Dark Patterns in Web Design

A reflection on the intersection between design, ethics, and politics

SIYANA M IVANOVA
Interactive Media Technology student, KTH

The present paper aims to highlight the importance of ethical design practices by focusing on the phenomenon of "dark patterns" occurring in contemporary web design: features and choices which aim to deceive the user in order to achieve a goal related to corporate or political profit.

Keywords and phrases: dark pattern, ethical design, online presence, data protection

1 Introduction

In 2016 - practically a couple of decades ago in internet years - the European Union passed a regulation known as the General Data Protection Regulation or GDPR [1]. We will not be discussing the legal intricacies of this document in this essay. Rather, we will observe the practical effects of it from a regular internet user's point of view: suddenly, a lot of websites began asking for consent - to collect data, to display "tailored" advertisements, etc. - and they were asking in a wide variety of ways, from clear-cut forms to what could best be described as a scavenger hunt for the "I do not agree" button. This has been punctuated by the occasional scandal, e.g. Facebook gathering and selling 50 million people's data to Cambridge Analytica [2].

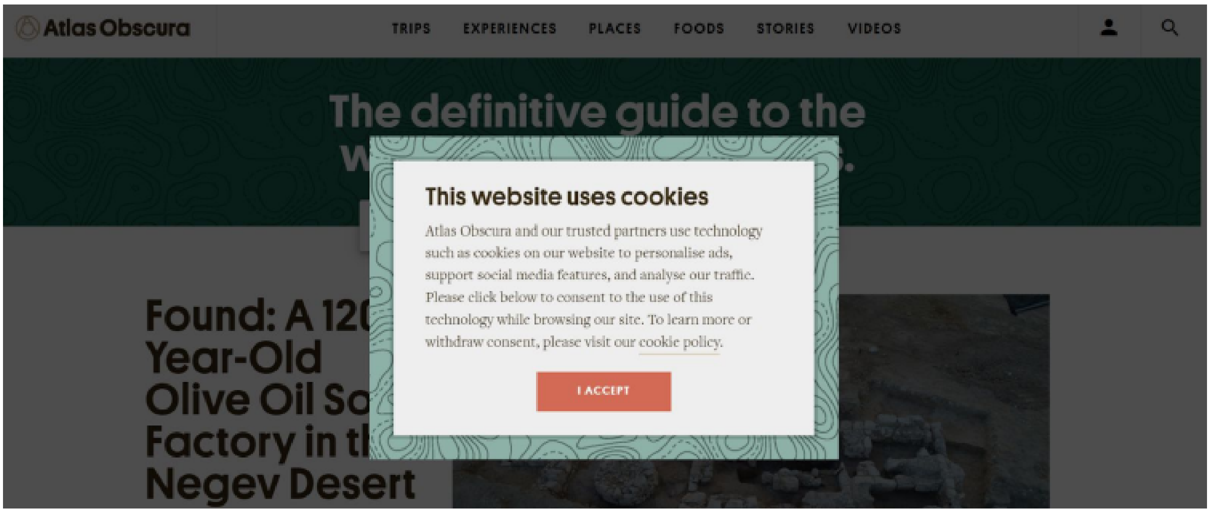
In the meantime, two US presidential elections and one global pandemic have happened, pushing people to become "more online" in different ways - from the advent of online political discourse and even radicalization (more than once resulting in non-digital acts of terrorism, such as the extremely recent case of a teenage far-right terrorist who fatally shot two people in the US [3]) to the convenience and even necessity of online shopping, online socializing, online entertainment. It is becoming apparent that the popular acronym "IRL" may be outdated; life on the internet *is* real life.

In this context of online presence being a large, diverse (and, pertinently, traceable) part of one's life, a new level of seriousness applies to online environments and regulations on their content and presentation. An internet user will encounter hundreds, if not thousands of design choices on multiple devices over the course of a single day, and this inevitably has a certain impact and consequences. This paper's focus will be on corporations and organizations making such choices with malicious intent and with the goal of manipulating user behaviour to their own advantage through the use of so called dark patterns.

