DECEPTIVE DESIGN: COOKIE CONSENT AND MANIPULATIVE PATTERNS

THOMAS MEJTOFT, ERIK FRÄNGSMYR,
ULRIK SÖDERSTRÖM & OLE NORBERG

Umeå University, Digital Media Lab, Sweden; e-mail: thomas.mejtoft@umu.se, erik.frangsmyr@gmail.com, ulrik.soderstrom@umu.se, ole.norberg@umu.se

Abstract As a larger proportion of our lives moves onto the web, so does important and valuable information. This has led to an increase in different kinds of manipulative patterns (dark patterns) in web design with the sole purpose of being deceptive and tricking users. This paper discusses the comprehensive suite of deceptive design patterns on Internet services where the users are expected to comply with the use of cookies. This was done by analyzing 50 different home cooking recipe websites, regarding their appliance to GDPR and how they use different dark patterns in their design. Even though legislation tries to move the choices from the website to the user, it is clear that by using deceptive design patterns it is possible to "bypass" the legislation and trick the user into making a favorable choice for the owners behind the website. The results show that out of the websites that were GDPR approved, a majority still use two types of deceptive design patterns - misdirection and sneak into basket.

Keywords: deceptive design, dark patterns, cookie consent, GDPR

University of Maribor Press

DOI https://doi.org/10.18690/978-961-286-485-9.29
ISBN 978-961-286-485-9

1 Introduction

Since the very first web page, there has been constant changes to the design to create usable designs that increases the user experience. New guidelines have gradually evolved to enable great designs for various digital devices (Nielsen, 2018; Shneiderman, 2009). This constant perfection has made the vast majority of web sites intuitive and easy to use for most users. However, as the field of user experience on the web has gradually evolved during the last 25 years, so have underhanded tactics colloquially known as dark patterns or deceptive designs (Brignull, 2011). These features of design are just as carefully crafted but with another purpose than to lead the user in the right direction. Hence, a dark pattern is "a user interface carefully crafted to trick users into doing things they might not otherwise do, such as buying insurance with their purchase or signing up for recurring bills" (Brignull, 2013). Unlike concepts like e.g. digital nudging, which is about creating solutions that help the user to make the choices in their best interest by altering the choice environment (Thaler & Sunstein, 2008; Mejtoft et al., 2019), deceptive design is about manipulating a user into doing something that is not in the user's best interest but in the interest of the owner of the website.

As people spend an increasing proportion of their lives on the web and the self-disclosure increase with more user generated content (Blackshaw & Nazzaro, 2006) and the use of e.g. social media (Kaplan & Haenlein, 2010), the need for digital integrity and privacy becomes important issues. This has become even more important during the Covid-19 pandemic, when an increasing part of our leisure and work time is spent online. Integrity is a "personal choice" (Killinger, 2010) and privacy is the "right to be let alone" (Warren & Brandeis, 1890). All this collection of data can e.g. be done by a company with, or without, consent or totally voluntarily by the users, so called personal informatics (Wilson, 2012). One important difference between the old analogue systems with notes and the current digital systems is the much higher traceability and foreverness of digital information and the opportunities to manipulate users using this information to alter systems (Kramer, Guillory & Hancock, 2014). This has led to an increase in different types of manipulative patterns in web design with the sole purpose to be deceptive and trick the users. A common way of creating deceptive design patterns and purposely tricking the user into making non-favorable decisions when collecting and using user data is to use cookies. Recently, there have been legal initiatives to try to strengthen the consumers rights within this area e.g. the General Data Protection Regulation (GDPR) (European Commission, n.d.).

The objective of this paper is to discuss and analyze different deceptive web design patterns where users are expected to comply with the use of cookies. To achieve the objective the following research questions will be discussed: (1) What are the most commonly used deceptive design patterns and the effect of those? (2) How can users avoid involuntary sharing of personal data?

