2021-7

The Design of a Framework for the Detection of Web-Based Dark Patterns

Andrea Curley
Technological University Dublin, Andrea.F.Curley@TUDublin.ie

Dympna O'Sullivan
Technological University Dublin, dympna.osullivan@tudublin.ie

Damian Gordon
Technological University Dublin, Damian.X.Gordon@TUDublin.ie

See next page for additional authors

Recommended Citation

Curley, A., O'Sullivan, D., Gordon, D., Tierney, B., Stavrakakis, I. (2021) The Design of a Framework for the Detection of Web-Based Dark Patterns", *ICDS 2021: The 15th International Conference on Digital Society*, Nice, France, 18th – 22nd, July 2021 (online).

“Give light, and the darkness will disappear of itself”: The Design of a Framework for the Detection of Web-Based Dark Patterns

Andrea Curley, Dympna O’Sullivan, Damian Gordon, Brendan Tierney, Ioannis Stavrakakis
School of Computer Science, Technological University Dublin, Dublin, Ireland
Email: Andrea.F.Curley@TUDublin.ie, Dympna.OSullivan@TUDublin.ie, Damian.X.Gordon@TUDublin.ie,
Brendan.Tierney@TUDublin.ie, Ioannis.Stavrakakis@TUDublin.ie

***Abstract*— In the theories of User Interfaces (UI) and User Experience (UX), the goal is generally to help understand the needs of users and how software can be best configured to optimize how the users can interact with it by removing any unnecessary barriers. However, some systems are designed to make people unwillingly agree to share more data than they intend to, or to spend more money than they plan to, using deception or other psychological nudges. User Interface experts have categorized a number of these tricks that are commonly used and have called them Dark Patterns. Dark Patterns are varied in their form and what they do, and the goal of this research is to design and develop a framework for automated detection of potential instances of web-based dark patterns. To achieve this we explore each of the many canonical dark patterns and identify whether or not it is technically possible to automatically detect that particular pattern. Some patterns are easier to detect than others, and there others that are impossible to detect in an automated fashion. For example, some patterns are straightforward and use confusing terminology to flummox the users, e.g. “Click here if you do not wish to opt out of our mailing list”, and these are reasonably simple to detect, whereas others, for example, sites that prevent users from doing a price comparison with similar products might not be readily detectable. This paper presents a framework to automatically detect dark patterns. We present and analyze known dark patterns in terms of whether they can be: (1) detected in an automated way (either partially or fully), (2) detected in a manual way (either partially or fully) and (3) cannot be detected at all. We present the results of our analysis and outline a proposed software tool to detect dark patterns on websites, social media platforms and mobile applications.**

Keywords: Dark Patterns; User Experience; Digital Ethics; Privacy.

I. INTRODUCTION

Computers and technological applications are now central to many aspects of life and society, from industry and commerce, government, research, education, medicine, communication, and entertainment systems. Computer scientists and professionals from related disciplines who design and develop computer applications have a significant responsibility as the systems they develop can have wide ranging impacts on society where those impacts can be beneficial but may also at times be negative. Grosz et al. [17] argue that modern technology cannot be considered “value-neutral” (p. 54); as it can have unplanned negative consequences.

In this paper, we outline and explore the ethical limits of a technology design phenomenon known as "dark patterns”. Dark patterns are user interfaces that benefit an online service by leading users into making decisions they might not otherwise make. At best, dark patterns annoy and frustrate users. At worst, they can mislead and deceive users, e.g., by causing financial loss, tricking users into giving up vast amounts of personal data or inducing compulsive and addictive behavior in adults and children. They are an increasingly common occurrence on digital platforms including social media sites, shopping websites, mobile apps, and video games.

Although they are gaining more mainstream awareness in the research community, dark patterns are the result of three decades-long trends: one from the world of retail (deceptive practices), one from research and public policy (nudging), and the third from the design community (growth hacking) [26]. For example, techniques, such as psychological pricing (that is, making the price slightly less than a round number), have become normalized in retail, nudging has long been used to change user behavior in retail and marketing through suggestions and reinforcement of messages and growth hacking is using low-cost strategies such as spamming a user’s contacts with invitations to try a service in order to help businesses acquire and retain customers.

