Unit 1 Collaborative Discussion 1

Peer Responses

Contents

Response to Shan Swanlow

Hi Shan,

I liked the hypothetical case study described above that highlights the fine balance between doing what is right and laws that restrict those right acts. For instance, the post states it was negligent not to inform affected e-commerce stores so they could prepare and backup their data. On the one hand, it seems reasonable that the worm's authors should have informed the affected stores (principles 1.2 and 1.3 -- honest and trustworthy). On the other hand, using the technique of a software worm is questionable. Perhaps, an alternate approach would have been to impose a financial fine or takedown notice. Despite this, do you think web hosting services have a role in preventing the upload of any malicious code (principle 3.1)?

Response to Gennaro Coppola

Hi Gennaro,

I found the recommendation to encourage employees to report abusive incidents and implement reviews for positive outcomes a good point. According to Flesichman et al. (2019), management are pivotal in reinforcing ethics within organisations. One way they can strengthen ethics is (as mentioned) via incentives and goals. They consider that establishing morals improves employee loyalty and dedication, fosters transparent business relationships and reduces capital costs.

These are positive aspects, however, do you think the term "abusive" may be too vague a word, and any ethics guidelines should be specific regarding what is classified as "abuse"? I ask this while considering the human impact to managers who may suffer complaints of being abusive when their words or actions were not intended as such; and likewise, some employees may be vengeful or (in contrast) socially awkward and, in both cases, misclassify organisation behaviour as abusive.

References

Fleischman, G.M., Johnson, E.N., Walker, K.B. & Valentine, S.R. (2019). Ethics versus outcomes: Managerial responses to incentive-driven and goal-induced employee behavior. Journal of Business Ethics, 158(4):951-967.

Response to Doug Leece

Hi Doug,

In reference to your statement "Some large technology firms have consistently shown they are willingly pay fines rather than refine their product to align with regulations and ethical expectations (Braun, 2022)", what do you consider the driving reasons behind these actions? If these companies fail to abide by some level of ethical expectations, could it be laying a precedent for other organisations to emulate such behaviour?

Response to Hendrik van Rooyen

Hi Hendrik,

Your post mentions that IT professionals are responsible for guiding clients to make better decisions. Suppose a "better decision" does not close a sale or causes the customer to choose cheaper options. Do you think this ultimately has negative consequences for an organisation's financial position? Suppose organisations decide to use dark UX patterns. In that case, it seems they take advantage of human behaviour and psychology (Gray et al., 2018) to direct users into decisions that are not in their best interest. Given the post's recommendation to guide clients, I am interested in exploring your thoughts on how IT professionals balance organisations' (legitimate) needs versus taking advantage of human-computer interactions.

References

Gray, C.M., Kou, Y., Battles, B., Hoggatt, J. & Toombs, A.L. (2018). The dark (patterns) side of UX design. Proceedings of the 2018 CHI conference on human factors in computing systems: 1-14.

Response from Tutor (Steph Paladini)

Hello Michael,

thank you for this.

Quite interestingly, I had advised the reading of this specific case to one of your colleagues here, because I found it really worth a reading or two.

Good analysis here, well handled.

Best wishes,

Steph

Response from Hendrik van Rooyen

Hi Michael,

Thank you for your insightful post. I just wanted to touch on your example “intentionally confusing visual prompts with loaded questions that end with acceptance as default” in regards to consent banners employed by website owners.

According to Nouwens et al. (2020), Consent Management Platforms (CMPs) are third-party services being employed by website owners to “outsource regulatory compliance”. Obviously with the rise of such services, competing platforms need to have a reason for organisations to use them and thus have to find that competitive advantage. An example of getting more users to give consent (not exclusive to CMPs) is shown in a study by Machuletz. & Böhme (2019), where they revealed that having a “Select all” option often nudged the user in giving consent where Nouwens et al. (2020) recorded a 22-23% decrease in consent with a “Reject all” option. Another study by Soe et al. (2020) found that 99% of their sample size of consent notices used some sort of dark design pattern to elicit consent.

The ethical obligations of computing professionals go beyond complying with laws or regulations as laws are often behind technology or techniques applied (Loui & Miller, 2008). However, Bazerman & Tenbrunsel (2011) makes the argument that in many situations individuals will not make the ethical judgement in their decision-making process, even if they have received training.

Fortunately, it does seem that dark patterns are being taken more seriously as the European Data Protection Board have recently published a draft containing guidelines on how to avoid dark patterns and by extension, avoid attracting the attention of European privacy authorities (EDPB, 2022).

References

Nouwens, M., Liccardi, I., Veale, M., Karger, D. and Kagal, L. (2020) ‘Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence’, In Proceedings of the 2020 CHI conference on human factors in computing systems. 13 April. 1-13.

Machuletz, D. and Böhme, R. (2019) ‘Multiple purposes, multiple problems: A user study of consent dialogs after GDPR’, Proceedings on Privacy Enhancing Technologies. 481-498.