2 Background and Theory

The main idea behind web design and the guidelines (Nielsen, 2018; Shneiderman, 2009) for creating accessible and usable websites is to create an honest design. This is also one of the ten principles of good design stated by Dieter Rams in the 1970s - "Good Design is honest: It does not make a product more innovative, powerful or valuable than it really is. It does not attempt to manipulate the consumer with promises that cannot be kept" (Rams, n.d.). However, deception is pretty much the opposite. Deception can be described as the act of "hiding the truth" and in the realm of business this means "dishonest or illegal methods that are used to get something, or to make people believe that something is true when it is not" (Cambridge dictionary, n.d.). This can be used to describe design choices that have the users unconsciously share information which they normally would not do (D'Onfro, 2015).

The term Dark Patterns was coined in the aftermath of the boom of e-commerce websites that in order to generate sales and traffic were designed using deceiving user interfaces to manipulate users in different ways (Jaiswal, 2018). In a broader aspect, Dark Patterns use developers' and designers' knowledge of human psychology (Gray et al., 2018) and UX design to theoretically flip "honest" design into "evil" (Valjak, 2018).

The design patterns in Table 1, describes some of the psychological effects, inflicted among the users, that the designers want to build on. Persuasive design is a practice where the idea is to purposely influence the users' behaviors through the characteristics of a service. This can be done by designing for a behavior as a product of motivation, ability and triggers (Fogg, 2009). Consequently, many game mechanics used to enhance activities through gamification (Robson, 2015; Zichermann & Cunningham, 2011) touch upon the problem and similar patterns as deceptive design. There are usually two sides - the same mechanics that can be used to enhance motivation to make users do good (Papworth & Mejtoft, 2015), can also be used to cause harm to the users in different ways.

Table 1: Description of common Dark Patterns (Brignull & Darlo, 2019)

Dark pattern	**Description**
Misdirection	The design purposefully focuses the attention on one thing to distract the attention away from another.
Sneak into Basket	The user attempt to purchase something, but somewhere in the purchasing journey, the site sneaks an additional item into your basket, often using an opt-out radio button or checkbox on a prior page.
Trick Questions	While filling in a form the users respond to a question that tricks the user into giving a non-intended answer. When glanced upon quickly, the question appears to ask one thing, but when reading carefully it actually asks another thing.
Bait and Switch	The users set out to do one thing, but a different, undesirable thing happens instead.
Confirmshaming	Guilting users to “opt in” by making them feel bad for saying no.

2.1 GDPR approved

The General Data Protection Regulation (GDPR) (European Commission, n.d.) is a regulation on privacy and data protection within the European Union (EU). The regulation applies to all companies that collect or use data of citizens that reside within the EU and the EEA, regardless of the location of the company. Since May 2018, when GDPR was put into action, Internet services who utilize cookies (Koch, n.d.) to collect user data are obligated to inform the user of e.g. what type of data is collected and how the service is using the data. To comply with the GDPR, Internet services appear to do the following (Dabrowski et al, 2019; Koch, n.d.): (1) services refrain from using persistent cookies at all, (2) EU users are banned from using the specific service, and (3) a service asks for explicit user consent and only then sets the cookies, leaving the site usable without consent. If consent is asked for, there is frequently a banner spanning over a service’s pages asking for consent. The latter alternative sites tend to use deceptive design patterns to have the user consent to cookies by applying different types of Dark Patterns.

To be able to define if the usage of cookies is according to the regulations, GDPR.EU (European Commission, n.d.) has a general explanation of what cookies are and how they should be implemented according to the GDPR (Koch, n.d.). There are four different types of cookies purposed - Strictly necessary cookies, Preferences cookies, Statistics cookies, and Marketing cookies. In this paper the focus is on the Strictly necessary cookies, as Strictly necessary cookies are the cookies that are essential for the user to be able to use the website and its features in an intended fashion. Other types of cookies are those which must be confirmed by the user or those that the user need to be informed about according to the GDPR. According to EU requirements, cookies on a website must comply with the following: (1) Have the users' consent before any cookies are in use, except strictly necessary cookies, (2) Provide the necessary information about the cookie and its collection of data before the consent, (3) Save the consent information from the user, (4) Provide the user of accessing the service even if they do not allow the use of certain cookies, and (5) Provide an easy way for the user to change their consent or cookie settings.