The aim of our work is the development of a framework for detecting web-based dark patterns. The framework forms the basis of a software tool that can automatically alert users to the presence of dark patterns on websites, social media platforms and mobile applications.

In developing the framework we analysed common documented types of data patterns. We present these dark patterns to the reader and classify each dark pattern using the following taxonomy: (1) A pattern that can be detected in an automated way (either partially or fully); (2) A pattern that can be detected in a manual way (either partially or fully); and (3) A pattern that cannot be detected. These classifications dictate the type of automated software. In this paper we outline the features and functionality of the proposed tool. This research is part of a larger research project (called Ethics4EU) whose goal is develop a repository of teaching and assessment resources to support the teaching of ethics in computer science courses, supported by the Erasmus+ programme [28].

II. LITERATURE REVIEW

Since the early 1980s computer programmers have used the concept of patterns in software engineering as a useful

way of categorizing different types of computer programs. The term dark patterns has been used since 2010 to refer to interface design solutions that intend to deceive users into carrying out undesirable actions [9]. Gray, et al. [16] defined dark patterns as "instances where designers use their knowledge of human behavior (e.g., psychology) and the desires of end users to implement deceptive functionality that is not in the user's best interest".

There has been significant research done on dark patterns from the fields of Cognitive Psychology, Usability, Marketing, Behavioural Economics, Design and Digital Media. All this research has led to the abandonment of the rational choice theories for explaining decision making, particularly for matters of privacy [2] and has prompted new examinations that attribute the effectiveness of dark patterns on human cognitive limitations. However, there is still not a universal theoretical explanation of the 'whys' and 'hows' of the effectiveness of dark patterns. For example, Maier [22] argues that manipulation is closely linked to decision making and the latter can be easily influenced through one's emotions and mood leading to decisions lacking rational thought [24].

What is more, according to Kahneman [19] there are two distinct systems of thought in the human brain. There is the non-conscious, spontaneous, simplified system of thinking on the one hand and the rational, conscious thinking system on the other. In his 2011 book, Kahneman argues that humans are more intuitive than rational thinkers and most of their daily reasoning is performed by the former system.

Below are the main human psychological mechanisms being targeted or exploited by Dark Patterns [10]:

- Nudging, which is based on soft paternalism, positive reinforcement and compliance [1]. Nudging can be and has been used with good intentions in mind and has been proved effective [29][7]. However, because of its proven efficiency, nudging is one of the most common digital manipulation strategies used to mislead users into bad decisions privacy-wise.

- Persuasion techniques built on what Cialdini [12] identifies as the "six basic tendencies of human behaviour" [13] (p.76). These tendencies namely are: reciprocation, consistency, social validation, liking, authority and scarcity.

- Cognitive biases that fundamentally are information processing limitations of the human mind and are rooted in cognitive heuristic systems [19]. According to Waldman [33] the five most pervasive are: anchoring [8], framing [5], hyperbolic discounting [4][30][34], overchoice [11][25][18][14] and metacognitive processes such as cognitive scarcity [32] and cognitive absorption [6].

- Cognitive dissonance, an uncomfortable state of mind where one's beliefs and actions are contradictory. Bosch et al. [10] (p.247) mention "[i]n terms of privacy dark patterns, this process can be exploited by inconspicuously providing justification arguments for sugar-coating user decisions that have negatively affected their privacy".

Although, so far, it appears that the cognitive and psychological factors play a significantly important role on users' failure to protect their privacy when dealing with Dark Patterns, some researchers argue that contextual and social factors are important too. For example, Acquisti et al. [2] claim that incomplete or asymmetric access to information between two agents in a transaction can significantly disadvantage one party leading to problematic decisions. Furthermore, users are not always certain of what they are agreeing to share as the collection of personal data is not always apparent and therefore people remain unaware of what information is collected about them by both private and public organisations [3]. This is usually the norm in digital environments where the user has no control over the design and information processing they are being shown.

On the other hand, research has shown that users, care about their privacy [20], however, the contextual, social and cognitive aspects mentioned earlier lead users to a set of behaviours that are inconsistent to their attitudes towards privacy [27][33]. Norberg et al. [27] have called this the 'privacy paradox'.

