

Mathias Sætersdal

Layered Trust Signals in E-Commerce Interfaces

A Comparative Analysis of Regulatory,
Institutional, and Interface-Level Trust
Construction

Graduate thesis in Interaction Design (MIXD)

Supervisor: Aliaksei Miniukovich

June 2026



Norwegian University of
Science and Technology

Mathias Sætersdal

Layered Trust Signals in E-Commerce Interfaces

A Comparative Analysis of Regulatory, Institutional,
and Interface-Level Trust Construction

Graduate thesis in Interaction Design (MIXD)
Supervisor: Aliaksei Miniukovich
June 2026

Norwegian University of Science and Technology
Faculty of Architecture and Design
Department of Design



Norwegian University of
Science and Technology

Preface

This thesis was written as part of the Master's programme in Interaction Design at the Norwegian University of Science and Technology (NTNU) in Trondheim. It examines how trust is constructed across three structural layers of e-commerce interfaces — regulatory, institutional, and interface-level — through a comparative analysis of Amazon, Temu, eBay, and Apple's online store.

My interest in this topic grew from a broader concern with how digital design shapes behaviour in ways that users rarely notice. Cookie consent interfaces, payment pages, and product pages are encountered constantly, yet the trust signals embedded in them are seldom made explicit. The gap between what the design communicates and what users actually process seemed worth investigating — not through user testing, but through close analytical attention to the design itself.

The thesis develops an original analytical framework, the Layered Trust Signals framework, and applies it consistently across four platforms. My aim throughout has been to produce a piece of work that is both theoretically grounded and practically useful for interaction designers working in digital commerce.

Trondheim, June 202

Acknowledgements

I would like to thank Aliaksei Miniukovich for the guidance and feedback throughout this project. Thanks also to everyone who read drafts, offered comments, or simply asked good questions along the way. I would also like to thank my family for their encouragement and support throughout the process.

Abstract

Trust underpins every act of online commerce. Because consumers cannot physically inspect or interact with the companies and the products themselves - though some retailers operate both online and physical stores, where the physical presence can strengthen trust - there has to be a level of trust created by those platforms. A lot of research exists on the topic of e-commerce trust, but the research exists in different fields and does not often cross over with other fields related to e-commerce trust. The way that trust is created within each of these levels has yet to be addressed by existing literature on the topic of e-commerce trust.

To address that gap, I developed the Layered Trust Signals framework - an analytical model that identifies three distinct levels at which trust is constructed in e-commerce interfaces. Layer 1 (Regulatory Trust) is about the regulatory and privacy context made visible through cookie consent design. Layer 2 (Institutional Trust) is about trust that's outsourced to recognised third parties - payment providers, certification bodies, reputation systems - whose authority transfers to the platform. Layer 3 (Interface-Level Trust) is about how trust gets built directly through visual design: aesthetic coherence, information hierarchy, prototypicality, and persuasive cues.

By integrating the theories of trust, signalling, institutional trust, and visual credibility into a unifying framework, the study can investigate the degree of trust that is present on the e-commerce websites of companies including Amazon, Temu, eBay, and Apple.

Each platform turns out to embody a different trust architecture, shaped by its commercial model, brand identity, and target users. The three layers don't operate independently either: a weakness in one layer can be offset by strengths in another, and tensions between layers produce identifiable patterns of trust asymmetry. I introduce the concept of trust compensation to describe these cross-layer dynamics and draw out what they mean for interaction design practice.

Rather than measuring user trust empirically, the focus here is on how trust is designed. It contributes a replicable analytical framework, a vocabulary for describing layered trust architectures, and practical insights for designers working in digital commerce.

Sammendrag

Tillit er grunnlaget for all netthandel. Fordi forbrukere ikke kan inspisere produkter eller samhandle fysisk med selskaper, må plattformene selv skape tillit. Det finnes mye forskning på tillit i e-handel, men den er spredt på tvers av fagfelt og kobler sjelden de ulike nivåene sammen. Hvordan tillit konstrueres på tvers av disse nivåene er derfor ikke tilstrekkelig behandlet i eksisterende litteratur.

For å adressere dette gapet har jeg utviklet rammeverket Layered Trust Signals — en analytisk modell som identifiserer tre nivåer der tillit konstrueres i e-handelsgrensesnitt. Lag 1 (regulatorisk tillit) handler om det regulatoriske og personvernmessige kontekst som gjøres synlig gjennom samtykkedesign for informasjonskapsler. Lag 2 (institusjonell tillit) handler om tillit som er satt ut til anerkjente tredjeparter — betalingsleverandører, sertifiseringsorganer og omdømmesystemer — hvis autoritet overføres til plattformen. Lag 3 (grensesnittbasert tillit) handler om hvordan tillit bygges direkte gjennom visuelt design: estetisk sammenheng, informasjonshierarki, prototypikalitet og overtalende virkemidler.

Ved å integrere teorier om tillit, signalteori, institusjonell tillit og visuell troverdighet i ett samlende rammeverk, undersøker studien hvordan tillit er designet på e-handelsplattformene til Amazon, Temu, eBay og Apple.

Hver plattform viser seg å ha en ulik tillitsarkitektur, formet av forretningsmodell, merkevareidentitet og målgruppe. De tre lagene opererer heller ikke uavhengig av hverandre: en svakhet i ett lag kan kompenseres av styrker i et annet, og spenninger mellom lagene skaper identifiserbare mønstre av tillitsasymmetri. Begrepet tillitskompensasjon introduseres for å beskrive disse dynamikkene på tvers av lag, og hva de betyr for interaksjonsdesignpraksis.

Fremfor å måle brukertillit empirisk er fokuset på hvordan tillit er designet. Oppgaven bidrar med et analytisk rammeverk som kan repliseres, et vokabular for å beskrive lagdelte tillitsarkitekturer, og praktiske innsikter for designere som arbeider innen digital handel.

Keywords: trust, e-commerce, interface design, dark patterns, cookie consent, signalling theory, visual credibility, interaction design, persuasive design, comparative analysis.

