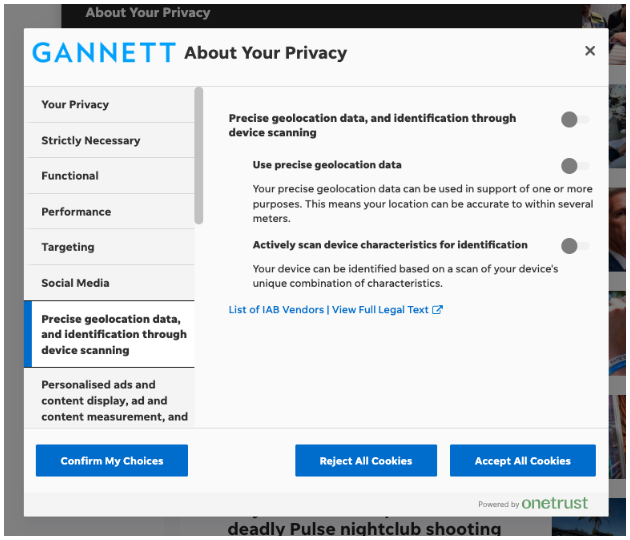


About Your Privacy

We process your data to deliver content or advertisements and measure the delivery of such content or advertisements to extract insights about our website. We share this information with our partners on the basis of consent and legitimate interest. You may exercise your right to consent or object to a legitimate interest, based on a specific purpose below or at a partner level in the link under each purpose. These choices will be signaled to our vendors participating in the Transparency and Consent Framework. More information

Allow All
Manage Consent Preferences
+ Strictly Necessary Cookies
Always Active
+ Advertising Cookies
+ Social Media Cookies
+ 3rd Party Analytics
+ Store and/or access information on a device
+ Use precise geolocation data
Confirm My Choices
Powered by onetrust

Figure 1: Example of sneaking in MSN consent workflow. Information is hidden/delayed to the user via placement behind + expansion/toggle. Users must click the + button to reveal more detailed information on each type of cookie.



About Your Privacy
GANNETT About Your Privacy
×
Your Privacy
Strictly Necessary
Functional
Performance
Targeting
Social Media
Precise geolocation data, and identification through device scanning
Personalised ads and content display, ad and content measurement, and

Precise geolocation data, and identification through device scanning

Use precise geolocation data

Your precise geolocation data can be used in support of one or more purposes. This means your location can be accurate to within several meters.

Actively scan device characteristics for identification

Your device can be identified based on a scan of your device's unique combination of characteristics.

List of IAB Vendors | View Full Legal Text
Confirm My Choices
Reject All Cookies
Accept All Cookies
Powered by onetrust
deadly Pulse nightclub shooting

Figure 2: Example of sneaking from USA Today. Information is hidden behind each panel in the sidebar. User must click on each panel to reveal information about each type of tracking. Additionally, list of IAB vendors and full legal text can only be accessed by clicking on the hyperlinks.

notices, which appeared on 4 of the 10 websites, force the user to make a choice regarding their consent. In the case of the tracking wall on New York Times, the user is truly forced to give their consent: there is no other option. In the case of Google's consent wall and Yahoo News' and USA Today's pop-ups, the user has the option to accept or reject but is forced to make a choice before accessing the website.

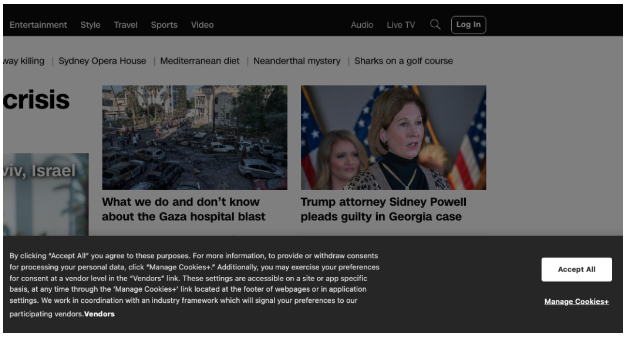
Interface Interference. Similar to sneaking, the hidden information strategy within interface interference consisted mainly of hiding information beneath toggles with the option to expand upon click. Additionally, several cookie settings pages contained hyperlinks to lists of vendors and "full legal text" documents pertaining to a particular use of cookies. While it may be unrealistic or detrimental to provide these lists/full texts on the cookie settings page in the first place, it's unclear what information may be uncovered in these hyperlinks and whether or not the key information a user needs to know has already been provided on the cookie settings page. In other words, it's unclear whether the information "hidden" in these hyperlinks is necessary for the user to examine in order to make an informed choice.