In today's digital environment most digital platforms' provide services seemingly for free. In order for these services to generate revenue they have become dependent on accumulating and processing users' data, oftentimes personal data [15]. According to Zuboff [35] user data is the raw material that produces, what she calls, 'behavioural surplus' which has become a valuable commodity for companies. Behavioural surplus is a powerful tool for predicting user behaviour and many companies use it to influence users into providing more data which leads into a vicious cycle of user data, influence, prediction and so on [31].

Mathur et al. [23] did a meta-analysis of 11,286 shopping websites, and found that 11.1% (1254 websites) of the sites had dark patterns, and recommend the development of plug-ins for browsers to help detect these patterns. They also found that many of these patterns are unlawful in the United States law (under Section 5 of the Federal Trade Commission Act and similar state laws), and in the European Union, under the Unfair Commercial Practices Directive.

Dark patterns are only just beginning to emerge as a topic in the software development literature. In 2021 Kollnig et al. [21] reported in the development of a functional prototype that allows users to disable dark patterns in apps selectively. This differs from our approach where we are developing a comprehensive framework for identifying dark patterns across a range of platforms, from apps to websites.

III. METHODS

A vital step in developing the web-based Dark Patterns Framework is to clearly define each pattern and to categorize the patterns into themes. In the research literature previously discussed there is some variance as to the exact meaning of each pattern, therefore below we present definitions that

attempt to be as inclusive as possible to the range of definitions for each pattern, but always prioritising the original canonical definitions developed by the pioneer of dark patterns - user experience designer Harry Brignull [9].

A. *Sneaking*

- **Sneak into Basket:** When purchasing a product, an additional item is added into the basket, usually the new product is added in because of an obscured opt-out button or checkbox on a previous page.
- **Hidden Costs:** When reaching the last step of the checkout process, some unexpected charges have appeared in the basket, e.g. delivery charges, tax, etc.

B. *Misdiretion*

- **Trick Questions:** Often found when registering for a new service. Typically, a series of checkboxes are shown, and the meaning of checkboxes is alternated so that ticking the first one means "opt out" and the second means "opt in".
- **Misdirection:** When the design 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.
- **Confirmshaming:** This involves guilting the user into opting into something. The option to decline is worded in such a way as to shame the user into compliance, for example, "No thanks, I don't want to have unlimited free deliveries".
- **Disguised Ads:** 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.

C. *Obstruction*

- **Roach Motel:** When users find it easy to subscribe to a service (for example, a premium service), and find it is hard to get out of it, like trying to cancel a shopping account.

D. *Forced Action*

- **Forced Continuity:** When a user gets a free trial with a service comes to an end and their credit card silently starts getting charged without any warning, and there isn't an easy way to cancel the automatic renewal.

E. *Variegations*

- **Privacy Zuckering:** Tricking users into sharing more information than they intended to, for example, Facebook privacy settings were historically difficult to control.
- **Price Comparison Prevention:** The retailer makes it hard for you to compare the price of an item with another item, so you cannot make an informed decision. Retailers typically achieve this by creating different bundles where it is not easy to work out the unit price of the items within the bundles.
- **Bait and Switch:** The user sets out to do one thing, but a different, undesirable thing happens instead, for example, Microsoft's strategy to get users to upgrade their computers to Windows 10.
- **Friend Spam:** The product asks for users for their email or social media permissions under the pretense it will be used for a desirable outcome (for example, finding friends), but then spams all their contacts in a message that claims to be from the user.

IV. FRAMEWORK FOR DERECTING DARK PATTERNS

With these definitions established, it becomes possible to categorize the patterns into one of the following three classifications:

1) A suspected pattern that can be detected in an automated way (partially or fully) based on the text, images or HTML in a webpage or website.
2) A suspected pattern that can be detected in a manual way (partially or fully) based on the text, images or HTML in a webpage or website.
3) A suspected pattern that cannot be detected, based on the fact that there is so much variation in either how the pattern is defined or in how the pattern is implemented

Our full framework is presented below in Table 1 where each of the patterns presented in Section III is classified as to how it can be detected (automated, manually or cannot be detected), as well as some detail as to how such a pattern can be detected (or, in fact, if it cannot be detected) as shown in the *Rationale* column.