3 Method

A comprehensive analysis of 50 different home cooking recipe websites was done by first distinguishing how many websites were GDPR approved. Then out of the approved websites, an extended evaluation of the design was made to discern any types of deceptive designs. From these designs, an A/B test was created consisting of two websites (Test A and B) combined with a survey, to then be evaluated.

3.1 Website analysis

Using Alexa (2019) Top 500 Ranking, the top 50 websites on the list were analyzed by comparing each website's approach to using cookies to the definition of a correct usage according to GDPR.EU (European Commission, n.d.; Koch, n.d.). To see if the websites are using cookies correct each website was launched into Google Chrome Incognito mode, where the website was inspected with Developer tools >

Application > Cookies. In this mode all active cookies appeared, which could be categorized between Strictly necessary cookies or others.

After distinguishing which websites were GDPR approved, these websites were evaluated to determine if, and what type of, deceptive designs were being used. Brignull and Darlo's (2019) Types of Dark Patterns were used as a reference to find the most commonly used deceptive design patterns.

3.2 Testing and survey

An A/B-test was conducted with two websites created, to be able to compare two different cookie prompt approaches. Test A included a website with a cookie prompt made by using the most common Dark Patterns found from the Website analysis, and Test B's cookie prompt was made without Dark Patterns. The two different websites had three possible surveys, where all surveys had the same content and questions. The only thing differentiating the tests was the fact that if a participant Accepted or Declined the cookie prompt they would come to the corresponding survey. If the participant remained undecided, they stayed on the current survey (Figure 1).

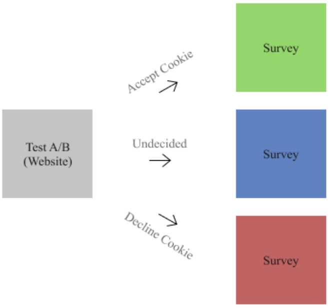
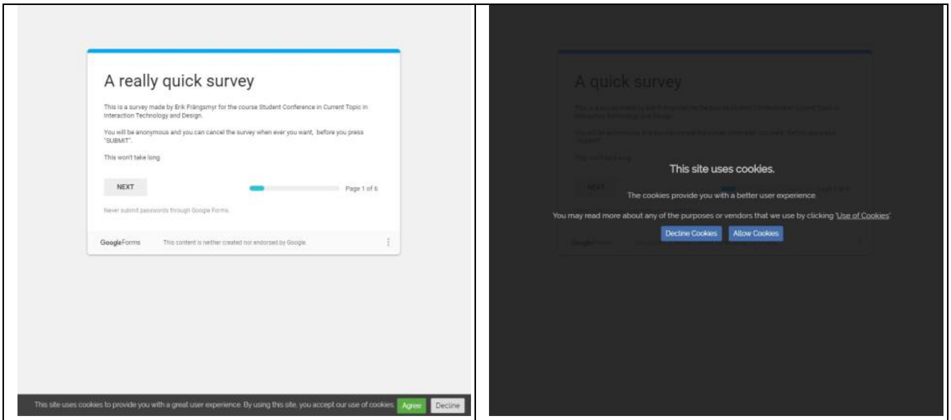


Figure 1: Flowchart showing how participants decision on *accepting*, *declining* or remaining *undecided* affected which survey was shown

Test A (small banner cookie prompt): The Test A cookie prompt (Figure 2a) was inspired by two defining Dark Pattern Methods - Sneak in the Basket and Misdirection. The prompt was small to not distract the user from the website content too much. The text on the prompt stated: "This site uses cookies to provide you with a great user experience. By using this site, you accept our use of cookies.”, which corresponded to the Sneak in the Basket method, as it informed the user that if a decision is not actively made, the user automatically accepted the cookies when using the site. Note that there were no other cookies used on the website than the strictly necessary ones, to be able to know if the participants Accepted or Declined the cookie prompt. The Accept button was green and bright, while the Decline button was gray an unattractive, which corresponded to Misdirection. The text even had a hidden link under “Use of Cookies”, where it would explain what types of cookies were being used. This was purposely hidden to not draw attention away from a big green button.