Table of Contents

Preface	1
Acknowledgements	1
Abstract	1
Sammendrag	2
Table of Contents	4
List of Figures	7
List of Tables	8
1 Introduction	9
1.1 Background and Motivation	9
1.2 Research Aim and Questions	9
Aim	9
Main Research Question	9
Sub-questions	10
1.3 Scope and Delimitations	10
1.4 Thesis Structure	11
2 Theoretical Background	12
2.1 Trust in Digital Environments	12
Defining trust	12
Trust typologies in e-commerce	13
Trust and first-time visitors	13
2.2 Regulatory Trust and Privacy	14
Dark patterns: definition, scale, and ethics	14
Cookie consent as the primary regulatory trust interface	15
2.3 Institutional Trust and Signalling	16
Signalling theory and the credibility of institutional signals	16
Institution-based trust and trust transfer	16
Assurance seals: effectiveness and limits	17
2.4 Visual Credibility and Interface Design	18
Design look as the primary credibility channel	18
The temporal structure of first impressions	18
Prototypicality and category-based trust	18
2.5 Synthesis: The Theoretical Gap	19
3 The Layered Trust Signals Framework	21
3.1 Rationale for a Layered Approach	21
3.2 Layer 1 - Regulatory Trust	22
Definition	22
Analytical dimensions	22

3.3 Layer 2 - Institutional Trust	22
Definition	22
Analytical dimensions	23
3.4 Layer 3 - Interface-Level Trust	23
Definition	23
Analytical dimensions	23
3.5 Cross-Layer Dynamics	24
4 Methodology	26
4.1 Research Design	26
4.2 Platform and product selection	26
4.3 Observation protocol	27
4.4 Analytical approach	28
4.5 Limitations	29
5 Comparative Interface Analysis	31
5.1 Layer 1: Regulatory Trust - Cookie Consent	31
Amazon	31
Temu	32
eBay	33
Apple Online Store	33
Cross-Platform Comparison	34
5.2 Layer 2: Institutional Trust - Payment and Checkout	35
Amazon	35
Temu	36
eBay	36
Apple Online Store	37
Cross-Platform Comparison	38
5.3 Layer 3: Interface-Level Trust - Product Page	38
Amazon	39
Temu	39
Cross-Platform Comparison	40
6 Discussion	42
6.1 Interactions Between Trust Layers	43
6.2 Trust Compensation and Asymmetry	44
6.3 Platform Trust Archetypes	45
Amazon: Systemic trust	45
Temu: Tension-first trust	46
eBay: Reputation-centred trust	46
Apple: Aesthetic-institutional trust	46
6.4 Implications for Interaction Design Practice	47
7 Contribution and Originality	48
1. The Layered Trust Signals framework	49

2. The concept of trust compensation	49
3. Comparative characterization of platform trust architectures	50
4. A replicable observation protocol	50
5. Synthesis of fragmented research	50
8 Limitations and Future Research	51
8.1 Limitations of This Study	51
Non-empirical scope	51
Snapshot analysis	51
Scope of case selection	51
Western and European user perspective	51
Researcher as an analytical instrument	52
8.2 Directions for Future Research	52
References	54
Appendix A: Observation Protocol	58
Layer 1 - Regulatory Trust: Cookie Consent	58
Layer 2 - Institutional Trust: Checkout and Payment	58
Layer 3 - Interface-Level Trust: Product Page	59
Appendix B: Interface Screenshots	59
Amazon	59
Figure B.1 - Amazon: Cookie consent / absent dialogue (Layer 1)	59
Figure B.2 - Amazon: Account-level opt-out in settings (Layer 1 supplementary)	60
Figure B.3 - Amazon: Checkout / payment page (Layer 2)	61
Figure B.3a - Amazon: Buyer protection display (Layer 2)	62
Figure B.4 - Amazon: Product page above the fold (Layer 3)	63
Figure B.5 - Amazon: Review / ratings section (Layer 3)	63
Temu	64
Figure B.6 - Temu: Cookie consent dialogue, initial state (Layer 1)	64
Figure B.7 - Temu: Cookie preferences layer showing advertising cookies off by default (Layer 1)	65
Figure B.8 - Temu: Named third-party vendor disclosure in advertising cookies layer (Layer 1)	66
Figure B.9 - Temu: Checkout / payment page (Layer 2)	68
Figure B.9a - Temu: Buyer protection display (Layer 2)	69
Figure B.10 - Temu: Product page above the fold (Layer 3)	70
Figure B.11 - Temu: Review / ratings section (Layer 3)	71
Figure B.12 - Temu: Page footer showing security certifications and accepted payments (Layer 2/3)	72
eBay	73
Figure B.13 - eBay: Cookie consent banner (Layer 1)	73
Figure B.13a - eBay: Cookie preferences / manage layer (Layer 1)	74
Figure B.14 - eBay: Checkout / payment page (Layer 2)	74

Figure B.14a - eBay: Buyer protection display (Layer 2)	75
Figure B.15 - eBay: Product page above the fold showing seller reputation block (Layer 3)	76
Figure B.15a - eBay: Review / ratings section (Layer 3)	77
Figure B.16 - eBay: 'This one's trending' social proof cue, workbook record (Layer 3)	77
Apple Online Store	78
Figure B.17 - Apple: No cookie consent on first load (Layer 1)	78
Figure B.17a - Apple: Privacy settings / manage layer (Layer 1)	78
Figure B.17b - Apple: Checkout / payment page (Layer 2)	79
Figure B.18 - Apple: Product configuration page above the fold (Layer 2/3)	80
Figure B.19 - Apple: Page footer showing legal notices and privacy links (Layer 1/2)	81

List of Figures

Figure B.1 – Amazon: Cookie consent / absent dialogue (Layer 1)	Appendix B
Figure B.2 – Amazon: Account-level opt-out in settings (Layer 1 supplementary) ...	Appendix B
Figure B.3 – Amazon: Checkout / payment page (Layer 2)	Appendix B
Figure B.3a – Amazon: Buyer protection display (Layer 2)	Appendix B
Figure B.4 – Amazon: Product page above the fold (Layer 3)	Appendix B
Figure B.5 – Amazon: Review / ratings section (Layer 3)	Appendix B
Figure B.6 – Temu: Cookie consent dialogue, initial state (Layer 1)	Appendix B
Figure B.7 – Temu: Cookie preferences layer (Layer 1)	Appendix B
Figure B.8 – Temu: Named third-party vendor disclosure (Layer 1)	Appendix B
Figure B.9 – Temu: Checkout / payment page (Layer 2)	Appendix B
Figure B.9a – Temu: Buyer protection display (Layer 2)	Appendix B
Figure B.10 – Temu: Product page above the fold (Layer 3)	Appendix B
Figure B.11 – Temu: Review / ratings section (Layer 3)	Appendix B
Figure B.12 – Temu: Page footer – security certifications and payments (Layer 2/3) .	Appendix B
Figure B.13 – eBay: Cookie consent banner (Layer 1)	Appendix B
Figure B.13a – eBay: Cookie preferences / manage layer (Layer 1)	Appendix B