Patterns that can be detected automatically will typically have terms in them such as "opt-in", "activate", or "subscribe". These, and other indicators such as the placement or configuration of images, or in the formulation of the HTML tags, allow for the automated detection of dark patterns. In contrast, there are some web-based activities or transactions that cannot, in and of themselves, be automatically detected, but are sufficiently indicative to suggest the presence of a dark pattern. In these cases the framework proposes the development of an ancillary (or appurtenant) window to highlight to the users that there may be something suspicious occurring in the transaction that they are undertaking. Finally, it is worth noting that, there are some patterns that cannot readily be detected, but may be reported using the reporting feature of the system.

The potential detection of *web-based* patterns can be implemented using web crawling and web scraping techniques, as well as natural language processing approaches.

TABLE I. DARK PATTERNS AND THEIR DETECTION

Category	*Pattern*	*Detection*	*Rationale*
Sneaking	Sneak into Basket	Manual (fully)	Highlight changes in cost
	Hidden Costs	Manual (fully)	Highlight changes in cost
Misdirection	Trick Questions	Automated (partially)	Look for phrases like "opt-in" and "opt-out", as well as pre-ticked checkboxes
	Misdirection	Cannot be detected	There is too much variation in how this pattern is implemented.
	Confirmshaming	Cannot be detected	There is too much variation in how this pattern is implemented.
	Disguised Ads	Automated (partially)	Look for buttons (noting colour and size) and see which ones link to external sites.
Obstruction	Roach Motel	Automated (fully)	Look for sites with "activate" or "subscribe" links or buttons but with no "deactivate" or "unsubscribe"
Forced Action	Forced Continuity	Cannot be detected	There is too much variation in how this pattern is implemented.
Variegations	Privacy Zuckering	Cannot be detected	There is too much variation in how this pattern is implemented.
	Price Comparison Prevention	Manual (fully)	Highlight if products are displayed with different units of the product
	Bait and Switch	Cannot be detected	There is too much variation in how this pattern is implemented.
	Friend Spam	Automated (partially)	Check if the site asks for email or social media permissions, and notify users.

Some patterns will have words or images that make them easy to identify ("opt in", "offer ends soon", "in demand", etc.) and therefore we can say that they are automatically detectable (either partially or fully). And, in contrast, some patterns are implemented in such a range of different ways depending on the particular interface (and the definitions of some patterns vary in different research literature), that they are impossible to consistently detect, so we classify these as "Cannot be detected". Other patterns require human judgement, such as determining if using pre-ticked checkboxes is being deceptive, or if the site is asking for security permissions, and so we classify these as being detectable manually (either partially or fully). To help recognise the patterns that can potentially be manually detected, the proposed system will allow the user to display an ancillary window that will help highlight some potential issues of concern on a given webpage or website. The new window can display things like:

- The percentage of the webpage that is visible in the browser window, to ensure the user is aware that there may be instructions or options that are not visible on the current page, but are elsewhere on the page.
- The total number of checkboxes on the page, and the number that are pre-ticked.
- The total number of radio buttons on the page, and the number that are pre-ticked.
- The shopping basket total, that will be zero if there are no items.
- A "fake review detection" tool that allows a user to select the text of a review, and to automatically search for that text elsewhere on the web.
- Highlight the number of links on the page, noting which are from text and which from images (to help detect potential Disguised Ads).
- Highlight which tick boxes or radio buttons are concerned with privacy issues, looking for words such as "privacy" or "GDPR".
- Indicate if the current webpage or website has already been reported as having a dark pattern.

Further, to help users locate suspected dark patterns on a webpage, the system will provide two modes of operation:

(1) where the system highlights all of the areas on that webpage to show suspected patterns on the page with suitable pointers, and
(2) if the user clicks on a particular type of issue on the auxiliary window, only those areas on the page will be highlighted, for example, if the user selects the "Radio Buttons" section of the panel, then all of the radio buttons on the webpage will be highlighted with pointers.

Two additional elements of the proposed system are the Reporting and Educational features:

- The *Reporting Feature* is designed to compensate for the fact that some patterns are difficult (or impossible) to detect, and it will allow users to record and report websites and webpages that they suspect have dark patterns. For example, if a user feels that they have been a victim of Forced Continuity, they can report the webpage or website, and indicate which pattern they feel is present.
- The *Educational Feature* which is designed to educate the users on each of the main dark patterns, as well as the variation among different researchers. This feature will help the users appreciate why they are being warned about a particular feature on a website as well as giving them sufficient information to allow them to accurately categorize patterns that they encounter if they wish to report them. It is envisioned that a central part of this feature will consist of a series of videoed micro-lessons.