There were several instances of aesthetic manipulation and false hierarchy. For example, in terms of aesthetic manipulation, the "Accept All" choice on CNN's cookie banner is an actual button. The button is filled in white with black text, which is stark against the black background of the cookie notice box. This draws more attention to the button than to the "Manage Cookies+" choice, which is only hyperlinked text. Additionally, once you click "Manage Cookies+", the "Accept All" button appears again: this time, it is bright green and at the top of the page, drawing a user's eye to it. Regarding false hierarchy, several consent banners placed the "Accept" button above the "Reject" button, therefore giving it higher preference, or placed the "Accept" button on the right side of the page, a side most users naturally gravitate to, while placing the "manage cookies" (or equivalent) option off to the left outside of the typical reading order.

There was only one case of the toying with emotion strategy, but it was particularly impactful. CNN's cookie settings page contained the following text in bold letters underneath the "Accept All" button: "PLEASE NOTE: Consent to store and/or access information on a device is required to customize and improve your experience." This language attempts to confuse the user and pressure them into accepting cookies; the message makes it seem as though the user will miss out on a better experience if they don't accept, even without being specific about what that better experience really entails.

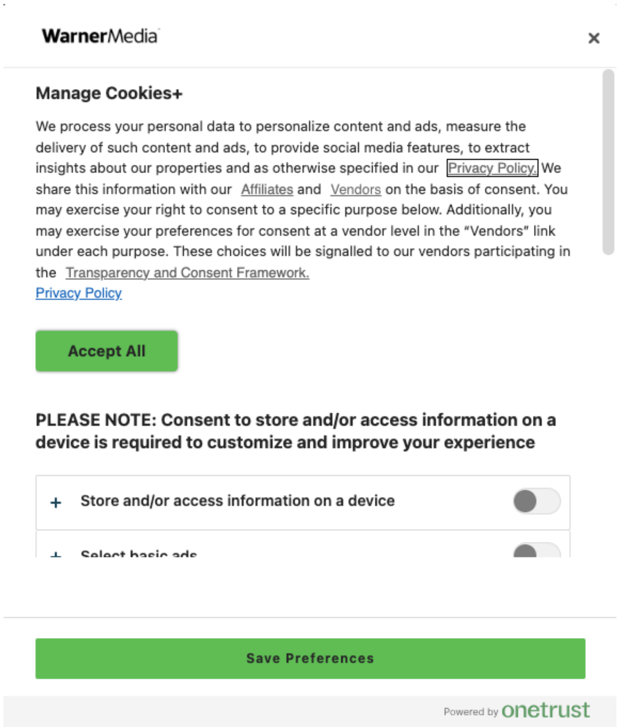
5.3 Website-Specific Findings

Of the 10 websites examined, the ones with the highest number of instances of manipulative patterns were CNN and Google News (both had 7 instances). Of the two, CNN has the poorest consent workflow overall, for the following reasons:



By clicking "Accept All" you agree to these purposes. For more information, to provide or withdraw consents for processing your personal data, click "Manage Cookies+." Additionally, you may exercise your preferences for consent at a vendor level in the "Vendors" link. These settings are accessible on a site or app specific basis, at any time through the 'Manage Cookies+' link located at the footer of webpages or in application settings. We work in coordination with an industry framework which will signal your preferences to our participating vendors.**Vendors**

Figure 3: CNN cookie banner with instance of aesthetic manipulation and false hierarchy. "Accept All" is a white button, which is stark against the black background, while "Manage Cookies+" is only hyperlinked text. "Accept All" button is above the "Manage Cookies+" option.