2 What is a dark pattern?

A simple definition of dark patterns from the website darkpatterns.org (created by the inventor of the term, Harry Brignull) states, “Dark Patterns are tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something” [4]. The site aims to spread awareness about these practices and give regular internet users the tools to notice and avoid them. Among an extensive list of dishonest design are “trick questions” on forms, guilting users into agreeing to a particular option, visuals which purposefully lead the gaze away from important information, misleading the user into sharing more personal information than they intended, and “disguised” advertisements posing as, say, useful articles [5].

An easy way to grasp the concept is by example. Almost anyone could recognize a situation like the following, which happened in this exact sequence on a website providing local-knowledge-style guides to less mainstream tourist locations. You, the user, may click on a link shared by one of your colleagues (like I did) and be confronted with the following webpage (like I was).



This website uses cookies

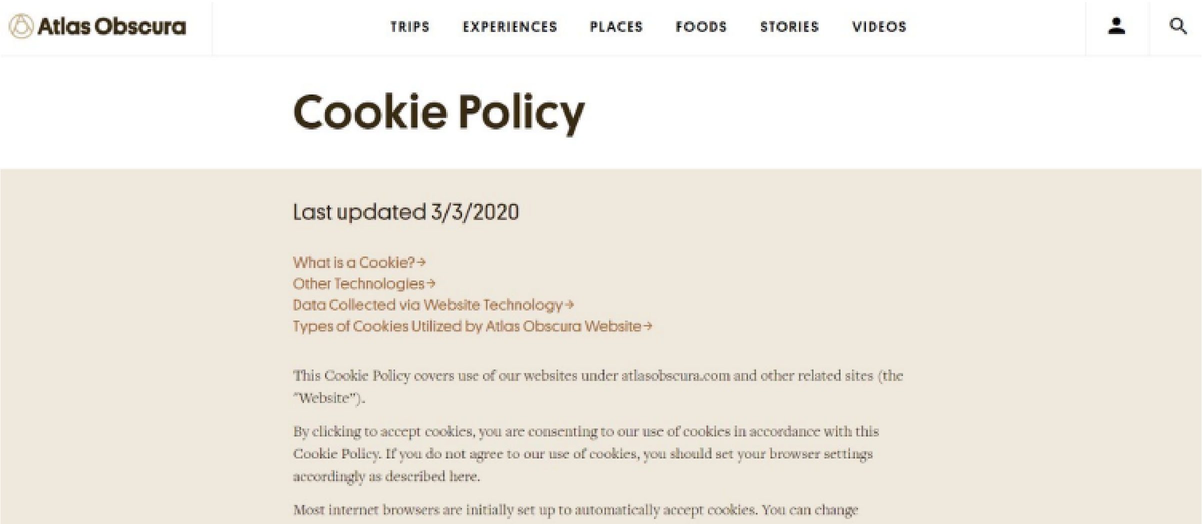
Atlas Obscura and our trusted partners use technology such as cookies on our website to personalise ads, support social media features, and analyse our traffic. Please click below to consent to the use of this technology while browsing our site. To learn more or withdraw consent, please visit our cookie policy.

Figure 1: Modal window asking for consent to use cookies, Atlas Obscura website (atlasobscura.com)

As you may notice, the button to accept cookies is placed front and center and is a prominent colour. On the other hand, to “withdraw consent,” you must visit an inconspicuous link leading to the cookie policy - not where you would normally expect to perform this action. This is a clear-cut example of misdirection: leading the user away from the place where they may choose not to share cookie information. Even if this doesn’t work, and you click on the link, a strange sequence of events occurs.

1. The cookie policy is opened in a different tab, while the page where you clicked the link remains the same.
2. Upon switching to the new tab, you discover that it contains a wall of text detailing the website’s cookie policy.

