# BIG TECH AND DARK PATTERNS: HOW COMPANIES MANIPULATE PRIVACY CHOICES

J Jerusha Devanesam, Vellore Institute of Technology University, Chennai

## ABSTRACT

In today's digital world, personal data has become a highly valuable asset, forming the backbone of the business models of leading technology companies. While data collection is often presented as necessary for delivering personalized services, many corporations rely on "dark patterns" that are design strategies that subtly push users into disclosing more personal information than they might otherwise choose. These tactics, embedded in interfaces, privacy settings, and consent flows, exploit cognitive biases and a lack of clarity, ultimately weakening informed consent and undermining the right to privacy. This paper explores the prevalence and impact of dark patterns used by Big Tech, showing how such practices clash with both legal and ethical principles of data protection. Through case studies it examines how privacy options are often obscured, default settings are biased toward maximum data collection, and opting out is made unnecessarily difficult.

The discussion places dark patterns within the context of global privacy regulations, including the GDPR and India's Digital Personal Data Protection Act of 2023, while also examining regulatory challenges in enforcing these standards. It critically assesses how effective these regulations have been in limiting manipulative design practices. The study investigates how corporations exploit user vulnerabilities and the extent to which regulation can protect digital privacy. It concludes that while legal frameworks provide an essential safeguard, stronger enforcement, greater user awareness, and the adoption of ethical design principles are necessary to counter dark patterns and ensure privacy remains a meaningful and enforceable right in the digital ecosystem.

**Keywords:** Dark Patterns, Data Protection, Digital Privacy, Informed Consent, Personal Data, User Autonomy

## Objective of the study

The purpose of this study is to explore how major technology companies use dark patterns to influence the choices people make about their privacy. It looks at how these tactics affect user autonomy and examines whether modern data protection laws are doing enough to stop them.

## Learning Outcomes:

1. Readers will be able to recognize and understand the different forms of dark patterns used by technology companies and how these designs manipulate user behaviour.

2. Readers will be able to critically evaluate how effective laws like the GDPR and India's Digital Personal Data Protection Act of 2023 are in limiting manipulative design practices and promoting ethical online experiences.

## Research Questions

1. How do Big Tech companies use dark patterns to influence the way users give consent or share personal data?

2. How well do existing data protection laws prevent or control manipulative design practices that threaten privacy?

## Introduction

In today's digital world, personal data has become the fuel that drives the global economy. Every click, search, and scroll creates valuable information that powers the business models of companies like Google, Meta, and Amazon. These companies claim that collecting data helps them provide better, more personalized services. But behind this promise of convenience lies a system that quietly gathers far more data than most users realize or truly consent to share (Zuboff, 2019).

The digital environment we inhabit is not neutral. Every feature, from pop-up notifications to privacy prompts, is carefully designed to guide behavior. The interfaces we interact with are built to encourage constant engagement, maximize clicks, and collect as much data as possible. What appears to be a simple "yes" or "accept" button is often the outcome of deep behavioural research aimed at shaping user decisions. This silent form of manipulation has become an invisible layer of the internet's infrastructure, blurring the boundaries between free choice and engineered behaviour.

A key part of this system is the use of **dark patterns**. These are not accidents or innocent design choices but they are intentional strategies that make it easier for users to say "yes" to data collection and harder to say "no" (Brignull, 2011). Through misleading buttons, confusing menus, and emotional wording, users are subtly guided toward decisions that benefit the platform rather than themselves.

The issue of dark patterns isn't just technical, it's deeply ethical and legal. It raises tricky questions about free will, consent, and whether people can truly control their information in an online world built to undermine that control. As governments race to regulate Big Tech, the tug-of-war between innovation, profit, and privacy grows stronger.

## Understanding Dark Patterns

The term "dark patterns" describe design features that "trick users into doing things they might not otherwise do" (Brignull, 2011). Instead of helping people make informed decisions, these designs exploit human psychology especially the tendency to choose the easiest or fastest option (Mathur, et al., 2019). Some common examples include:

- **Privacy Zuckering:** pushing users to share more data than they intended.
- **Forced Continuity:** making it nearly impossible to cancel a subscription or delete an account.
- **Hidden Costs:** revealing extra fees or permissions only at the last step.
- **Confirm shaming:** using guilt-inducing language like "No thanks, I don't care about security."
- **Obstruction:** burying the opt-out process under layers of confusing steps.

These tactics rely on people's natural desire for simplicity. Most users do not read long privacy policies or navigate complex settings. In one study, researchers estimated that reading the privacy policies for every website a person visits in a year would take over 70 hours (McDonald

& Cranor, 2008). When faced with a maze of options, many simply click "accept" to move on and companies design interfaces knowing this.