Manage Cookies+

We process your personal data to personalize content and ads, measure the delivery of such content and ads, to provide social media features, to extract insights about our properties and as otherwise specified in our Privacy Policy. We share this information with our Affiliates and Vendors on the basis of consent. You may exercise your right to consent to a specific purpose below. Additionally, you may exercise your preferences for consent at a vendor level in the "Vendors" link under each purpose. These choices will be signalled to our vendors participating in the Transparency and Consent Framework.
Privacy Policy

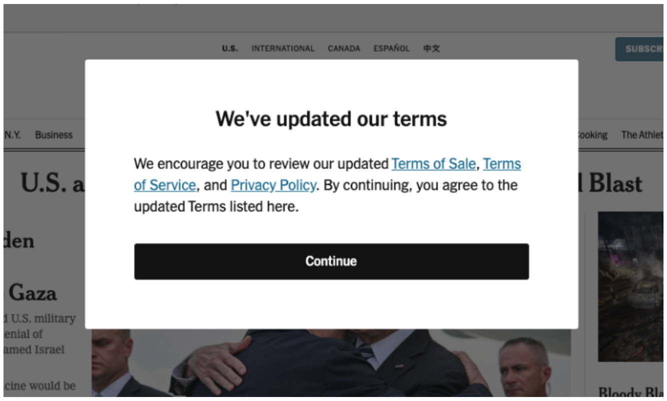
PLEASE NOTE: Consent to store and/or access information on a device is required to customize and improve your experience

+ Store and/or access information on a device
+ Select basic ads

Figure 4: An example of "toying with emotions" manipulative pattern from CNN.

(1) The initial consent notice is in the form of a banner, which makes it ambiguous what the default setting is or what the implications of not making a choice are for the user.
(2) Once you click "Manage Cookies+" you are faced with 16 distinct subsections for cookie types. Each one has information hidden behind a + sign that you can click to reveal more information. Within each section, there are external links to vendors and the "full legal text" pertaining to that use of cookies. This combination of design choices makes the settings page overwhelming and difficult for the user to navigate.
(3) The banner and cookie settings page use both aesthetic manipulation and false hierarchy to favor the choice to accept cookies.
(4) The cookie settings page contains the "PLEASE NOTE" message described in the above section to toy with the emotions of the user in an effort to make them accept cookies.
(5) The consent workflow did not contain any privacy-friendly patterns (more on privacy-friendly patterns discussed in the next section).

But it's important to consider both breadth and severity of manipulative patterns. New York Times, while only having 3 instances of manipulative patterns, ultimately has the starkest effect on limiting user autonomy. The tracking wall only gives users the option to "Accept" and does not even link to a cookie settings page with segmented information. Instead, the tracking wall contains hyperlinks to the company's Terms of Sale, Terms of Service, and Privacy Policy. Bundling these links all in one also causes confusion; it's unclear which the user should click on, and which may be most relevant to the user.



We've updated our terms

We encourage you to review our updated Terms of Sale, Terms of Service, and Privacy Policy. By continuing, you agree to the updated Terms listed here.

Figure 5: New York Times tracking wall.