3. Provided you stick around, you may find that the link to withdraw consent is hidden among the text.
4. At that point, it turns out that clicking it does not remove the notification window in the first tab: meaning that, ultimately,
5. To withdraw consent from cookies and also view the content of the site, you must first agree to cookies, and *then* switch to the other tab to withdraw your cookie consent.



Cookie Policy

Last updated 3/3/2020

What is a Cookie?→
Other Technologies→
Data Collected via Website Technology→
Types of Cookies Utilized by Atlas Obscura Website→

This Cookie Policy covers use of our websites under atlasobscura.com and other related sites (the "Website").

By clicking to accept cookies, you are consenting to our use of cookies in accordance with this Cookie Policy. If you do not agree to our use of cookies, you should set your browser settings accordingly as described here.

Most internet browsers are initially set up to automatically accept cookies. You can change

Figure 2: Atlas Obscura website cookie policy (https://www.atlasobscura.com/cookies)

This is a completely random example that I did not seek out but just happened upon in my regular online activities. Surely, many more easily come to mind: Facebook encouraging its users to share as much personal information as possible; YouTube's algorithm pushing "related content" in the hopes people will keep watching for as long as possible (this, incidentally, will become very relevant to this paper later on); Amazon hidden costs, like delivery, being added to the user's cart at the very end; Buzzfeed running articles which contain hidden advertisements for a product and sometimes even direct links to buy it; LinkedIn sending spam emails under its users' real names to their entire list of email contacts; and so on, and so forth.

This means that it is increasingly difficult to safely navigate online spaces, even trusted or unavoidable ones. Due to the fact that design knowledge is for the most part not common knowledge, it is easy for many people (especially less tech-savvy or older ones) to fall into the traps set up by malicious design. This is why it's crucial to educate the public (for example, through sites such as darkpatterns.org), but also to ponder the consequences of employing design skill for the purpose of generating profit rather than providing a quality user experience. Just as with programming, AI, or robotics, the practice of design comes with ethical considerations and responsibilities, which, as we have seen, have the potential to be compromised.

3 The ethical angle

A commonly found feature of dark patterns and deceptive design is that they are difficult to regulate by legal means. While in the example of LinkedIn sending spam emails a lawsuit was eventually filed and resulted in the company paying roughly $10 per scammed user, usually such practices are technically legal [6]. So, the question arises: how much of the responsibility for them lies on the shoulders of the designers and programmers who implement them?

An argument could be made that the user has a personal responsibility to become educated and careful when it comes to such problems. Harry Brignell himself states that the best way to combat dark patterns is to educate the average person about them [6]. However, this argument shares a weakness with many others of its type when it comes to issues that occur on the level of society rather than a single individual: there are many factors that may preclude users from looking out for themselves - age, ability, access to education, even simply time. When a service is locked behind agreement to "terms and conditions," which are long, convoluted, and usually involve data harvesting, is the user (who may be required to use the service) really providing informed consent? Furthermore, as the ancient Bulgarian saying goes, "The fault is not with him who buys the banitza*, but with the one who sells it."

Then, the next question we must ask is: Who sells the banitza? Is it the developers and designers, the corporations who employ them, both, or the very system they operate under? It is easy to place responsibility at the feet of the creators of the product itself, such as design teams - after all, they are the ones who facilitate its existence. However, they are rarely the ones who call the shots when it comes to product requirements - is it then the company and its board that we must hold responsible for putting profit margins above user wellbeing? Or can we go several levels up and claim that a company, if it wishes to continue existing, must strive for maximum competitiveness, and so it becomes almost inevitable to resort to unethical means like the use of dark patterns in design? The scope of a short reflection paper does not cover the answers to these questions, which can lead us down a philosophical rabbit hole with the likes of Hannah Arendt (*Personal Responsibility Under Dictatorship*) and Derrida (*Specters of Marx*). But nevertheless, I believe simply raising them is not meaningless, as it invites a personal answer for individual designers who may end up working with such companies - and personal philosophy need not always be rooted in theory. (In addition, it is not impossible to organize the workplace and thus take responsibility collectively instead of individually.)