Figure B.14 – eBay: Checkout / payment page (Layer 2)	Appendix B
Figure B.14a – eBay: Buyer protection display (Layer 2)	Appendix B
Figure B.15 – eBay: Product page above the fold (Layer 3)	Appendix B
Figure B.15a – eBay: Review / ratings section (Layer 3)	Appendix B
Figure B.16 – eBay: ‘This one’s trending’ social proof cue, workbook record (Layer 3) ..	Appendix B
Figure B.17 – Apple: No cookie consent on first load (Layer 1)	Appendix B
Figure B.17a – Apple: Privacy settings / manage layer (Layer 1)	Appendix B
Figure B.17b – Apple: Checkout / payment page (Layer 2)	Appendix B
Figure B.18 – Apple: Product configuration page above the fold (Layer 2/3)	Appendix B
Figure B.19 – Apple: Page footer – legal notices and privacy links (Layer 1/2) ..	Appendix B

List of Tables

Table 1 – Layer 1: Regulatory Trust Dimensions Across Platforms	Chapter 5
Table 2 – Layer 2: Mechanism Strength vs. Mechanism Prominence	Chapter 5
Table 3 – Layer 3: Visual Density and Prototypicality	Chapter 5

1 Introduction

1.1 Background and Motivation

Online commerce runs on trust. You're buying from a platform you can't visit, a seller you've never met, through a payment system whose security you can't verify. That degree of vulnerability has no real equivalent in face-to-face exchange, and it's not incidental to e-commerce - it's baked into the structure of it. For interaction designers, how platforms build trust through design isn't a side issue. It's the central one.

Since the late 1990s, research on e-commerce trust has accumulated across several disciplines - organisational psychology, information systems, privacy law, UX, and visual design - each producing useful findings without much contact with the others. All of these traditions have contributed something important - but they don't speak to one another, and none of them addresses the core design question: how do trust signals operate simultaneously across different structural levels of an e-commerce interface?

This thesis develops a framework to fill that gap. Existing models treat trust either as a psychological outcome to be measured or as a design artefact evaluated within a single domain. None of them treats regulatory, institutional, and visual trust signals as co-present elements of a single design architecture, where the interactions among those layers matter as much as the properties of each one. The Layered Trust Signals framework, developed here, is built to do exactly that: to give interaction designers a vocabulary for trust as a layered design problem, and to support comparative analysis of how different platforms construct, sustain, or undermine trust across all three levels at once.

1.2 Research Aim and Questions

Aim

The aim of this thesis is to develop a layered analytical framework for understanding how trust is built in e-commerce interfaces and to apply it in a comparative interface analysis.

Main Research Question

How are trust signals structured across regulatory, institutional, and interface levels in contemporary e-commerce platforms?

Sub-questions

- How do cookie consent mechanisms construct or undermine regulatory trust?
- How do third-party payment providers and institutional signals function as trust-transfer mechanisms?
- How does product-page visual structure influence perceived credibility and quality?
- How do these trust layers interact or compensate for one another across different platforms?

1.3 Scope and Delimitations

This study is non-empirical and aims to analyse the design of the platforms. The study does not consider the internal workings of these platforms but instead considers the user interface. The platforms considered in this study are Amazon, Temu, eBay, and Apple's online store. "Contemporary e-commerce platforms" here refers to general-purpose retail interfaces that are active in the European market, serve consumers directly, and are large enough that their design choices are unlikely to be accidental. They were selected because they represent structurally different trust architectures - a hybrid marketplace (Amazon), a direct-from-manufacturer platform under regulatory scrutiny (Temu), a C2C marketplace (eBay), and a closed brand storefront (Apple) - rather than as a representative sample of e-commerce at large. Desktop versions are analysed throughout. Mobile versions are excluded from the analysis. Off-canvas navigation, overlay menus, and compressed layouts on mobile create enough structural variation that comparing trust signal dimensions across four different platforms becomes unreliable. All observations used the European versions of each platform, accessed from a Norwegian IP, because all four fall under GDPR - that shared regulatory context makes consent design differences attributable to platform decisions rather than to different legal obligations.

This study does not measure user responses to these interfaces. The security and data practices behind them are equally out of scope. Trust signals, as used throughout this thesis, refers to the design features through which a platform communicates trustworthiness to users - covering regulatory, institutional, and visual dimensions. Chapter

2 develops this in full. The observations for each platform's user interface were taken between 19 and 26 May 2026. As the user interfaces for these companies are constantly changing, the findings of this study are only specific to the user interface of each of these platforms on the date of its observation.

1.4 Thesis Structure

Chapter 2 sets up the theoretical background - foundational trust theory, regulatory trust and privacy design, institutional trust and signalling theory, and visual credibility research. Chapter 3 develops the Layered Trust Signals framework: each layer, its analytical dimensions, and the cross-layer dynamics. Chapter 4 covers the methodology. Chapter 5 presents the comparative interface analysis, layer by layer across the four platforms. Chapter 6 discusses the findings, developing trust compensation, and platform trust archetypes. Chapters 7 and 8 cover contributions and limitations.

2 Theoretical Background

The Layered Trust Signals framework is based on four research areas that examine trust in digital commerce, though they are rarely combined. Section 2.1 covers foundational trust theory. Section 2.2 examines regulatory trust through the lens of the literature on privacy design and dark patterns. Section 2.3 addresses institutional trust through signalling theory and institution-based trust research. Section 2.4 covers visual credibility and its relationship to perceived trustworthiness. Section 2.5 pulls these together and identifies the gap the framework is designed to address.

2.1 Trust in Digital Environments

Defining trust

The most influential definition of trust in the management and organisational literature is Mayer, Davis, and Schoorman's (1995): "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party" (p. 712). A few things in this definition are worth holding on to. Trust isn't the same as confidence or reliance - it specifically requires accepting vulnerability, so risk is a precondition, not trust's opposite. It is also a relationship between specific parties, not a property of either one in isolation. And it operates in the absence of control: where monitoring is possible, you don't need trust, you can just verify.