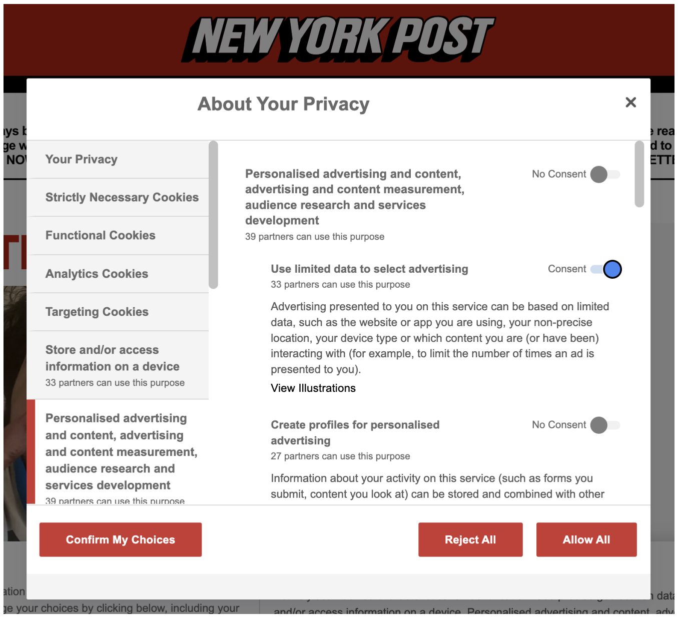
Thus, based on analysis of both breadth and severity, the two news websites with the worst cookie consent workflows are CNN and New York Times.

5.4 Privacy-Friendly Patterns

Certain design patterns (commonly called "bright patterns") have been found to successfully nudge users toward privacy-friendly choices [1]. Within the 10 cookie consent workflows examined, 15 instances of or privacy-friendly patterns were detected. These instances consist of 11 unique privacy-friendly patterns including:

(1) The presence of a "Confirm my Choices" button instead of a "Save Preferences" button. This potentially makes it clearer that the user has a choice in accepting or declining cookies.
(2) The presence of a "Reject All" button on the first cookie notice (whether banner, pop-up, or wall). This gives users an easy way to reject all forms of cookies/tracking.
(3) The toggle options on the cookie settings page display the text "Consent" when turned on and "No Consent" when

turned off. This makes it clearer to the user what each toggle option means, as sometimes it's unclear whether a toggle is pointed to off or on.



NEW YORK POST

About Your Privacy ×

Your Privacy

Strictly Necessary Cookies

Functional Cookies

Analytics Cookies

Targeting Cookies

Store and/or access information on a device
33 partners can use this purpose

Personalised advertising and content, advertising and content measurement, audience research and services development
39 partners can use this purpose

Personalised advertising and content, advertising and content measurement, audience research and services development — No Consent
39 partners can use this purpose

Use limited data to select advertising — Consent
33 partners can use this purpose

Advertising presented to you on this service can be based on limited data, such as the website or app you are using, your non-precise location, your device type or which content you are (or have been) interacting with (for example, to limit the number of times an ad is presented to you).

View Illustrations

Create profiles for personalised advertising — No Consent
27 partners can use this purpose

Information about your activity on this service (such as forms you submit, content you look at) can be stored and combined with other

Confirm My Choices | Reject All | Allow All

Figure 6: Privacy-friendly pattern from New York Post. Toggle options clearly display "No Consent" when toggled off. They also display "Consent" when toggled on.

(4) Toggle has "off" and "on" text next to it, clearly indicating if a toggle is turned off or on.

(5) "Reject All" and "Accept All" buttons on the cookie notice are side by side rather than one on top of the other, therefore not obviously favoring one over the other.

(6) There is no "Accept All" button on the cookie settings page, only the "Confirm My Choices" (or equivalent) button. This may nudge a user to make an informed choice regarding consent, rather than simply selecting "Accept All" if they are overwhelmed by the amount of information on the cookie settings page.

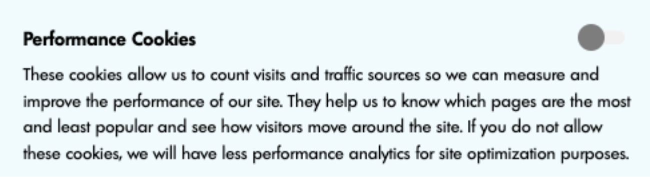
(7) Cookie settings page subsections make a good faith attempt to succinctly summarize the different types/uses of cookies and the consequences of not enabling them. It uses plain language that does not overly favor one choice versus another.