* Delicious cheese-filled Bulgarian pastry, and in this case, a metaphor.

4 The political angle

Earlier on I touched lightly on the matter of informed consent: if a website is using a dark pattern to trick users into surrendering more data than they otherwise would have, or showing them “native advertising” that masquerades as a lifestyle article, that is clearly neither informed nor really consent. Furthermore, if the content of a page is behind an “agreement” window such as the one from our earlier example, and the user must, for one reason or another, view said content, is that a case of giving informed consent (even if one is not being actively deceived)? The necessity of viewing the website, depending on the context, could be coercing users into “consenting” to terms they would not have normally accepted.

Few users will actually have read the long, technical-sounding texts of most terms and conditions agreements. If I asked you, the rhetorical user, to tell me what data each website collects, where it stores it and how securely, how long it keeps it for, or who it shares it with, I would not actually expect you to be able to tell me - and that is not a problem just in the realm of ethics [7]. In her work *Data*, British philosopher Abigail Thorn discusses the possibility of corporations sharing data with governments: “Targeted advertising requires targeted surveillance” [7]. So, in this sense, dark patterns, especially ones that mislead users into sharing their private data, may lead to real-world political consequences for those users or the society they live in, such as free speech limitations and the advent of monitoring systems based on AI/ bioinformatics.

That, however, is not the only kind of dark pattern with potentially serious political consequences. Infamously, YouTube’s recommendation algorithm tends to lead some of its users down the path of far-right radicalization [8]. In a 2019 interview, former rightwing radical Caleb Cain details how he got sucked in: from watching self-help videos, through clicking on a recommendation for white supremacist Stefan Molyneux’s channel, to consuming hundreds of “alt-right” videos [9]. The algorithm, while a YouTube user could technically tailor it by repeatedly clicking “I’m not interested” (an option hidden in an on-hover menu to the side of the video thumbnail) on recommendations, is not really a feature one gets to agree to or can get rid of. All of the responsibility to avoid this evidently frequent pitfall falls on the user, who, like Mr. Cain and many others, may be vulnerable emotionally or in other ways to such methods of online radicalization.

5 Conclusion

In the end, this paper poses more questions than it answers; but if there can be one takeaway, it should be that practices like dark patterns affect more than just the user of a website, and that as a designer, one must put thought into not only producing quality products, but also how those products are being used. It is worth discussing what can be done on both an individual and a collective level to ensure that design truly is user-centered: performed with people’s wellbeing in mind first, and at all times.

REFERENCES

[1] “Official Legal Text.” General Data Protection Regulation (GDPR), 2 Sept. 2019, gdpr-info.eu.

[2] Cadwalladr, Carole, and Emma Graham-Harrison. “Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach.” The Guardian, 17 Mar. 2018.

[3] Devega, Chauncey. “What the Kenosha Shooter Tells Us about Donald Trump's America.” Salon, 28 Aug. 2020.

[4] Brignell, Harry. Edited by Alexander Darlington, Dark Patterns, darkpatterns.org/index.html.

[5] Brignell, Harry. Edited by Alexander Darlington, Dark Patterns - Types of Dark Pattern, darkpatterns.org/types-of-dark-pattern.html.

[6] Nerdwriter1. How Dark Patterns Trick You Online. YouTube, 28 Mar. 2018, www.youtube.com/watch?v=kxkrdLI6e6M.

[7] Thorn, Abigail. Data. YouTube, 31 Jan. 2020, www.youtube.com/watch?v=fCUTX1jurJ4.

[8] Basu, Tanya. “YouTube’s Algorithm Seems to Be Funneling People to Alt-Right Videos.” MIT Technology Review, 29 Jan. 2020.

[9] Roose, Kevin. “The Making of a YouTube Radical.” The New York Times, 8 June 2019.