

2022-09-19

## **“Be a Pattern for the World”: The Development of a Dark Patterns Detection Tool to Prevent Online User Loss**


Jordan Donnelly  
*Technological University Dublin*

Alan Downley  
*Technological University Dublin*

Yunpeng Liu  
*Technological University Dublin*

*See next page for additional authors*

Follow this and additional works at: <https://arrow.tudublin.ie/ascnetart>

 Part of the [Applied Ethics Commons](#), [Computer Sciences Commons](#), [Data Science Commons](#), and the [Mass Communication Commons](#)

---

### **Recommended Citation**

Donnelly, J., Dowley, A., Liu, Y., Su, Y., Sun, Q., Zeng, L., Curley, A., Gordon, D., Kelly, P., O'Sullivan, D., Becevel, A. “Be a Pattern for the World”: The Development of a Dark Patterns Detection Tool to Prevent Online User Loss. Proceedings of Ethicomp, 20th International Conference on the Ethical and Social issues in Information and Communication Technologies, Turku, Finland, 26-28th July, 2022. DOI: 10.21427/2Y2Q-6323

This Conference Paper is brought to you for free and open access by the Applied Social Computing Network at ARROW@TU Dublin. It has been accepted for inclusion in Articles by an authorized administrator of ARROW@TU Dublin. For more information, please contact [arrow.admin@tudublin.ie](mailto:arrow.admin@tudublin.ie), [aisling.coyne@tudublin.ie](mailto:aisling.coyne@tudublin.ie), [gerard.connolly@tudublin.ie](mailto:gerard.connolly@tudublin.ie), [vera.kilshaw@tudublin.ie](mailto:vera.kilshaw@tudublin.ie).

Funder: European Union

---

## Authors

Jordan Donnelly, Alan Downley, Yunpeng Liu, Yufei Su, Quanwei Sun, Lan Zeng, Andrea Curley, Damian Gordon, Paul Kelly, Dymphna O'Sullivan, and Anna Becevel

## “Be a Pattern for the World”: The Development of a Dark Patterns Detection Tool to Prevent User Loss

Jordan Donnelly<sup>1</sup>, Alan Dowley<sup>1</sup>, Yunpeng Liu<sup>1</sup>, Yufei Su<sup>1</sup>, Quanwei Sun<sup>1</sup>, Lan Zeng<sup>1</sup>, Andrea Curley<sup>1</sup>, Damian Gordon<sup>1</sup>, Paul Kelly<sup>1</sup>, Dymrna O'Sullivan<sup>1</sup> Anna Becevel<sup>1</sup>

<sup>1</sup>Technological University of Dublin, Ireland

Damian.X.Gordon@TUDublin.ie

**Abstract.** Dark Patterns are designed to trick users into sharing more information or spending more money than they had intended to do, by configuring online interactions to confuse or add pressure to the users. They are highly varied in their form, and are therefore difficult to classify and detect. Therefore, this research is designed to develop a framework for the automated detection of potential instances of web-based dark patterns, and from there to develop a software tool that will provide a highly useful defensive tool that helps detect and highlight these patterns

### 1 Introduction

Research on dark patterns covers a range of different fields, including Cognitive Psychology, Usability, Marketing, Behavioural Economics, Design and Digital Media. There is no general agreement that explains their effectiveness, however the traditional decision-making theories, including rational choice theories have been shown to be ineffective in explaining their success (Acquisti, *et al.*, 2017). However, two things that appear to be able to explain some of their effectiveness are *cognitive biases* and *digital nudges*. Cognitive biases are short-cuts (or heuristics) that the human brain makes in decision-making due to the fundamental limitations of the information processing of the brain (Kahneman, 2011). According to Waldman (2020) the five most pervasive are: anchoring, framing, hyperbolic discounting, overchoice, and metacognitive processes such as cognitive scarcity and cognitive absorption. Digital nudges are a manipulation strategy based on the notion that small changes can have a big effect (for example, a personalized email that reminds someone to complete an enrolment form) and nudges are based on the notions of soft paternalism, positive reinforcement and compliance (Acquisti, 2009; Almuhiemedi, *et al.*, 2015). However, unlike dark patterns, nudges can be used either for positive outcomes or negative ones (Peer, *et al.*, 2020).