Dark patterns are built on behavioural science principles such as the "nudge." A nudge is a small push that influences behaviour without removing freedom of choice (Thaler & Sunstein, 2008). In theory, nudges can be helpful like encouraging people to save for retirement. But when used deceptively, they become manipulative. People operate under what psychologists call "bounded rationality" in the online sphere where they make decisions with limited time, attention, and understanding. Companies exploit this by presenting privacy options that are too complicated to evaluate, knowing that users will often take the path of least resistance (Susser, Roessler, & Nissenbaum, 2019). Consent, in this sense, becomes a performance rather than a real choice.

**Big Tech and the Data Economy**

In the modern economy, data is often described as the new oil. It fuels targeted advertising, predictive analytics, and the algorithms that shape what we see online (Zuboff, 2019). For companies like Meta, Google, and Amazon, collecting and analyzing user data is central to how they make money. The more data they gather, the more precisely they can target ads and personalize content and the more valuable their platforms become. This economic incentive creates a powerful motivation to keep users sharing data, willingly or not. Dark patterns serve as the invisible tools that make this constant flow of information possible (Mathur, et al., 2019).

One of the most well-known examples of data misuse was the ***Cambridge Analytica scandal***, where Facebook users unknowingly shared personal information that was later used to influence political campaigns. The interface made it easy to give broad permissions without realizing how much data was being accessed not only from individual users but also from their friends (Isaak & Hanna, 2018). Google has faced similar criticism. In 2018, an investigation by the Associated Press revealed that disabling "Location History" did not fully stop Google from tracking users. They had to disable another option, "Web & App Activity," buried deep in the settings (Associated Press, 2018). This is a classic example of obstruction, where design complexity makes opting out nearly impossible.

***Amazon's Prime cancellation process*** offers another example. A 2021 report by the Norwegian Consumer Council found that users trying to unsubscribe faced multiple confirmation screens and emotional messages designed to make them reconsider (Forbrukerrådet, 2021). The experience feels intentionally exhausting, encouraging users to give up before completing the process. These examples show that dark patterns are not rare mistakes rather they are systemic features of how digital platforms are built to maximize engagement and data collection. ***Instagram's account deletion process*** also demonstrates how platforms intentionally complicate user exits. Instead of offering a simple "delete account" button within the app, users are redirected through multiple steps on an external website, discouraging them from completing the process (Narayanan, Mathur, Chetty, & Kshirsagar, 2020). This "friction by design" approach shows how companies prioritize retention over respect for choice.

Another striking case involves ***TikTok***, whose privacy settings have drawn criticism for nudging young users toward public profiles and exposing personal information by default. Investigations by European consumer groups found that TikTok's design made it easier to accept permissive privacy settings than to restrict data sharing (Forbrukerrådet, 2021). This example highlights how dark patterns can exploit not just convenience but also inexperience, especially among minors. ***LinkedIn's onboarding process*** offers another example. New users are encouraged to "connect with their contacts," but the platform often imports entire address books by default, sending invitations without explicit consent. This design blurs the line between convenience and exploitation, illustrating how social media platforms turn personal networks into data assets (Narayanan, Mathur, Chetty, & Kshirsagar, 2020).

Even operating systems have been implicated in dark pattern design. ***Microsoft's Windows 10 installation process*** once pushed users toward "Express Settings," which automatically enabled broad data sharing. Custom privacy controls existed but were deeply buried, demonstrating how even infrastructure-level software can nudge users toward surveillance-friendly defaults.

## Legal and Ethical Frameworks

Europe's General Data Protection Regulation (GDPR) sets one of the strongest global standards for privacy. It defines consent as something that must be freely given, specific, informed, and unambiguous. In other words, people should know exactly what they're agreeing to, and they should have a genuine choice. However, dark patterns directly challenge this idea. When privacy options are hidden or confusing, consent loses its meaning. However, in practice, many companies still rely on misleading design to nudge users toward consent. For example, popups that highlight the "Accept All" button in bright colours while hiding the "Reject" option in grey violate the spirit of the law (Mathur, et al., 2019).

Even though the GDPR allows regulators to fine companies for such behaviour, enforcement remains a major challenge. The Irish Data Protection Commission, responsible for many major tech firms headquartered in Dublin, has been criticized for slow responses and limited action (Ryan, 2021). In practice, this means that the power imbalance between Big Tech and users often remains unchanged. The *Bundeskartellamt v. Facebook* case (Bundeskartellamt v. Facebook , 2019) in Germany demonstrated how competition law and privacy law can overlap: Facebook was accused of abusing its market dominance by forcing users to consent to excessive data collection. This case highlighted how dark patterns can be not only unethical but also anti-competitive.