V. CONCLUSIONS AND FUTURE WORK

This paper presented a framework for the detection of web-based dark patterns and an accompanying proposed software tool. It begins with a review of some of the key literature in this field, which highlights some of the reasons for the success of dark patterns, as well as their ubiquity. It follows this with an explanation of some of the key dark patterns, and a categorization of the patterns as being in one of the following three classifications:

1. A suspected pattern that can be detected in an automated way (partially or fully), in other words there is some characteristic either in the text, images or HTML of a webpage or website that indicates that it is a dark pattern.
2. A suspected pattern that can be detected in an manual way (partially or fully), in other words there is some characteristic either in the text, images or HTML of a webpage or website that indicates that there is potential for dark pattern on this page or site, but because it cannot be detected definitively, the potential pattern is highlighted to the user.
3. A suspected pattern that cannot be detected, in other words there is so much variation in either how the pattern is defined or in how the pattern is implemented, there is no direct way of detecting it just using web crawling and web scraping techniques.

This classification, in turn, leads to the design of a proposed software tool with the ability to detect patterns from category 1, and to highlight potential instances of patterns from category 2. For those patterns in category 3, even if there is no obvious way to identify them, nonetheless, it is important to deal with them in some way, therefore additional features are required for the system, a *Reporting feature* to address instances of patterns for category 3, as well as an *Educational feature* to create awareness about dark patterns in general.

An initial prototype system has been developed using the Python programming language which provides ample software libraries for web crawling and web scraping. It, thus, has features that have the ability to detect some of the patterns that have been classified as “Automated (partial)” and “Automated (fully)”, and early work has been undertaken on the development of the Manual features of the system.

Future work will focus on full implementation of the software tool and the inclusion of the Reporting and Education features. The Reporting features of the system are envisioned to work either in *stand-alone mode*, or *shared mode*. In stand-alone mode the reporting process is recorded locally on the user’s own computer as a series of XML files, whereas in shared mode, the user can share their suspicions about potential dark patterns with other users also using the system, and they can also label and add a description to the suspected pattern.

The Educational features will consist of a series of micro-lessons describing the range of dark patterns. Also, a series of pop-up windows will be developed with simple explanations (and links to examples) of a specific pattern will be developed, to remind the users about the key characteristics of each specific pattern.

It is worth noting that that the implementation of this framework will result in some additional challenges, for example, 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. Nonetheless, the framework provides a way forward to deal with dark patterns in a comprehensive and comprehensible manner. This has become more and more important as the number of services that have become available online continues to grow, and in many cases these services are available only exclusively online. It, therefore, becomes a matter of necessity that as many people as possible are aware of these deceitful patterns, and incumbent on IT practitioners to spread the word about these patterns.

ACKNOWLEDGMENT

The authors of this paper and the participants of the Ethics4EU project gratefully acknowledge the support of the Erasmus+ programme of the European Union. The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

REFERENCES

[1] Acquisti, A. (2009). Nudging privacy: The behavioral economics of personal information. IEEE Security & Privacy, 7(6), 82-85.

[2] Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. ACM Computing Surveys (CSUR), 50(3), 1-41.

[3] Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514.

[4] Acquisti, A., & Grossklags, J. (2003). Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. In 2nd Annual Workshop on Economics and Information Security-WEIS (Vol. 3, pp. 1-27).

[5] Adjerid, I., Acquisti, A., Brandimarte, L., & Loewenstein, G. (2013). Sleights of privacy: Framing, disclosures, and the limits of transparency. In Proceedings of the ninth symposium on usable privacy and security (pp. 1-11).

[6] Alashoor, T., Baskerville, R. (2015). The privacy paradox: The role of cognitive absorption in the social networking activity. In Thirty Sixth International Conference on Information Systems, Fort Worth, Texas, USA, 1–20.

[7] Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Agarwal, Y. (2015, April). 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).

[8] Ariely, D., Loewenstein, G., & Prelec, D. (2003). "Coherent arbitrariness": Stable demand curves without stable preferences. The Quarterly journal of economics, 118(1), 73-106.