Chugh and Jain (2021) explored dark patterns from the perspective of consumer protection, as well as their impact on democratic political processes. The researchers make a key distinction between dark patterns and regular advertisements that are persuasive. Their research indicates that dark patterns are deliberately manipulative, whereas persuasive advertisements merely attempt to influence people to revise their preferences. They indicate that there are two major issues with dark patterns, (1) users are typically unaware that they are interacting with dark patterns, and are, therefore, unable to safeguard themselves against their effects, and (2) market forces and market competition are not penalizing organizations for using these patterns. The researchers recommend that legislation and regulations are necessary to combat these patterns.

Bongard-Blanchy *et al.* (2021) looked at the impact of dark patterns on endusers by surveying 406 participants. They found that although all of the respondents were aware of the manipulative techniques that online services use, they are nonetheless unable to combat their impact. The researchers advocate a multi-faceted approach to addressing these issues, including an education programme to explain to people about the different patterns and how they work, as well as providing information on how to resist and avoid these patterns. They also suggest that a combination of strong legal penalties and regulations are required, as well as new software tools to help detect and highlight the existence of these patterns.

Mathur, *et al.*, (2019) undertook a meta-analysis of over 11,000 shopping websites, and created a taxonomy to try to explain how dark patterns affects user decision-making, and their taxonomy has the following characteristics: Asymmetric, Covert, Deceptive, Hides Information, and Restrictive. They found that 11.1% (1254 websites) of the sites had dark patterns, and they recommend the development of plug-ins for browsers to help detect these patterns.

UX researcher Harry Brignull (2011) was a pioneering researcher in this field, and first presented definitions of dark patterns, some of which are:

1. **Sneak into Basket:** Some websites add an additional item into the customer's digital shopping basket, and it is usually the new product that is added in because of a hidden opt-out button or checkbox on a previous page.
2. **Hidden Costs:** Some websites add unexpected charges into the customer's digital shopping basket, e.g. delivery charges, etc.
3. **Trick Questions:** When registering for a new service, some websites present a series of checkboxes, and the meaning of checkboxes is alternated so that ticking the first one means "opt out" and the second means "opt in".
4. **Misdirection:** Some website purposefully focuses users' attention on one thing in order to distract their attention from another, for example, a website may have already undertaken a function and added a cost to it, and the opt out button is small.
5. **Confirmshaming:** Some websites try to guilt the user into opting into doing something, for example, "No thanks, I don't want to have unlimited free deliveries".
6. **Disguised Ads:** Some websites include advertisements that are disguised as other kinds of content or navigation, in order to get you to click on them, for

example, advertisements that look like a “download” button or a “Next >” button.

UX researcher Reed Steiner (2021) identified six types of patterns:

1. **Fake Activity:** Some websites claim that other shoppers are looking at the same products, for example, websites that claim “five other people are viewing this item right now” might not be fully truthful.
2. **Fake Reviews:** Some websites include reviews of products and services that may be fake, and exact matches with different customer names can be found on several sites.
3. **Fake Countdown:** Some websites countdown or timers, and in most cases these timers only add urgency to a sale.
4. **Ambiguous Deadlines:** Some websites indicate that a product is only on sale for a limited amount of time, but don’t mention a specific deadline.
5. **Low Stock Messages:** Some websites claim that they are low on a particular item.
6. **Deceptive High Demand:** This is similar to the low stock messages, but focuses on the high demand for a particular product.

## 2 Development

The software tool was developed as an overlay onto a browser page, using a combination of Python, NodeJS and Javascript. It is possible to detect six dark pattern types with this tool: Fake Activity, Fake Countdown, Fake Limited-time, Fake Lowstock, Fake High-demand, and Confirmshaming. To detect dark patterns on the webpage, the HTML of the webpage needs to be analyzed first for text extraction. A specific tag type will be assigned to each text string extracted and the pre-processed data will be ready for detection. To detect text in an image, Optical Character Recognition (OCR) is used. OCR is the technology that allows users to detect, analyze and extract texture data from the image file. If image detection is enabled (when OCR is on), the image detection will be conducted first to extract text from the source images and add the extracted text back to the pre-processed dataset for detection. If image detection is not enabled (when OCR is off), the detection will be directly conducted after data pre-processing.

User evaluation and usability testing can be done in many different forms, from a simple questionnaire about the product to letting the users use it and gathering their reactions and thoughts throughout the process using both the think-aloud protocol and cognitive walkthrough, with 96 users. Those users felt the systems was very helpful and clear in its purpose and detection process.