A really quick survey

This is a survey made by Erik Frängsmyr for the course Student Conference in Current Topic in Interaction Technology and Design.

You will be anonymous and you can cancel the survey when ever you want, before you press "SUBMIT".

This won't take long

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google.

This site uses cookies to provide you with a great user experience. By using this site, you accept our use of cookies.

A quick survey

This site uses cookies.

The cookies provide you with a better user experience

You may read more about any of the purposes or vendors that we use by clicking 'Use of Cookies'.

(a) Screenshot of Test A.
The user is shown a small banner cookie prompt.

(b) Screenshot of Test B.
The user is shown a full screen cookie prompt.

Figure 2: Screenshot of (a) Test A and (b) Test B

Test B (full screen cookie prompt): The cookie prompt created for Test B was much clearer and more informative than Test A (Figure 2b). The text was more informative and showed the option to go to “Use of Cookies” more distinctly. The option to Decline or Accept cookies was made less hierarchically than in Test A by having the buttons the same color and they explained what each button was meant to do, either to decline cookies or to allow cookies.

3.3 Participants

In total 40 respondents took part of the study, 20 respondents did Test A and 20 respondents did Test B. All participating respondents were from Sweden and was between the age of 20 and 65 years, where a majority were students between the age of 20-25 years. The research study was carried out during 2019. The tests were conducted online and a link to the corresponding test website was sent to each participant, where they could participate in the test and fill out the survey as they perceived it.

4 Results and discussion

Out of the 50 home cooking websites analyzed, less than half, 22 websites, turned out to comply to the GDPR. The other 28 websites either did not give a choice of complying with the cookies, or they asked the question for user compliance after the fact that they already ran all the cookies. Even if the usage of cookies was declined, the cookies were already in use and, consequently, the compliance did not matter. Hence, these websites did not meet the requirements of the GDPR legislation. Since the websites were chosen from the top of the Alexa Top 500 ranking, the websites in this test are very popular websites. Noteworthy is that still over half of 50 most common websites did not comply to the legislation.

Out of the 22 GDPR approved home cooking websites, 7 websites had no dark patterns and 15 websites had some kind of dark pattern in their design. From the websites analyzed there were two clear Dark Patterns used – *misdirection* and *sneak into basket*.

Misdirection methods were used in such way that the design purposefully focused the attention to accept all cookies by having the user focus on the biggest green button that says "Accept recommended setting" to distract the attention from reading more about the other cookies used. Out of the 22 GDPR approved websites analyzed, 4 websites had "misdirection" patterns.

Sneak into Basket methods were used in such a way that the user was prompted to comply with the website only uses the Necessary Cookies (Koch, n.d.) but it also adds third-party cookies without full consent from the user, which then manually have to be removed through the use of an opt-out radio button or checkbox on a prior page. Out of the 22 GDPR approved websites analyzed, 11 websites had a "sneak into basket" design.

The task to present a how-to guide on how to avoid involuntary sharing of data is a seemingly hard task. One could think it would be as simple as being careful of not accepting the Privacy Policies or specifically the Use of Cookies. Maybe to go to the settings of every site and uncheck any unwanted cookie, or do so the first time launching a site. But to give this as convincing advice would give the false impression of having the control of what is being shared and not. Sadly, this is not the case, which can be seen from the results of the website analyses.

4.1 Cookie consent test

The cookie consent test was done on the two mock-up websites created to simulate the two dark patterns identified in the website analysis described above. The results from the survey show that all participants answered that they did *not* read the Use of Cookies page. One of the participants even expressed their concern about this issue by commenting this in the survey: "I usually get super annoyed when these prompts appear... I always click 'accept' because I have this weird fear that I won't be able to enter if I don't accept the cookies. I want to click 'decline', but for some reason I always accept." In Test A, where the users were shown the small banner cookie prompt a majority (60%) made no decision on either accepting or declining the cookies.

