

Initial Post

The Association for Computing Machinery (ACM) released a case study where Stewart's team knowingly made changes, based on a client request, that made it confusing to exit a page on the client's website. Where your two options looked to be to exit the page or accept a product. Clients were actually either accepting a contract for a default product or upgrading the client to a more expensive product. Where clients would also accept a protection warranty without any prompts asking for confirmation. Stewart was invited to a celebration the client was hosting shortly after the changes Stewart's team made. There he found out the client was well aware of the situation and the client purposefully made these changes to rather deal with the clients who noticed and complained the new debit orders, as it seems to have outweighed the clients who did not.

This is known as dark user experience (UX) patterns. These are tactics that are intended to trick clients into harm. In this case, tricking clients into accepting products they were not aware of for company financial gains. Though the client had requested to make these changes, Stewart's team had failed their baseline professionalism to uphold morals and use their knowledge to benefit users and not trick them. (Association for Computing Machinery, N.D.) Stewart's team and no concern for public interest and failed to follow principles of having regards for the wellbeing of others as per the British Computer Society (British Computer Society, N.D.) code of conduct. (ref)

Dark UX patterns can be against the law. As discussed in (ref) European law prohibits designing nudging tactics that can benefit website operators. So, Stewart, his team and the client stakeholders could have breached the law using these tactics (ref)

Ethically, if the client had a great business with great products and Stewart and his team used their skill and knowledge to build an engaging and understandable website. The client's company could have seen profit margins without breaching law or morals. More people need to know about IT law and understand where the line is drawn so society is able to fight back whenever they are caught in these situations. Better, if government or institutions had the funds or were rewarded for finding law breaking companies then society would benefit further from having less chances of being caught in these situations.

References

Association for Computing Machinery. N.D. ACM Code of Ethics and Professional Conduct. Available from: <https://www.acm.org/code-of-ethics/case-studies/dark-ux-patterns> [Accessed 2 August 2025]

British Computer Society. N.D. BCS Code of Conduct. Available from: <https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct> [Accessed 2 August 2025]

Nelissen, L.G.M., Funk M. (2022) Rationalizing Dark Patterns: Examining the Process of Designing Privacy UX Through Speculative Enactments. Available from: <https://research.tue.nl/en/publications/rationalizing-dark-patterns-examining-the-process-of-designing-pr> [Accessed 2 August 2025]

Gray, C.M. et al. (2021) Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. Available from: <https://dl.acm.org/doi/abs/10.1145/3411764.3445779> [Accessed 2 August 2025]

Feedback

Hi Matthew,

I enjoyed reading your post and, adding to your points regarding broken codes of conduct/ethics, I also think that the company's actions - and Stewart's subsequent inaction - breached the following principles of the BCS Code of Conduct (BCS, 2024):

1. Public Interest

You shall:

- a. have due regard for public health, privacy, security and wellbeing of others and the environment.
- b. have due regard for the legitimate rights of Third Parties.
- c. conduct your professional activities without discrimination on the grounds of sex, sexual orientation, marital status, nationality, colour, race, ethnic origin, religion, age or disability, or of any other condition or requirement.

2. Duty to Relevant Authority

You shall:

- c. accept your personal duty to uphold the reputation of the profession and not take any action which could bring the profession into disrepute.

4. Duty to the Profession

- a. accept your personal duty to uphold the reputation of the profession and not take any action which could bring the profession into disrepute. Seek to improve professional standards through participation in their development, use and enforcement.
- c. uphold the reputation and good standing of BCS, The Chartered Institute for IT.
- d. act with integrity and respect in your professional relationships with all members of BCS and with members of other professions with whom you work in a professional capacity.

Although I broadly agree with your suggestion that more needs to be done to expose dark UX patterns, I believe that offering monetary rewards for uncovering and reporting these could lead to unintended consequences such as cyber criminals hacking code to make existing websites display these patterns, before reporting and claiming the money for themselves. My suggestion would be to look to utilising AI within a tool that could automatically scan sites to detect such patterns.

References

BCS. (2024) BCS Code of Conduct. British Computer Society. Available at: <https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct> (Accessed: 04 August 2025).