Mayer et al. identify three dimensions of trustworthiness in the trustee: ability, the perception that the trustee has the competence to do what the trustor needs; benevolence, the perception that the trustee cares about the trustor's interests beyond pure self-interest; and integrity, the perception that the trustee adheres to acceptable principles. These three dimensions aren't interchangeable. A seller who's highly competent but dishonest fails the integrity dimension. A well-intentioned seller without relevant expertise fails the ability dimension. A business that puts its own interests ahead of the trustor's fails benevolence. The ABI model doesn't just define trustworthiness - it's a diagnostic tool for identifying which dimension of trust a given design mechanism is targeting.

Although Mayer et al. developed their model in an organizational context, it has been adopted almost universally in e-commerce trust research as the foundational typology of trustworthiness dimensions. In the interface analysis conducted in this thesis, each trust signal is evaluated partly in terms of which ABI dimension it addresses: institutional signals such as payment logos speak primarily to ability (the platform is capable of processing the transaction securely) and integrity (it is legitimate); aesthetic coherence signals speak to benevolence and integrity; and regulatory design speaks primarily to integrity (the platform respects user rights).

Trust typologies in e-commerce

The translation of Mayer et al.'s model into e-commerce is most thoroughly done by McKnight, Choudhury, and Kacmar (2002), who develop and validate a multidimensional trust typology for online commerce. They identify four constructs. Disposition to trust is a person's general tendency to trust others, formed by personality and experience - it shapes all other trust processes but can't be addressed through interface design. Institution-based trust is the belief that structural safeguards exist - legal frameworks, platform policies, industry standards - that make online transactions safe regardless of the specific party involved. Trusting beliefs are the specific impressions someone holds about a particular vendor's ability, benevolence, and integrity. Trusting intentions are the behavioural willingness to act on those beliefs - sharing personal information, completing a purchase.

This typology maps directly onto the Layered Trust Signals framework. Institution-based trust corresponds to the institutional layer - the user's sense that structural safeguards exist regardless of who the specific seller is. Trusting beliefs correspond to the interface layer - impressions of ability, benevolence, and integrity formed through direct interaction with visual design. The regulatory layer is the one thing McKnight et al.'s typology doesn't explicitly address, which isn't surprising given that it predates GDPR.

Trust and first-time visitors

Gefen, Karahanna, and Straub (2003) found a direct consequence for interface design: for first-time visitors to an online store, trust is the dominant driver of purchase intention - substantially ahead of perceived usefulness or ease of use. That shifts for repeat users, but trust stays significant throughout. This means that interface-level trust signals aren't supplementary. For the large proportion of users who are new to a platform, visual and

aesthetic design is the primary factor determining whether someone engages at all, which is exactly what motivates treating it as a trust-building activity rather than a mere stylistic preference.

2.2 Regulatory Trust and Privacy

Dark patterns: definition, scale, and ethics

Dark patterns - interface designs that serve commercial interests at users' expense - were introduced to academic UX research by Gray et al. (2018). Their content analysis of practitioner-identified examples makes a key point: dark patterns aren't produced by malicious actors so much as by design cultures that optimise for business metrics without ethical guardrails. Designers can end up complicit through A/B testing that rewards conversion rates, client pressure, and a lack of ethical training. The 'complicity' framing matters analytically here: it means that the presence of dark patterns in an interface is a design choice, whether deliberate or not, and therefore constitutes evidence of intent.

Mathur et al. (2019) crawled 11,000 shopping websites and found 1,818 dark pattern instances across 15 types in seven categories: sneaking, urgency, misdirection, social proof manipulation, scarcity claims, obstruction, and forced action. Twenty-two third-party vendors sell dark pattern designs as commercial products - this is a market, with suppliers and buyers, not a set of independent decisions by individual designers. Nie et al. (2024) subsequently extend the taxonomy to 64 types and note that automated detection tools still cover only around half of them. Chapter 5 uses qualitative interface analysis partly for that reason: automated tools would miss too much.

The consequences of dark patterns in the law and in human behavior are documented by Luguri and Strahilevitz (2021). In their randomized experiment, which exposed users to mild, aggressive, and no dark patterns, those exposed to mild patterns were more than twice as likely to subscribe to a dubious third-party service compared to users who did not experience any dark patterns. Those exposed to aggressive dark patterns were nearly four times as likely to subscribe. However, those exposed to aggressive dark patterns were also more likely to experience backlash towards the platform overall; users exposed to aggressive dark patterns were more likely to be aware of the presence of those design elements in the platform, and developed a hostility towards the platform as a result. This element directly relates to the discussion of Temu in Chapter 5 of this thesis.

Cookie consent as the primary regulatory trust interface

Nouwens et al. (2020) tested 10,000 live consent interfaces and found two design choices explained most of the variance in how many users accepted: whether a reject option appeared at the top level at all, and whether the accept and reject buttons looked the same. Neither finding is surprising given the regulatory context. GDPR came into force in 2018 requiring freely given consent to non-essential data collection, but the legislation said nothing about how consent interfaces had to be designed. What followed was extensive optimisation for acceptance rates - hiding the reject option, greying it out, making it smaller. Chapter 5 evaluates each platform's consent design against Nouwens et al.'s two criteria.

Berens et al. (2024) find that reject label wording moves acceptance rates: the more cognitive or emotional effort the label demands, the higher the consent rate. They also find that a substantial share of websites install non-essential tracking cookies regardless of what the user chose - the interface and the data practice are not connected. Papenmeier, Halama, and Reichert (2025) study consent behaviour longitudinally rather than at a single point and find that roughly two-thirds of users settle into a fixed pattern - always accepting or always rejecting - early in their exposure to a given type of interface. That pattern held even when users encountered consent designs that differed from what prompted the initial habit. For platforms trying to maximise consent rates, the practical implication is that first-contact design carries disproportionate weight; subsequent exposures mostly reinforce what was already decided. Kocyigit, Rossi, and Lenzini (2023) operationalise this body of work as 31 measurable features for detecting dark patterns in consent flows; the observation protocol in Chapter 5 is built on that feature set. Jamalifard, Russell-Rose, and Brignull (2024) added a physiological dimension to this. Using eye-tracking and electromyography, they found that obfuscated cancellation flows produce stronger negative emotional responses than transparent ones. The manipulation is measurable in the body, not just in behaviour.