(8) The presence of a "Save Settings" button may indicate to the user that they can be changed in the future (drawing upon the common convention of "user settings").

(9) "Save Choices" button positioned in between the "Reject All" and "Accept All" buttons, implying it is a middle ground between the two ends of the spectrum. This may reiterate to a user that they have autonomy over their privacy choices, urging them to make an informed decision rather than accept a default.

(10) "Reject All" and "Accept All "buttons are side by side, with "More Options" right below, rather than off to the side. This makes it clearer that the user can opt to look at more specific options instead of only accepting or rejecting all trackers.

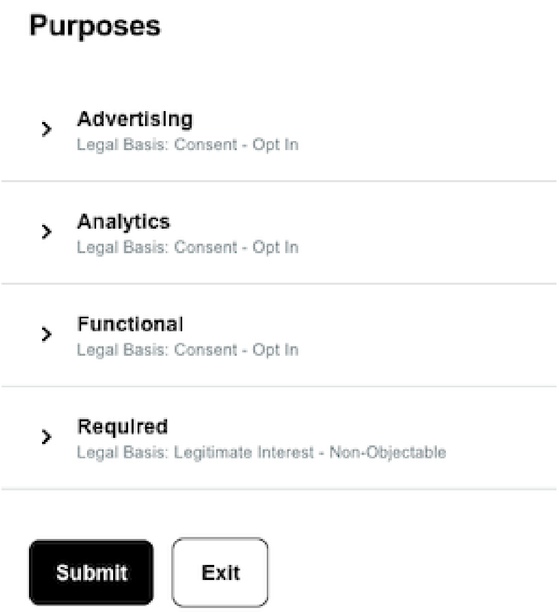
(11) "Legal basis" text underneath each cookie category explains how consent must be given for that specific type of cookie/tracker. While some users may not immediately understand this, this text does provide some transparency into the legal requirements surrounding privacy consent.



Performance Cookies

These cookies allow us to count visits and traffic sources so we can measure and improve the performance of our site. They help us to know which pages are the most and least popular and see how visitors move around the site. If you do not allow these cookies, we will have less performance analytics for site optimization purposes.

Figure 7: Example of a privacy-friendly pattern from People's cookie consent workflow. Subsections describing each type of cookie clearly indicate the consequences of not allowing. For example, here it says: "If you do not allow these cookies, we will have less performance analytics for site optimization purposes."



Purposes

› Advertising
Legal Basis: Consent - Opt In

› Analytics
Legal Basis: Consent - Opt In

› Functional
Legal Basis: Consent - Opt In

› Required
Legal Basis: Legitimate Interest - Non-Objectable

Submit | Exit

Figure 8: An example of a privacy-friendly pattern from Forbes: each subsection of cookie type includes a "legal basis" explanation.

5.5 Legal Analysis

Using the less severe threshold for legal compliance (i.e., a consent workflow meets 2 out of 3 criteria), 6 out of the 10 total websites were deemed compliant and 4 were deemed non-compliant. Of note is that neither New York Times nor CNN, discussed above as the two worst consent workflows of the group, met this threshold for legal compliance. In regards to the first criterion—"consent must be explicit"—the workflows that did not comply were the ones that had an optional consent banner. Without having to make a choice, it's unclear if the user consented to cookies or not. Thus, these forms of cookie notices are not compliant with GDPR's definition of explicit consent. This is somewhat at odds with the "forced action" manipulative pattern. If users are not forced to take action regarding their consent, then consent is not explicit. This begs the question of if forced action is really detrimental in all cases. Often times, forcing a choice may be the only way to actually gain explicit consent. However, this could be remedied by having opting in to cookies be an optional action. Currently, opting out of cookies is the default action. If cookies were turned off by default, then perhaps the idea of explicit consent would not be as important.