Hi Matthew,

Good job with your research. I agree that the example clearly illustrates how dark UX patterns can breach both ethical and legal standards. You explained well how these tactics conflict with professional responsibilities, and the link to the BCS Code of Conduct is appropriate. I particularly agree with your point that profit should not outweigh user wellbeing, and that public awareness of IT law is essential. You could strengthen your argument by directly naming the specific clauses in the BCS Code of Conduct that were violated, as this would make your case even more compelling.

What I learnt:

- I learned that when discussing professional codes like the BCS Code of Conduct, it's not enough to just say they were "broken." Naming the exact clauses (Public Interest, Duty to Relevant Authority, Duty to the Profession) makes the analysis more accurate and convincing.
- I realised my suggestion about rewarding people to expose dark UX patterns could backfire. My peers showed me how it could be exploited, and that using AI tools to automatically detect these practices is a better long-term solution.
- I also saw the importance of balance in ethical analysis: profit can never outweigh user wellbeing, and pointing this out clearly strengthens the argument.
- Finally, I learned that presenting my analysis with clarity and detail—like giving enough context about Stewart's case before diving into the ethics—helps readers follow my reasoning better and shows stronger professionalism.

Summary post:

The Association for Computing Machinery (ACM) released a case study where Stewart's team knowingly implemented client-requested design changes that created a misleading user journey. The altered interface presented two options that appeared to allow users to either exit the page or accept a product. In reality, both options locked users into either a default product contract, an upgrade, or even a protection warranty without clear prompts for consent. At a subsequent client celebration, Stewart discovered the client was fully aware of these tactics and had deliberately chosen to prioritise short-term profit by only responding to those customers who noticed and complained about unexpected debit orders (ACM, n.d.).

This design is an example of dark user experience (UX) patterns—intentional design practices that deceive or manipulate users into choices they might not otherwise make (Nelissen & Funk, 2022). Stewart's team failed in their duty of professionalism by prioritising client profit over ethical obligations to users. According to the ACM Code of Ethics, computing professionals should avoid harm and contribute positively to society, yet here they actively undermined user trust (ACM, n.d.).

When assessed against the British Computer Society (BCS) Code of Conduct, several breaches are clear. Under Section 1: Public Interest, the team did not “have due regard for public health, privacy, security and wellbeing of others” or for “the legitimate rights of Third Parties” (BCS, 2024). Their actions also violated Section 2: Duty to Relevant Authority, which requires members to uphold the profession's reputation and avoid conduct that could bring it into disrepute. Finally, Section 4: Duty to the Profession was breached, as the team failed to act with integrity, nor did they seek to improve or uphold professional standards. Explicitly naming these clauses highlights the depth of misconduct (BCS, 2024).

Dark UX patterns may also carry legal consequences. European legislation, for instance, prohibits manipulative “nudging” tactics that undermine valid consent (Gray et al., 2021). By deploying such deceptive interfaces, Stewart, his team, and the client risked breaching these requirements, exposing themselves to regulatory and reputational harm.

Instead of resorting to harmful patterns, professionals could have leveraged their expertise to design an engaging, transparent website that promoted genuine uptake of the client's products. As I suggested, society needs more awareness of IT law, but building on feedback, monetary incentives for whistleblowing may not be the best approach. They could unintentionally encourage malicious actors to introduce dark patterns in order to report them. A more sustainable solution would be deploying AI-driven tools to automatically detect manipulative design patterns across websites.

Ultimately, this case reinforces that professionalism in computing requires resisting harmful client demands, even at the cost of business. By embedding ethical practice, professionals protect both society and the long-term trust essential for sustainable technological development.

References

Association for Computing Machinery. (n.d.) ACM Code of Ethics and Professional Conduct. Available from: <https://www.acm.org/code-of-ethics/case-studies/dark-ux-patterns> [Accessed 2 August 2025].

BCS. (2024) BCS Code of Conduct. British Computer Society. Available from: <https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct> [Accessed 04 August 2025].

Nelissen, L.G.M., & Funk, M. (2022) Rationalizing Dark Patterns: Examining the Process of Designing Privacy UX Through Speculative Enactments. Available from: <https://research.tue.nl/en/publications/rationalizing-dark-patterns-examining-the-process-of-designing-pr> [Accessed 2 August 2025].

Gray, C.M. et al. (2021) Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective. Available from: <https://dl.acm.org/doi/abs/10.1145/3411764.3445779> [Accessed 2 August 2025].