Cookie consent isn't a legal formality that precedes the real experience. For most users it's the first interaction a platform initiates, and the design decisions visible in that moment - whether the reject path is easy, whether the buttons are equal, what the labels say - are

legible evidence of how the platform treats user autonomy when commercial incentives cut against it.

2.3 Institutional Trust and Signalling

Signalling theory and the credibility of institutional signals

Why do institutional signals - payment logos, assurance seals, buyer guarantee badges - actually influence behaviour? The answer lies in Spence's (1973) foundational account of signalling in markets with information asymmetry. Spence's argument, developed in labor markets but applied widely across social science, is that when buyers can't observe quality directly, credible quality signals must be costly - specifically, more costly for low-quality actors than for high-quality ones. A signal that's equally accessible regardless of underlying quality conveys nothing and can't sustain trust. Differential cost is what makes a signal informative.

Spence's framework explains why institutional affiliation carries weight in e-commerce. Operating under a payment network's terms means accepting real costs: compliance standards, chargeback liability, ongoing contractual obligations that fraudulent actors either cannot afford or cannot sustain. A Visa or PayPal logo is evidence of those costs having been accepted. Buyer guarantee programmes work on the same logic. Committing to reverse charges or cover losses is an obligation that bad actors would not take on. In Chapter 5, each institutional signal is evaluated on whether the costs behind it are real or whether the signal is essentially costless to deploy.

Institution-based trust and trust transfer

Pavlou and Gefen's (2004) framework defines institution-based trust as a buyer's belief that effective third-party mechanisms exist to guarantee a successful transaction, regardless of who the seller is. They identify three such mechanisms. Feedback systems aggregate seller history and make it visible, but are manipulable and depend on volume to work - Pavlou and Gefen call these "weak." Third-party escrow services hold payment until delivery is confirmed. Credit card guarantees give buyers legal recourse to dispute charges. The latter two are "strong" mechanisms: their protection is structural and does not hinge on what any particular seller does.

There's also what Pavlou and Gefen call trust transfer: trust in a marketplace platform as an institution partially carries over to the sellers it hosts. A buyer who trusts Amazon extends some of that trust to third-party sellers on the platform, even without seller-level information. That's why selling on an established platform gives a trust benefit that selling on an unknown independent website doesn't. And it's why a collapse in platform trust - through regulatory failures, data breaches, or exposure of manipulative practices - hits all sellers simultaneously.

Ba and Pavlou (2002) put numbers on it: sellers with higher feedback ratings get measurably higher prices, with the effect concentrated in categories where product quality is hard to verify in advance. Institutional signals cut perceived risk, and lower perceived risk shifts what terms buyers will accept. On eBay the feedback mechanism sits at the centre of the architecture rather than around it - the platform's buyer protection and its visual design both exist to support that signal rather than compete with it.

Seller-level trust and platform trust aren't the same thing, and the gap between them matters most in C2C markets. Wang et al. (2022) found in a meta-analysis that seller trust outweighed platform trust as a predictor of purchase intention in social commerce. Mayayise (2024) identifies seller reputation, feedback scores, and structural assurance as the main drivers in C2C e-commerce. In eBay's design the distinction is visible directly: the platform's own credibility mechanisms are present but positioned behind the seller's feedback score rather than in front of it.

Assurance seals: effectiveness and limits

Hu, Wu, and Zhang (2010) showed experimentally that assurance seal types are not interchangeable - they address different trust dimensions and interact. Privacy seals cover data handling. Security seals cover the transaction channel. Transaction integrity seals cover seller performance. Whether a platform needs a privacy seal or a transaction integrity seal depends on where its trust risks actually lie. Temu, under DSA scrutiny for data practices, faces a different problem than eBay, where the risk is seller reliability in a C2C market.

Head and Hassanein (2002) identify the standard failure mode for third-party seals: users who don't recognise the certifying body get nothing from the seal. A logo from an unknown organisation is not a credibility signal. Head and Hassanein call this "design

rhetoric.” The Chapter 5 analysis asks, for each of the four platforms, which seals a typical user could actually identify - and which ones are there for other reasons. Peña-García et al. (2024) find the same problem in review systems: perceived authenticity builds trust, while the perception of fake reviews damages all trust dimensions at once.

2.4 Visual Credibility and Interface Design

Design look as the primary credibility channel

Fogg et al.’s (2003) large-scale credibility study established this empirically. In a study with 2,684 participants evaluating pairs of live websites, design look, layout, typography, imagery, and overall visual treatment were the most frequently cited credibility factors, mentioned in 46.1% of all comments. Information structure came second at 28.5%. Users assess website credibility primarily through its visual surface, not its content quality, factual accuracy, or formal credentials - at least in the initial phase when they decide whether to stay. Information design ranking second confirms that structural clarity is itself a credibility signal, not just a usability feature.

Tractinsky, Katz, and Ikar (2000) call the mechanism the “what is beautiful is usable” heuristic. Their experiment showed that perceived aesthetics predicted perceived usability both before and after use; actual usability did not move aesthetic ratings in return. It runs one way. Robins and Holmes (2008) replicated the pattern at the content level - identical text rated more credible under higher-quality visual presentation. The effect applies element by element, not just to the overall page.

The temporal structure of first impressions

Lindgaard, Fernandes, Dudek, and Brown (2006) found something that matters for interface design: visual appeal can be assessed in as little as 50 milliseconds. Assessments formed that quickly correlate strongly with those formed after extended viewing. That first impression comes before any reading, before any processing of institutional signals, before any conscious evaluation of regulatory compliance. It comes before everything else. So the interface layer isn't just the third layer in a theoretical hierarchy - it's the first one users actually encounter in practice, and it sets the frame through which all subsequent trust signals are processed.

Prototypicality and category-based trust

Recent research has introduced prototypicality as a distinct and particularly powerful predictor of perceived trustworthiness. Miniukovich and Figl (2023) study 1,530 participants across multiple website categories and find that prototypicality - the degree to which a website's visual design matches users' expectations for what a website of that type should look like - has the strongest direct effect on trustworthiness, outweighing both aesthetics and usability as independent predictors. Their structural equation models indicate that prototypicality, aesthetics, and usability together account for 29 to 68 percent of the variance in trustworthiness, depending on the website category, a range that reflects the category-specific nature of prototypicality schemas.