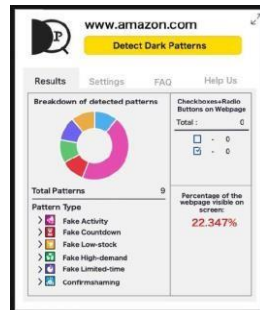


Figure 1. Dark Patterns Detection Tool

Some notable limitations of the study include the following:

1. It might be the case that some of the patterns simply cannot be detected, as they vary so much in implementation. If so, it significantly limits the efficacy of the final system - a thorough exploration of the Mathur *et al.* dataset is needed, as well as a number of further brainstorming sessions, to explore potential solutions.
2. Some sites have a special file called `Robots.txt` that prohibits the use of web scraping, and it is also the case that some sites use technologies that make them more difficult to parse, for example, frames or webpages implemented in Javascript or CSS.
3. Many shoppers use mobile applications instead of websites to purchase products and services, and the techniques outlined so far would be ineffective on these applications.

### 3 Conclusions

It is worth noting that sometimes the terminology itself can be a barrier, although everyone who has shopped online has experienced dark patterns, nonetheless, the terminology itself may be unfamiliar and therefore confusing, for example the terms “Roach Motel” and “Friend Spam” are opaque as to their meaning and impact (changing “Roach Motel” to “Hard to Unsubscribe”, and changing “Friend Spam” to “May use your addressbook” might a solution. It is also worth noting that the Optical Character Recognition (OCR) aspect of the system was able to read text from images to determine if there were dark patterns on the images, however, on websites that are image-heavy this proved to be prohibitive in terms of overall scan time of webpages, therefore a toggle to turn on and off the OCR features was added. Finally, perhaps one of the most significant outcomes of this research was that it created an opportunity to interrogate our fundamental understanding of the notion of a Dark Pattern. There is a fine line between dark patterns and persuasive advertisements (which do not rely on pressuring or confusing the customers). For example, an advertisement that includes the phrase: “Customers who bought this product also bought ...” were initially

classified as Dark Patterns by the system, as they are similar to a “Fake Activity” which may say something like “Other Customers are looking at this product”, but they are pressuring the customers in the same way.

## References

- Acquisti, (2009) “Nudging privacy: The behavioral economics of personal information”. *IEEE Security & Privacy*, 7(6), pp. 82-85.
- Acquisti, I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, S. Wilson. (2017) “Nudges for privacy and security: Understanding and assisting users’ choices online”, *ACM Computing Surveys (CSUR)*, 50(3), pp. 1-41.
- H. Almuhiemedi, F. Schaub, N. Sadeh, N.I. Adjerid, A. Acquisti, J. Gluck, Y. Agarwal. (2015) “Your location has been shared 5,398 times! A field study on mobile app privacy nudging”. In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pp. 787-796.
- K. Bongard-Blanchy, A. Rossi, S. Rivas, S. Doublet, V. Koenig, G. Lenzini. (2021) "I am Definitely Manipulated, Even When I am Aware of it. It s Ridiculous!--Dark Patterns from the End-User Perspective". *arXiv preprint arXiv:2104.12653*.
- H. Brignull. (2011) “Dark patterns: Deception vs. honesty in UI design”. *Interaction Design, Usability*, 338,
- Chugh, P. Jain (2021)"Unpacking Dark Patterns: Understanding Dark Patterns and Their Implications for Consumer Protection in the Digital Economy". *RGNUL Student Research Review Journal*, 7, 23.
- L. Di Geronimo, L. Braz, E. Fregnan, F. Palomba, A. Bacchelli, "UI Dark Patterns and Where to Find Them: A Study on Mobile Applications and User Perception", *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, April 2020.
- Kahneman. ( 2011) “Thinking, Fast and Slow”, Penguin Books.
- Peer, S. Egelman, M. Harbach, N. Malkin, A. Mathur, A. Frik. (2020) “Nudge me right: Personalizing online security nudges to people's decision-making styles”. *Computers in Human Behavior*, 109, 106347.
- Mathur, G. Acar, M. J. Friedman, E. Lucherini, J. Mayer, J. M. Chetty, A. Narayanan, A.(2019) “Dark patterns at scale: Findings from a crawl of 11K shopping websites”. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), pp. 1-32.
- R. Steiner. (2021) “Dark Patterns” . [Online]. Available from: <https://www.fyresite.com/dark-patternsa-new-scientific-look-at-ux-deception/>, 2021.06.24
- E. Waldman (2020) “Cognitive biases, dark patterns, and the ‘privacy paradox’”. *Current opinion in psychology*, 31, pp. 105-109