In terms of the second criterion—"accepting all must be as easy as rejecting all"—only the cookie notices that had both an "Accept All" and a "Reject All" option on the initial notice screen were compliant. In regards to the third criterion, the majority (8 out of 10) did not have pre-selected boxes and therefore were compliant. New York Times's tracking wall was deemed non-compliant in this respect because it did not offer a choice other than "Continue" (i.e., giving consent). Although it did not contain pre-selected boxes in literal terms, it has the same effect in that a user's choice is essentially pre-determined.

When applying the second, more severe threshold for legal compliance (i.e., a consent workflow must meet all 3 criteria), only 2 out of the 10 websites were deemed compliant: USA Today and Yahoo News.

Website	Explicit Consent	Accept Reject Equal	No Pre-Ticked Boxes	Overall
NY Times	Yes	No	No	No
CNN	No	No	Yes	No
MSN	No	Yes	Yes	Yes
NY Post	No	No	Yes	No
People	No	Yes	Yes	Yes
USA Today	Yes	Yes	Yes	Yes
CNBC	No	Yes	Yes	Yes
Yahoo News	Yes	Yes	Yes	Yes
Google News	Yes	Yes	No	Yes
Forbes	No	No	Yes	No

Table 3: Moderate compliance threshold: compliant if meets at least 2 of 3 criteria

Website	Explicit Consent	Accept Reject Equal	No Pre-Ticked Boxes	Overall
NY Times	Yes	No	No	No
CNN	No	No	Yes	No
MSN	No	Yes	Yes	No
NY Post	No	No	Yes	No
People	No	Yes	Yes	No
USA Today	Yes	Yes	Yes	Yes
CNBC	No	Yes	Yes	No
Yahoo News	Yes	Yes	Yes	Yes
Google News	Yes	Yes	No	No
Forbes	No	No	Yes	No

Table 4: Severe compliance threshold: compliant if meets all 3 criteria

6 DISCUSSION

These manipulative patterns and design strategies ultimately hamper user autonomy and add more confusion surrounding data privacy consent. But while some instances of manipulative patterns, such as the New York Times' tracking wall, have clear detrimental effects on user choice, others are not so clear.

There are several trade-offs when it comes to making the cookie consent process simpler or more complex. Reducing cookie choices down to one button, for example, makes the process easier. However, this does not give the user as much insight into the different uses of cookies and trackers. Some users may want to be able to pick and choose which cookies/trackers are used and for what purpose. On the other hand, these labyrinth-like consent flows contain a lot of information—more than a typical user can or is willing to digest in one sitting. That begs the question of whether "less is more" is the right strategy, and if inundating users with too much information regarding cookies is actually detrimental. For instance, does seeing all the options make a user want to customize their choices or does it just push them to just click "Accept All"? Research by Nouwens et al [3] found that providing more granular controls significantly decreases consent, which suggests that users may benefit from a "more is more" strategy. However, that study only surveyed 40 users; more research can be done to glean what users think about different cookie consent options and workflows.

Similar to obstruction, the patterns that fall into sneaking also come with trade-offs. Hiding information underneath + drop-downs can be considered sneaking, but it also makes the information presented to users more modular and interactive. Whereas, if the information is presented on one long page that users have to scroll through, that might make users less likely to engage with and actually process the information. One option to limit sneaking behavior in cookie consent notices and increase transparency to users is to clearly indicate on a cookie pop-up what the default option is. Many of the sites examined in this study had cookie banners at the bottom of their websites that users were not forced to engage with. But it was unclear what happened when users did not make a choice on the banner. Is the default option that cookies are turned off or turned on? Adding clear language to the cookie pop-up banner regarding the default settings would better address the implicit and explicit use of this manipulative pattern.

In terms of forced action, while it may be annoying for users to encounter a pop-up or wall before accessing a website, these types of consent notices ensure that there is no ambiguous consent and therefore may be more legally compliant. The alternative would be to use optional cookie banners that users don't have to engage with. But, as mentioned above, doing this would necessitate the default being cookies are turned off.