Miniukovich, Figl, and Ernst (2024) ran eye-tracking studies specifically on shopping websites. More visual complexity on a product page meant more fixations, lower perceived competence, and lower purchase intention - a pattern that didn't generalise to non-shopping contexts in their data. Jinchun, Yini, and Kexing (2024) put a cross-cultural dimension on this: the high density, stacked promotions, and urgency-heavy design that are standard on Pinduoduo - Temu's domestic Chinese platform - read as low-prototypicality and potentially manipulative to Western users while reading as normal to users familiar with that design vocabulary. Miniukovich and Figl (2023) describe the same mechanism from the other direction: in their structural equation models, prototypicality had the strongest direct path to trustworthiness ratings, outweighing both aesthetics and usability. Users aren't consciously evaluating whether a site looks like other sites they've trusted - the processing happens before that.

2.5 Synthesis: The Theoretical Gap

The four strands of literature reviewed here cover different pieces of the same problem. Trust theory - Mayer et al.'s ABI model, McKnight et al.'s e-commerce typology - gives the analysis its conceptual vocabulary. Dark pattern and consent design research shows how regulatory trust is constructed or stripped away at the interface level. Institutional trust research explains the mechanics of third-party credibility transfer and where it breaks down. Visual credibility research establishes that aesthetics are both the fastest and the most automatic trust channel, with prototypicality doing most of the work.

What none of these traditions does is account for how the mechanisms interact across a single interface. A user who hits a manipulative cookie banner, then a credible payment

page, then a visually authoritative product page has not gone through three separate trust processes. The overall impression depends on how those layers fit together - whether they reinforce each other or pull in different directions. Existing frameworks look at one layer at a time. None of them is built to characterise the architecture as a whole or compare architectures systematically across platforms.

The Layered Trust Signals framework, developed in Chapter 3, is designed to fill precisely this gap. It is not a theory of trust; the theoretical work reviewed above provides the necessary foundations. It is an analytical instrument that organises the existing theoretical knowledge into a design-applicable model capable of supporting comparative interface analysis.

3 The Layered Trust Signals Framework

Chapter 3 develops the Layered Trust Signals framework - a design-oriented analytical model for understanding how trust is constructed across three structural levels of the e-commerce interface. Section 3.1 makes the case for a layered approach, drawing on the theoretical foundations outlined in Chapter 2. Sections 3.2 through 3.4 define each layer, connect it to the relevant literature, and specify the analytical dimensions used in the interface analysis of Chapter 5. Section 3.5 addresses cross-layer dynamics as the basis for the discussion of trust compensation in Chapter 6.

3.1 Rationale for a Layered Approach

The Chapter 2 literature does not converge on a single account of trust. McKnight et al.'s (2002) typology separates institution-based trust - the sense that structural safeguards exist - from trusting beliefs about a specific vendor. Mayer et al.'s (1995) ABI model has three trustworthiness dimensions that are independent and non-substitutable. Fogg et al. (2003) show visual surface is the primary credibility channel. Nouwens et al. (2020) establish consent design as a trust-relevant domain in its own right. The shared implication is that trust is not a quantity with a single dial - it is formed through qualitatively different mechanisms at different interface levels, and a framework that treats it as uniform will produce a flat analysis.

Existing approaches in both research and practice tend to address one level at a time. Survey-based trust models aggregate responses into single-construct measures. Dark pattern audits focus on manipulative design without looking at how it interacts with other trust signals. Credibility assessments evaluate visual design in isolation from institutional context. No existing framework treats regulatory, institutional, and visual trust signals as co-present elements of a single design architecture - where the interactions among them matter.

The Layered Trust Signals framework addresses this by proposing that e-commerce trust is constructed across three structurally distinct layers - each grounded in a different theoretical tradition, each visible through different design features, and each capable of interacting with the others in analytically significant ways. The layers are not a hierarchy

of importance - all three are simultaneously present in a complete e-commerce interaction

- but a structural differentiation that reflects the different mechanisms, temporalities, and design vocabularies through which trust is constructed at each level.

3.2 Layer 1 - Regulatory Trust

Definition

Regulatory trust is a user's perception that the platform operates within legitimate legal and ethical limits on data and privacy. In European e-commerce, cookie consent is where that perception forms - it is the first moment the platform's stance on GDPR is made visible. A consent interface with a reject option as easy to reach as the accept option suggests the platform is taking the legal requirement at face value. One that hides the reject option, tilts the visual design toward acceptance, or uses manipulative copy suggests it is not: that compliance is the floor, not the standard.

Analytical dimensions

- Accept/Reject symmetry: whether the consent interface offers equivalent visual access to accepting and rejecting non-essential cookies
- Button hierarchy: whether colour, size, and position are used to steer users toward a particular choice
- Granularity of choice: whether category-level consent controls are available without sub-menu navigation
- Steps to reject: the number of interactions required to refuse all non-essential cookies
- Label wording: the specific language used on accept and reject options
- Default state: whether non-essential cookie categories are pre-selected

3.3 Layer 2 - Institutional Trust

Definition

Institutional trust is the user's sense that third-party mechanisms exist to protect the transaction - independent of who the specific seller is. Pavlou and Gefen (2004) are the anchor here: their framework defines institution-based trust through the visible presence of

payment provider logos, buyer protection guarantees, certification seals, and seller reputation systems. Following Spence (1973), the credibility of these signals depends on whether they are costly to acquire - that is, whether they represent real institutional accountability or are just design rhetoric: the appearance of legitimacy without anything behind it.

Analytical dimensions

- Payment provider logos: which providers are displayed, at what prominence, and at what point in the checkout flow
- Buyer protection messaging: the presence, specificity, and placement of guarantee or money-back commitments
- Seller identity signals: how seller identity and reputation are surfaced and distinguished from platform identity
- Assurance seals: the presence, recognisability, and type (privacy, security, transaction integrity) of certification badges
- Mechanism strength: whether dominant signals are weak (market-driven, e.g. ratings) or strong (legally binding, e.g. buyer guarantees)

3.4 Layer 3 - Interface-Level Trust

Definition

Interface-level trust is built through direct visual experience of the platform - aesthetic coherence, visual density, information hierarchy, prototypicality, and the persuasive design vocabulary of product pages. Two aspects of this layer are worth noting. It operates faster than the others: Lindgaard et al.'s (2006) 50-millisecond finding means visual appeal is assessed before the user has consciously processed anything else, so in practice this is often the first trust impression, not the last. And it works through implication - the interface does not assert trustworthiness, it produces that perception through aesthetic authority, structural clarity, and conformity to what users expect from that type of site.