In Test B, with full screen cookie prompt, all participants made a decision, and a majority (80%) accepted the use of cookies. The full screen cookie prompt, however, made it more or less necessary to make a decision to remove the prompt and either continue to the website or go back. Sure, as a user, it is a good thing to feel like you are in control. But if you do not trust the website, does it really matter?

Is it really necessary for websites to use Dark Patterns? The results show that in Test A, a clear majority are not making an active choice of whether they want to accept or decline the cookie. However, when asked "Did you notice the cookie prompt on this site?" both tests resulted in similar answers, where the majority did notice the cookie prompt. However, almost non (in both cases) did read the read the "Use of

Cookies" page. Hence, even though many of the participants made a active choice to accept the cookies, how free is the choice when focus is not on the cookie consent but to consume actually information on the website. It is hard to believe that the users would not care about the privacy, but still no not take time to read through how personal data is used. The symbiosis of the commercial companies' collection of data for customization as well as the privacy and choice of the users have been discussed by e.g. Appelgren, Leckner and Mejtoft (2014).

5 Concluding discussion

Legislation has become more important for users to avoid involuntarily sharing of personal data. EUs GDPR is one of the more common legislations in recent years. However, looking at the Alexa Top 500 popular websites, only about half of the top websites complied with the legislation. Other ways of getting a user to share data is by designing to deceive the users to, in different ways, give away data. However, to avoid involuntary sharing of personal data it does not matter if deceptive design patterns are avoided or not if the website is not abiding by the regulations. While deceptive design has a purpose to create deceiving design based on the general design principles to make e.g. intuitive choices, it is important that honest design makes us think. Even though legislation tries to move the choices from the website to the user, it is clear that by using deceptive design patterns it is possible to somehow "bypass" the legislation. This is done by purposely designing for moving the users from the reflective situation that the cookie consent should be to an automatic behavior (Hansen & Jespersen, 2013). The most common ways to deceive the users to give away more information than needed, is the patterns *misdirection* and *sneak into basket*. Both of these either trick you into accepting all cookies or show you options but add cookies that are not necessary for function.

One way of dealing with the automatic behavior that cookie consent has become is to purposely introduce more intentional friction into the design that encourage a reflective behavior. Consequently, it is possible to focus on the important elements at hand and make users do reflective choices (Mejtoft, Hale, & Söderström, 2019; Hansen & Jespersen, 2015; Kahneman, 2008).

Even if websites ask for user compliance there is no way of knowing how they will be using the data without reading the Privacy Policy or Use of cookie page. If the website in question seems to follow the GDPR, the key to limiting sharing of involuntary personal data seems to be (in incremental order); 1) not trusting any websites, 2) become familiar with Developer Tools or Cookie managements for the preferred web browser and 3) make sure to look out for Dark Patterns in the design.

References

Appelgren, E., Leckner, S., & Mejtoft, T. (2014). The media consumers' conscious and unconscious choices – a key to understanding the news media consumption of tomorrow. In S. Zlitni, F. Liénard, D. Dula & C. Crumiére (Eds.), Communication électronique, cultures et identités (pp. 521-528). Editions Klog.

Blackshaw, P., & Nazzaro, M. (2006). Consumer-Generated Media (CGM) 101 (2nd ed.). Technical Report. Nielsen BuzzMetrics. Retrieved December 2, 2020, from http://www.nielsen-online.com/downloads/us/buzz/nbzm_wp_CGM101.pdf

Brignull, H. (2011, November 1). Dark Patterns: Deception vs. Honesty in UI Design. A List Apart 338. Retrieved January 2, 2021, from https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design/

Brignull, H. (2013, August 29). Dark Patterns: inside the interfaces designed to trick you. The Verge. Retrieved June 2, 2020, from https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you

Brignull, H., & Darlo, A. (2019). Types of dark patterns. Retrieved April 2, 2021, from https://www.darkpatterns.org/types-of-dark-pattern

European Commission. (n.d.). Data protection in the EU. Retrieved April 1, 2021, from https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Dabrowski, A., Merzdovnik, G., Ullrich, J., Sendera, G., & Weippl, E. (2019). Measuring Cookies and Web Privacy in a Post-GDPR World. In D. Choffnes and M. Barcellos (Eds.), Passive and Active Measurement (pp. 258–270). Springer.