Soe, T.H., Nordberg, O.E., Guribye, F. and Slavkovik, M. (2020) ‘Circumvention by design-dark patterns in cookie consent for online news outlets’, In Proceedings of the 11th nordic conference on human-computer interaction: Shaping experiences, shaping society. 26 October. 1-12.

Loui, M.C. & Miller, K.W. (2008) Ethics and professional responsibility in computing. Wiley.

Bazerman, M.H. & Tenbrunsel, A.E. (2011) Blind spots. In Blind Spots. Princeton University Press.

EDPB. (2022) Dark patterns in social media platform interfaces: How to

recognise and avoid them. Available from: https://edpb.europa.eu/system/files/2022-03/edpb_03-2022_guidelines_on_dark_patterns_in_social_media_platform_interfaces_en.pdf [Accessed 26 June 2022].

Response to Hendrik van Rooyen

Hi Hendrik,

Thank you for your valuable contributions. I enjoyed exploring the information about Consent Management Platforms (CMP) and the interesting research by Machuletz and Böhme (2019) and Nouwens et al. (2020). I found the statement of Nouwens et al. intriguing that adding a "Reject All" option results in a 22-23% reduction in consent--a figure that might grow as more users realise the monetisation value of their data. I thought it was interesting that, according to Abrardi and Hoernig (2021), consent policies are generally favourable if they are not overly burdensome or restrict disclosure. However, consent pop-ups designed to induce full disclosure acceptance have adverse effects.

So, given the role of CMPs (whose use is likely to be mandated by management), I would love to read your thoughts on what computing professionals can do in applying CMPs and ethical guidelines—knowing that most users fail to make correct judgements.

Could it be that perhaps operating models based on monetisation of user data is inherently flawed? CMPs seem to be prolific on the web, and--in light of the ever-shrinking sense of privacy in today's society--users may consider automatic consent via pop-ups as normal.

References

Abrardi, L., Cambini, C. & Hoernig, S. (2021). "I don't care about cookies!" Platform Data Disclosure and Time-Inconsistent Users.

Nouwens, M., Liccardi, I., Veale, M., Karger, D. and Kagal, L. (2020) 'Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence', In Proceedings of the 2020 CHI conference on human factors in computing systems. 13 April. 1-13

Response from Alice Villar

Hi Michael,

Thank you for your engaging and well-researched post. I chose the same topic and have few observations to make about challenges in the push to regulate dark patterns.

Recently, the increasing use of dark patterns has caught the attention of state and federal regulators. Lawmakers and regulators are starting to address the use of dark patterns directly, focusing on how user interfaces are designed and their impact on consumer consent. Hartzog (2018), professor of law and computer science at Northeastern University, argues in his book "Privacy's Blueprint" the way user interfaces are designed plays a key role in eroding a user’s privacy. He writes privacy laws need to take into consideration how big of a role design play in privacy, noting privacy laws should “be careful to broach design in a way that is flexible and not unduly constraining” while also setting “boundaries and goals for technological design.”

While regulation of dark patterns is expected, we find ourselves at a new frontier in regulation due to the recent proliferation of dark patterns that has, to date, largely been unregulated, especially with respect to inadvertent or unintentional use of dark patterns. The proliferation of dark patterns will likely be accelerated through the use of machine learning and automation technology, which will iterate through automated testing and with little to no human intervention. Businesses that measure their success through user

acquisition or engagement should carefully consider if their products are designed in a manipulative manner that would be considered dark patterns by regulators. (Zhu, 2021)

REFERENCES:

Hartzog, W. (2018). PrivacyÕs Blueprint: The Battle to Control the Design of New Technologies. Harvard University Press.

Zhu, C (2021) Dark patterns — a new frontier in privacy regulation. Reuters. Available from: https://www.reuters.com/legal/legalindustry/dark-patterns-new-frontier-privacy-regulation-2021-07-29/

Response to Alice Villar

Hi Alice,

Thank you for the informative response, especially the reference to the use of machine learning and automated testing; there exists no reason why organisations (lacking sufficient regulation) would not seek to use this approach. Another good point raised relates to the reference by Zhu (2021) and the need to consider the (hidden) impact of such patterns programmed into the product. This adds another good point for consideration that such patterns, driven by user interface design, are on the whole, ungoverned.

Egberts (2021) writes, in their thesis on regulating dark patterns, that the need for regulating arises because of "inefficient allocation of resources", the need for users to protect themselves against "slugging", and self-regulation within the industry shows no noticeable effect in reducing their use. Unfortunately, additional regulation is necessary because, as Sibony (2014, pp. 922-926) points out, the European consumer model assumes consumers are reasonably well-informed and relies on the assumption that individuals generally act rationally.

References

Egberts, A. (2021). Manipulation through Design: A Law and Economics Analysis of EU Dark Patterns Regulation.

Sibony, A.-L. (2014). Can EU Consumer Law Benefit from Behavioural Insights? An Analysis of the Unfair Practices Directive. European Review of Private Law, 22(6):901-942.