Analytical dimensions

- Visual density: the number and complexity of distinct elements visible above the fold

- Aesthetic coherence: consistency of colour strategy, typography, and spatial organization
- Prototypicality: the degree to which the layout matches Western e-commerce category conventions for the product type
- Information hierarchy: the ordering and relative visual weight of product name, price, reviews, and description
- Review prominence: the placement, legibility, and accessibility of star ratings and review content
- Persuasive cues: the presence, type, and density of scarcity messages, urgency countdowns, and social proof indicators

3.5 Cross-Layer Dynamics

The core claim of the Layered Trust Signals framework is that the three layers interact, and that those interactions - not just the properties of each layer in isolation - are analytically central to understanding a platform's trust architecture. Three interaction types stand out.

Aligned layers reinforce each other. A user who passed through a clean consent interface and a familiar checkout page doesn't approach the product page neutrally - they've already built up a baseline. The same product page reads differently if it follows trust-consistent signals than if it follows an extractive banner and an unfamiliar checkout.

Conflicting layers put the user in an interpretive bind. Scarcity countdowns and urgency cues suggest a platform optimising hard for conversion; buyer protection badges at checkout suggest one with genuine commitments to the buyer. If a user registers both, they have to decide which is more representative - and there's no guarantee institutional signals win that comparison.

Compensation occurs when a weakness in one layer is partially covered by a strength in another. A platform with an extractive-consent design might still sustain user engagement through strong buyer protection or interface-level persuasion around price. The key question is whether this produces genuine trust or something structurally different - continued use of a platform despite distrust, which Liu and Gómez-Cruz (2025) call platform cynicism. Trust compensation and its limits are the original theoretical

contribution of this framework, developed through the comparative analysis in Chapter 5 and the discussion in Chapter 6.

4 Methodology

4.1 Research Design

This study is non-empirical. There are no user surveys, no experiments, and no behavioural data. The question driving the analysis is what is present in the interface - which trust signals exist, how they are designed, and how they relate to one another across layers. That's a design analytical question. It calls for close, structured observation, not statistical inference.

Interface auditing as a method has a track record. Mathur et al. (2019) used it to document dark pattern prevalence across thousands of shopping websites. Gray et al. (2018) used it to map manipulative design types from practitioner examples. Kocyigit, Rossi, and Lenzini (2023) broke GDPR compliance into 31 directly observable interface features and applied them systematically. In each case the researcher defines a feature set in advance, treats the interface as the unit of analysis, and applies it consistently. That's what this study does - using the Layered Trust Signals framework from Chapter 3 as the feature set.

4.2 Platform and product selection

The four platforms examined are Amazon, Temu, eBay, and Apple's online store. They weren't chosen to be a representative sample of e-commerce. The selection criterion was structural variety - each platform has a different trust architecture, and that's what makes the comparison useful.

Amazon is a hybrid marketplace: a platform-plus-seller model, with the A-to-z Guarantee providing strong institutional coverage regardless of who the seller is. Temu is a direct-from-manufacturer model that has been under DSA scrutiny for data practices and imports the high-density visual design of its parent company's Chinese domestic platform. eBay is a C2C marketplace where platform-level institutional trust is secondary and seller

reputation carries most of the load. Apple runs a closed storefront - it is always the seller - where brand identity substitutes for most of the third-party signals the other platforms rely on. Each one sits in a different position on the dimensions the framework measures.

All four platforms were observed in their European versions, accessed from a Norwegian residential IP. That access context matters most for Layer 1 - all four are under GDPR, so any differences in consent design come down to platform choices rather than different regulatory requirements. Desktop only, throughout. Mobile interfaces were excluded because compressed navigation and overlay menus make it too hard to compare the same features like-for-like across platforms.

A single product category was used across all four platforms where available: a portable Bluetooth speaker (JBL Flip 6 or equivalent). Using the same product category controls for one obvious source of variation in the interface layer - product type shapes visual density norms, typical review counts, and price display conventions.

4.3 Observation protocol

Observations followed the structure of the three framework layers. For Layer 1, each platform was loaded in a fresh browser session with no prior cookies, and the cookie consent dialogue - or its absence - was recorded before any interaction. Six dimensions were captured, following Section 3.2: accept/reject symmetry, button hierarchy, granularity at the top level, steps to reject, label wording, and default toggle state.

Layer 2 required navigating each platform from the product page to the checkout - or as close to checkout as was accessible without creating an account. Payment provider logos were recorded as they appeared: which ones, at what point in the flow, and whether they were present on the product page itself or only at checkout. Buyer protection language was captured verbatim where present. Seller identity was only a meaningful observation on eBay and Amazon, where a third-party seller can be distinguished from the platform; Apple and Temu are both always the seller, so there was nothing to record separately. Assurance seals were logged along with a judgment, following Head and Hassanein's (2002) criterion, of whether a typical European consumer was likely to recognise the certifying body. The mechanism classification - weak or strong in Pavlou and Gefen's (2004) terms - was applied after the observation, not during it.

Layer 3 meant sitting with each product page and logging what was visible before scrolling. Lindgaard et al. (2006) clocked aesthetic impressions forming in 50 milliseconds - before any deliberate reading - which is why I treated what loads in that initial viewport as the analytically meaningful zone rather than the full page. Element count in that zone went into the workbook as a rough indicator of density; I didn't try to weight individual elements against each other. Fogg et al.'s (2003) credibility study found that design look accounted for 46.1% of participants' comments about what made a site credible or not, so colour strategy, typographic consistency, and spatial organisation were documented with that hierarchy in mind. Any scarcity messages, countdown timers, or social proof claims were copied verbatim into the workbook - paraphrasing them would lose the specific language, which is part of what makes them work or not work on a given user. Whether the page looked like a typical e-commerce page for that product type was a judgment call, framed by Miniukovich and Figl's (2023) definition of prototypicality but ultimately mine to make.