Cambridge Dictionary. (n.d.). Deception. Retrieved February 7, 2020, from https://dictionary.cambridge.org/dictionary/english/deception

D'Onfro, J. (2015, October 3). LinkedIn might have to pay you money for spamming your email contacts. Business Insider. Retrieved June 1, 2020, from https://www.businessinsider.com/linkedin-settles-class-action-lawsuit-2015-10

Fogg, B. J. (2009). A Behavior Model for Persuasive Design. In Proceedings of the 4th International Conference on Persuasive Technology (Persuasive '09), Article 40. ACM.

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18), Paper 534. ACM.

Hansen, P. G., & Jespersen, A. M. (2013). Nudge and the Manipulation of Choice. European Journal of Risk Regulation 4(1), 3–28.

Alexa Internet. (2019). The top 500 sites on the web. Retrieved March 23, 2019, from https://www.alexa.com/topsites/category/Top/Home/Cooking.

Jaiswal, A. (2018, April 16). Dark patterns in UX. UX Collective. Retrieved June 4, 2020, from https://uxdesign.cc/dark-patterns-in-ux-design-7009a83b233c

Kahneman, D. (2008). Thinking, fast and slow. Farrar, Straus and Giroux.

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite!. Business Horizons 53(1), 59–68.

Killinger, B. (2010). Integrity: Doing the Right Thing for the Right Reason (2 ed.). McGill-Queen's University Press.

Koch, R. (n.d.). Cookies, the GDPR, and the ePrivacy Directive. Retrieved June 25, 2020, from https://gdpr.eu/cookies/

Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. Proceedings of the National Academy of Sciences 111(24), 8788–8790.

Mejtoft, T., Hale, S., & Söderström, U. (2019). Design Friction: How intentionally added friction affect users level of satisfaction. In Proceedings of the 31st European Conference on Cognitive Ergonomics (pp. 41-44). New York, NY: ACM.

Mejtoft, T., Ristiniemi, C., Söderström, U., & Mårell-Olsson, E. (2019). User experience design and digital nudging in a decision making process. In 32nd Bled eConference Proceedings (pp. 427-442). University of Maribor Press.

Nielsen, J. (2018). 10 Usability Heuristics for User Interface Design. Nielsen Norman Group. Retrieved June 6, 2020, from https://www.nngroup.com/articles/ten-usability-heuristics/

Papworth, S., & Mejtoft, T. (2015). Using game mechanics for motivational design in products and services. In 2015 ANZMAC Conference proceedings, 1047 – 1054.

Rams, D. (n.d.). The power of good design. Retrieved June 2, 2020, from https://www.vitsoe.com/us/about/good-design

Robson, K., Plangger, K., Kietzmann, J. H., McCarthy, I., & Pitt, L. (2015). Is it all a game? Understanding the principles of gamification. Business Horizons 58(4), 411-420.

Shneiderman, B., Plaisant, C., Cohen, M., & Jacobs S. (2009). Designing the User Interface: Strategies for Effective Human-Computer Interaction (5th ed.). Addison-Wesley Publishing Company.

Thaler, R. H., & Sunstein, C. R. (2008). Nudge: Improving decisions about health, wealth and happiness. Penguin Putnam Inc.

Valjak, A. (2018, April 16). Dark patterns in UX. Retrieved June 1, 2020, from https://infinum.com/the-capsizedeight/dark-patterns-designs-that-pull-evil-tricks-on-our-brains

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. Harvard Law Review, 4(5), 193-220.

Wilson, H. J. (2012). You, By the Numbers. Harvard Business Review, 90(9), 119 – 122.

Zichermann, G., & Cunningham, C. (2011). Gamification by Design. O'Reilly Media