India's Digital Personal Data Protection (DPDP) Act, passed in 2023, mirrors some ideas from the GDPR but adapts them for India's growing digital ecosystem (Dharod & Tauro, 2025). It promises that consent must be "free, specific, informed, unconditional, and unambiguous." The Act also establishes the Data Protection Board to oversee compliance. However, critics argue that the law gives too much discretion to the government through broad "legitimate use" exemptions. The Act also fails to address interface-level manipulation. This omission means that companies could still use deceptive design to obtain consent as long as they meet minimal legal formalities. Without explicit provisions targeting dark patterns, enforcement risks becoming a box-ticking exercise rather than a meaningful protection for users.

India's digital economy adds complexity because millions of new users are coming online through affordable smartphones and low-cost data. Many lack the literacy to understand privacy policies or manipulative design, making them especially vulnerable. This creates an urgent need for context-sensitive enforcement that accounts for unequal access to digital knowledge.

The ethical debate around dark patterns centers on autonomy and fairness. From a rights-based perspective, individuals have the moral right to control their own information. From a moral standpoint, it violates the principle of treating individuals as ends in themselves rather than as means to a corporate objective (Susser, Roessler, & Nissenbaum, 2019). Ethical design demands that technology respect the user's right to make decisions without deception or pressure. When companies design systems that subtly trick users, they treat people not as individuals with rights but as data sources to be exploited. This kind of manipulation doesn't just erode privacy but it damages trust. People begin to feel that the digital world is rigged against them, that every "choice" online is really a trap. In the long run, this weakens both the moral legitimacy of technology companies and public confidence in digital systems.

## Challenges in Regulation and Enforcement

Regulating dark patterns is difficult because technology companies operate across borders. Data often flows through multiple countries at once, making it hard to determine which laws apply. This fragmentation allows corporations to forum shop, i.e., to base their operations in countries with weaker or slower enforcement mechanisms (Narayanan, Mathur, Chetty, & Kshirsagar, 2020). Another major challenge is proving intent. Dark patterns are often subtle and disguised as user-friendly design. Regulators need technical expertise to recognize these patterns and demonstrate that they were deliberately deceptive (Mathur, et al., 2019).

Unfortunately, many data protection agencies lack the resources to conduct such detailed audits. Civil society organizations such as the Norwegian Consumer Council and the Electronic Frontier Foundation have been instrumental in exposing deceptive design practices. Their investigations have sparked public debate and, in some cases, legal reform. However, user awareness remains low. Without better education and digital literacy, most people remain vulnerable to the same manipulative tactics that have been used for over a decade (Cavoukian, 2011).

## Way Forward

A promising approach is "Privacy by Design" developed by privacy expert Ann Cavoukian. This principle argues that privacy protection should be built into a system from the ground up, not added as an afterthought (Cavoukian, 2011). Ethical design prioritizes clarity, fairness, and simplicity. Instead of hiding options, companies could present choices in plain language, ensuring that "decline" options are just as easy to find as "accept". Legal systems must evolve to keep pace with technology. Some recent laws, like California's Consumer Privacy Rights Act, explicitly ban manipulative design practices that "subvert or impair user choice." By including similar provisions in other countries' data laws would make it easier to hold companies accountable.

Transparency is essential. Companies should be required to publish privacy transparency reports that explain how their consent systems work and what data they collect. Independent audits could evaluate whether their designs respect privacy or exploit users. This would not only protect consumers but also help rebuild public trust. Ultimately, technology is only as ethical as the people who use and design it. People need to understand how digital systems work and how their choices are being shaped. Teaching digital literacy and promoting public awareness campaigns can empower users to recognize manipulative design and make informed decisions.

At the same time, addressing dark patterns cannot rest on any single actor. Governments, corporations, designers, and users must work together to establish an ecosystem of ethical accountability. Regulators should consult with behavioural scientists and UX experts to anticipate new manipulative tactics, while design teams should adopt internal ethical review boards similar to those used in medical or academic research. This collaborative approach can shift the focus of digital innovation from maximizing attention and data collection to promoting trust, transparency, and human well-being.

## Conclusion

Dark patterns represent one of the most pressing challenges in today's digital age. They blur the line between persuasion and deception, turning user consent into a formality rather than a choice. Behind their clean interfaces, many Big Tech companies have created systems designed to collect data first and ask questions later. Legal frameworks like the GDPR and India's DPDP Act mark important steps toward greater accountability, but laws alone cannot solve the problem. Enforcement remains slow and fragmented, while manipulative design continues to evolve faster than regulation can keep up.

A sustainable solution requires a holistic approach by combining stronger regulation, ethical design principles, corporate transparency, and public awareness. Privacy should not be treated as a checkbox on a website but as a fundamental human right embedded in the digital experience. If companies and policymakers embrace this vision, technology can move beyond manipulation and become what it was meant to be, i.e., a tool for empowerment, not exploitation.