[9] Brignull, H. (2011). Dark patterns: Deception vs. honesty in UI design. Interaction Design, Usability, 338.

[10] Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. Proceedings on Privacy Enhancing Technologies, 2016(4), 237-254.]

[11] Chernev, A., Böckenholt, U., & Goodman, J. (2015). Choice overload: A conceptual review and meta-analysis. Journal of Consumer Psychology, 25(2), 333-358.

[12] Cialdini, R. (1984). Influence. The Psychology of Persuasion. New York, NY: William Morrowe Company.

[13] Cialdini, R. B. (2001). The science of persuasion. Scientific American, 284(2), 76-81.

[14] D'Angelo, J. D., & Toma, C. L. (2017). There are plenty of fish in the sea: The effects of choice overload and reversibility on online daters' satisfaction with selected partners. Media Psychology, 20(1), 1-27./

[15] GDPR, (2016) EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament, Article 4, https://gdpr-info.eu/art-4-gdpr/

[16] Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018, April). The dark (patterns) side of UX design. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (pp. 1-14).

[17] Grosz, B. J., Grant, D. G., Vredenburgh, K., Behrends, J., Hu, L., Simmons, A., & Waldo, J. (2019). Embedded EthiCS: Integrating Ethics across CS Education. Commun. ACM, 62(8), 54–61. https://doi.org/10.1145/3330794

[18] Jilke, S., Van Ryzin, G. G., & Van de Walle, S. (2016). Responses to decline in marketized public services: An experimental evaluation of choice overload. J. of Public Administration Research and Theory, 26(3), 421-432.

[19] Kahneman, D. (2011) Thinking, Fast and Slow. Penguin Books.

[20] Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security, 64, 122-134.

[21] Kollnig, K., Datta, S. and Van Kleek, M. (2021) I Want My App That Way: Reclaiming Sovereignty Over Personal Devices. arXiv preprint arXiv:2102.11819.

[22] Maier, M. (2019).Dark patterns: An end user perspective. Master's thesis. Umeå University

[23] Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & 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), 1-32.

[24] Mehta, R. and Zhu, R. J. (2009). 'Blue or red? Exploring the effect of color on cognitive task performances', Science (New York, N.Y.), vol. 323, no. 5918, pp. 1226–1229

[25] Nagar, K., & Gandotra, P. (2016). Exploring choice overload, internet shopping anxiety, variety seeking and online shopping adoption relationship: Evidence from online fashion stores. Global Business Review, 17(4), 851-869.

[26] Narayanan, A., Mathur, A., Chetty, M., & Kshirsagar, M. (2020). Dark Patterns: Past, Present, and Future: The evolution of tricky user interfaces. *Queue*, *18*(2), 67-92.

[27] Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of consumer affairs, 41(1), 100-126.

[28] O'Sullivan, D., Gordon, D. (2020) "Check Your Tech – Considering the Provenance of Data Used to Build Digital Products and Services: Case Studies and an Ethical CheckSheet", IFIP WG 9.4 European Conference on the Social Implications of Computers in Developing Countries, 10th–11th June 2020, Salford, UK.

[29] Peer, E., Egelman, S., Harbach, M., Malkin, N., Mathur, A., & Frik, A. (2020). Nudge me right: Personalizing online security nudges to people's decision-making styles. Computers in Human Behavior, 109, 106347.

[30] Puaschunder, J. (2020). Towards a utility theory of privacy and information sharing and the introduction of hyper-hyperbolic discounting in the digital big data age. In Handbook of research on social and organizational dynamics in the digital era (pp. 157-200). IGI Global.

[31] Van Otterlo, M. (2014). Automated experimentation in Walden 3.0.: The next step in profiling, predicting, control and surveillance. Surveillance & society, 12(2), 255-272.

[32] Veltri, G. A., & Ivchenko, A. (2017). The impact of different forms of cognitive scarcity on online privacy disclosure. Computers in human behavior, 73, 238-246.

[33] Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. Current opinion in psychology, 31, 105-109.

[34] Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., & Cranor, L. F. (2011, July). " I regretted the minute I pressed share" a qualitative study of regrets on Facebook. In Proceedings of the seventh symposium on usable privacy and security (pp. 1-16).

[35] Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for Human Future at the New Frontier of Power. London: Profile Books, ISBN 978-1-7881-6316-3