Design choices in the realm of interface interference are equally, if not more, subjective. Easy pro-privacy design choices include toggles pre-selected to "off" and not using any language or warnings that confuse users or toy with their emotions. However, some design choices are not so clear. For example, making the "Accept All" and "Reject All" buttons in the same color, size, and style may be neutral in that neither option is favored over the other. But this can also be confusing as it becomes harder to distinguish between the two buttons. This may prompt users to pay less attention to the buttons or not know which one to click. A pro-privacy nudge would be to make the "Reject All" button stand out, or to include only "Reject All" and "Cookie Settings" options on the initial cookie notice (thus excluding an "Accept All" option). This would further enforce the default option as no cookies/tracking. However, it could be argued that these privacy-friendly patterns also influence the user and reduce their autonomy. It's not immediately clear if neutral design choices are better than pro-privacy design choices: this is subjective depending on the intention and motivation behind the design.

Ultimately, the consent workflows examined in this study contain both manipulative and privacy-friendly patterns. Several of the privacy-friendly patterns highlighted in the previous section could be combined to create an "optimal" or "ideal" cookie consent notice. Rather than add more manipulative patterns to the landscape, future work should focus on identifying (through user feedback) which manipulative patterns are most detrimental to user autonomy and which privacy-friendly patterns can reduce confusion, maximize user autonomy, and increase transparency.

Despite likely being under the purview of the GDPR, many of these consent workflows are not fully legally compliant. Lack of legal compliance can signal a poorly designed consent process that does not benefit users. Indeed, the presence of a non-compliant cookie notice could be an indication of more severe negative data privacy practices. Future work could explore ways to detect legal compliance of cookie consent workflows at scale. Doing so would also necessitate a more comprehensive (but still enforceable) definition of legal compliance. The criteria used for legal compliance in this study is succinct but limited, representing a minimum definition rather than an ideal definition.

Of course, legal compliance cannot be the sole criteria considered when designing these workflows. Companies and designers must go beyond legal compliance to design cookie notices and workflows that honor the true spirit of informed, explicit consent, not just the bare minimum legal requirements.

7 CONCLUSION

Although cookie consent notices may be an annoyance to users, they are required by GDPR. However, because GDPR does not specify what these notices must look like, they come in many forms, including banners, walls, and pop-ups. They also contain many design strategies that fall into four key manipulative pattern categories: obstruction, sneaking, forced action, and interface interference. These manipulative patterns, on the whole, nudge or force users to give their consent to the use of cookies. These cookies track their behavior across websites and devices and collect and share their personal information with third-party companies. While these cookie consent notices are just one piece of a much larger data privacy puzzle, they represent a prime opportunity for simple solutions that can enhance user autonomy. Requiring the use of privacy-friendly patterns (such as clear on/off toggles, neutral and easy-to-understand language, and no aesthetic manipulation of accept over reject) and prohibiting the use of certain severe manipulative patterns (such as the tracking wall that only gives an "accept" option) are low-hanging fruit options that can protect user privacy on a massive scale across the internet.

REFERENCES

[1] Colin M. Gray et al. "Dark Patterns and the Legal Requirements of Consent Banners: An Interactive Criticism Perspective". In: *CHI Conference on Human Factors in Computing Systems* (2021). DOI: https://doi.org/10.1145/3411764.3445779.

[2] Colin M. Gray et al. "The Dark (Patterns) Side of UX Design". In: *CHI Conference on Human Factors in Computing Systems* (2018). DOI: http://doi.org/10.1145/3173574.3174108.

[3] Midas Nouwens et al. "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence". In: *CHI Conference on Human Factors in Computing Systems* (2020).

[4] Alberto Monge Roffarello, Kai Lukoff, and Luigi De Russis. "Defining and Identifying Attention Capture Deceptive Designs in Digital Interfaces". In: *CHI Conference on Human Factors in Computing Systems* (2023). DOI: https://doi.org/10.1145/3544548.3580729.