A dark pattern (also known as a "deceptive design pattern") is "a user interface that has been carefully crafted to trick users into doing things, such as buying overpriced insurance with their purchase or signing up for recurring bills".[1][2][3] User experience designer Harry Brignull coined the neologism on 28 July 2010 with the registration of darkpatterns.org, a "pattern library with the specific goal of naming and shaming deceptive user interfaces".[4][5][6]

In 2021 the Electronic Frontier Foundation and Consumer Reports created a tip line to collect information about dark patterns from the public.[7]

Patterns Privacy Zuckering "Privacy Zuckering" – named after Facebook co-founder and Meta Platforms CEO Mark Zuckerberg – is a practice that tricks the user into sharing more information than they intended to.[8] Users may give up this information unknowingly or through practices that obscure or delay the option to opt out of sharing their private information.

California has approved regulations that limit this practice by businesses in the California Consumer Privacy Act.[9]

Bait-and-switch Bait-and-switch patterns advertise a free (or at a greatly reduced price) product or service that is wholly unavailable or stocked in small quantities. After announcing the product's unavailability, the page presents similar products of higher prices or lesser quality.[10][11]

Confirmshaming Confirmshaming uses shame to drive users to act. For example, when websites word an option to decline an email newsletter in a way that shames visitors into accepting.[11][12]

Misdirection Common in software installers, misdirection presents the user with a button in the fashion of a typical continuation button. A dark pattern would show a prominent "I accept these terms" button asking the user to accept the terms of a program unrelated to the one they are trying to install.[13] Since the user typically will accept the terms by force of habit, the unrelated program can subsequently be installed. The installer's authors do this because the authors of the unrelated program pay for each installation that they procure. The alternative route in the installer, allowing the user to skip installing the unrelated program, is much less prominently displayed,[14] or seems counter-intuitive (such as declining the terms of service).

Some websites that ask for information that is not required also use misdirection. For example, one would fill out a username and password on one page, and after clicking the "next" button, the page asks the user for their email address with another "next" button as the only option.[15] This hides the option to press "next" without entering the information. In some cases, the page shows the method to skip the step as a small, greyed-out link instead of a button, so it does not stand out to the user.[16] Other examples include sites offering a way to invite friends by entering their email address, to upload a profile picture, or to identify interests.

Confusing wording may be also used to trick users into formally accepting an

option which they believe has the opposite meaning. For example a personal data processing consent button using a double-negative such as "don't not sell my personal information"[17]

Roach motel A roach motel or a trammel net design provides an easy or straightforward path to get in but a difficult path to get out.[18] Examples include businesses that require subscribers to print and mail their opt-out or cancellation request.[10][11]

For example, during the 2020 United States presidential election, Donald Trump's WinRed campaign employed a similar dark pattern, pushing users towards committing to a recurring monthly donation.[19]

In 2021, in the United States, the Federal Trade Commission (FTC) has announced they will ramp up enforcement against dark patterns like roach motel that trick consumers into signing up for subscriptions or making it difficult to cancel. The FTC has stated key requirements related to information transparency and clarity, express informed consent, and simple and easy cancellation.[20]

Research In 2016 and 2017 research has documented social media anti-privacy practices using dark patterns.[21][22] In 2018 the Norwegian Consumer Council (Forbrukerrådet) published "Deceived by Design," a report on deceptive user interface designs of Facebook, Google and Microsoft.[23] A 2019 study investigated practices on 11,000 shopping web sites. It identified 1818 dark patterns total and grouped them into 15 categories.[24]

Research from April 2022 found that dark patterns are still commonly used in the marketplace, highlighting a need for further scrutiny of such practices by the public, researchers and regulators.[25]

Under the European Union General Data Protection Regulation (GDPR), all companies must obtain unambiguous, freely-given consent from customers before they collect and use ("process") their personally identifiable information. A 2020 study found that "big tech" companies often used deceptive user interfaces in order to discourage their users from opting out.[26] In 2022 a report by the European Commission found that "97% of the most popular websites and apps used by EU consumers deployed at least one dark pattern."[27]

Research on advertising network documentation shows that information presented to mobile app developers on these platforms is focused on complying with legal regulations, and puts the responsibility for such decisions on the developer. Also, sample code and settings often have privacy-unfriendly defaults laced with dark patterns to nudge developers' decisions towards privacy-unfriendly options such as sharing sensitive data to increase revenue.[28]

Legality United States Bait-and-switch is a form of fraud that violates US law.[29]

On 9 April 2019, US senators Deb Fischer and Mark Warner introduced the

Deceptive Experiences To Online Users Reduction (DETOUR) Act, which would make it illegal for companies with more than 100 million monthly active users to use dark patterns when seeking consent to use their personal information.[30]

In March 2021, California adopted amendments to the California Consumer Privacy Act, which prohibits the use of deceptive user interfaces that have "the substantial effect of subverting or impairing a consumer's choice to opt-out."[17]

In October 2021, the Federal Trade Commission issued an enforcement policy statement, announcing a crackdown on businesses using dark patterns that "trick or trap consumers into subscription services." As a result of rising numbers of complaints, the agency is responding by enforcing these consumer protection laws.[20]

In 2022, New York Attorney General Letitia James fined Fareportal $2.6 million for using deceptive marketing tactics to sell airline tickets and hotel rooms[31] and the Federal Court of Australia fined Expedia Group's Trivago A$44.7 million for misleading consumers into paying higher prices for hotel room bookings.[32]

In March 2023, the United States Federal Trade Commission fined Fortnite developer Epic Games $245 million for use of "dark patterns to trick users into making purchases." The $245 million will be used to refund affected customers and is the largest refund amount ever issued by the FTC in a gaming case.[33]

European Union In the European Union, the GDPR requires that a user's informed consent to processing of their personal information be unambiguous, freely-given, and specific to each usage of personal information. This is intended to prevent attempts to have users unknowingly accept all data processing by default (which violates the regulation).[34][35][36][37][38]

According to the European Data Protection Board, the "principle of fair processing laid down in Article 5 (1) (a) GDPR serves as a starting point to assess whether a design pattern actually constitutes a 'dark pattern'."[39]

At the end of 2023 the final version of the Data Act[40] was adopted. It is one of the three EU legislations which deal expressly with dark patterns.[41] The other one being the Digital Services Act.[42] The third EU legislation on dark patterns in force is the directive financial services contracts concluded at a distance.[43]

United Kingdom In April 2019, the UK Information Commissioner's Office (ICO) issued a proposed "age-appropriate design code" for the operations of social networking services when used by minors, which prohibits using "nudges" to draw users into options that have low privacy settings. This code would be enforceable under the Data Protection Act 2018.[44] It took effect 2 September 2020.[45][46]