Both sessions used Chrome 136, a Norwegian residential IP, no VPN, and no incognito mode. All button text, badge wording, guarantee copy, and scarcity claims were copied verbatim into the observation workbook as they appeared. Where the two sessions produced different readings - a different product listing, an apparently updated consent design, or an element read differently on second viewing - both readings were retained and the discrepancy is noted in the Chapter 5 analysis rather than resolved before writing. The workbook, including all verbatim label transcriptions, observation tables, and inter-session discrepancy notes, is retained as a research record and is available on request.

4.4 Analytical approach

The analysis runs layer by layer rather than platform by platform. A platform-by-platform structure would produce four separate profiles. A layer-by-layer structure produces three cross-platform comparisons, which fits the framework better - the main claim is about how layers differ and interact across platforms, and that's only visible when you look across all four at once.

Within each layer, I work through each platform against the protocol dimensions, then look across all four to identify patterns. Where observed design features connect to or contradict

theoretical constructs from Chapter 2, those connections are made explicit in the analysis rather than left to the reader to infer.

4.5 Limitations

The clearest limitation of snapshot analysis is that commercial interfaces change constantly through A/B testing. The version observed on a given date is not necessarily the version another user sees a week later. This isn't a flaw in the method - it's just a property of the object being studied. The observation date is recorded precisely so the findings are traceable. The second session on 26 May 2026 gives some mitigation: any changes between sessions are documented rather than glossed over.

Because this study is non-empirical, trust is inferred from design features rather than measured from actual user behaviour. The analysis identifies design choices that the literature links to trust construction or erosion - it does not confirm that users of these specific platforms respond to them in exactly the way the literature predicts. Variation in prior experience, cultural background, and what McKnight et al. (2002) call disposition to trust falls outside the scope of this analysis.

The analysis was conducted from a single access context: Norwegian residential IP, desktop Chrome, unauthenticated for Layer 1 observations. Interfaces vary by geography, login state, device, and browsing history. Some platforms serve different consent interfaces based on detected location. Some hold institutional signals behind a login wall - Amazon's checkout is the clearest case, where payment logos and buyer protection information only appear post-login. Where access conditions affect what's observable, the constraint is noted in the analysis rather than treated as equivalent to a condition without it.

The four platforms don't cover the full range of e-commerce. Vertical specialists, mobile-native platforms, and non-Western markets are all outside scope. And qualitative interface analysis is interpretive by nature - the observation protocol grounds judgements in theory-derived criteria, but applying those criteria still requires judgement. The analyst can't be factored out.

The two-session design was a response to interface instability rather than a planned replication. Between sessions A and B, Temu had updated its cookie consent flow - a change a single-session study would not have detected. That discovery motivated returning

to check all four platforms for updates. Most were unchanged between 19 and 26 May 2026. Where the two sessions produced different readings, both are retained and the discrepancy is flagged in the Chapter 5 analysis. This is a partial mitigation for snapshot instability, not a solution to it: any interface observed within this window may have changed by the time this thesis is read.

5 Comparative Interface Analysis

Chapter 5 applies the Layered Trust Signals framework to a systematic comparative analysis of the four selected platforms. The analysis moves layer by layer: Section 5.1 examines the regulatory layer through cookie consent interfaces, Section 5.2 covers the institutional layer through payment and checkout pages, and Section 5.3 examines the interface layer through the product page's visual structure. Each section ends with a cross-platform synthesis.

5.1 Layer 1: Regulatory Trust - Cookie Consent

Amazon

Amazon's Norwegian storefront presents no cookie consent dialogue on first visit. Accessing amazon.com from a Norwegian residential IP in an unauthenticated session produces no GDPR consent banner - not on page load, not after scrolling, not at any point during the unauthenticated session. Tracking is on by default from the first visit. The only opt-out path runs through account settings: Account → Browsing History → Turn off, and separately to Account → Advertising Preferences. Both require login to access. Non-account users have no opt-out path at all without blocking cookies manually in the browser. Several Amazon privacy management pages also return dead or redirected links, making the path less accessible still.

Nouwens et al.'s (2020) two criteria - a top-level reject option, and visual equivalence between accept and reject buttons - both require a consent dialogue to be present in the first place. Amazon has none, so both fail by default. Berens et al.'s (2024) work on label wording is equally inapplicable; the labels don't exist. Amazon's Layer 1 design treats data collection as the default condition of access rather than something requiring active consent, which puts it structurally at odds with GDPR's requirement for freely given, specific, informed, and unambiguous consent at the point of collection.

What this signals about the platform's stance toward user autonomy is straightforward: the design burden falls entirely on the user who wants to opt out. Amazon's consent architecture is the inverse of symmetry. It reflects a platform that has constructed a

post-login account infrastructure as the primary privacy management tool - not incidentally out of compliance, but as a deliberate design model that prioritises conversion over regulatory consent.

Temu

On first visit, a modal dialogue appears before the page is usable. Three options: 'Tilpass informasjonskapsler' (Customise) as a plain text link, 'Avvis alle' (Reject all) as an orange filled button, and 'Godta alle' (Accept all) as an orange filled button of identical size and visual weight. Rejection is one click. In the preferences layer, advertising cookies arrive toggled off by default. Amazon and Apple present no consent mechanism at all; eBay's has a colour asymmetry that steers toward acceptance. Temu runs the most compliance-forward design of the four, which sits in sharp contrast to what its product pages do.

On Nouwens et al.'s (2020) criteria, both pass: a reject option at the top level, and the two primary buttons identical in size, fill, and colour. The one remaining asymmetry is positional - 'Godta alle' sits on the right, the conventional primary-action slot in left-to-right reading, which gives it a marginal positional advantage without a visual one. Session B also picked up something worth noting: Temu breaks the industry norm of a filled accept button next to a greyed or outlined reject button. Users who have been conditioned by that convention elsewhere may momentarily hesitate on Temu's interface, uncertain which button does what. It cuts both ways: higher GDPR compliance on visual equivalence, at the cost of some usability friction from deviating from the norm.

Navigating into 'Tilpass informasjonskapsler' reveals something unusual: under 'Informasjonskapsler for annonsering' (Advertising cookies), Temu lists specific third-party companies by name rather than by category. GDPR Article 13 doesn't require that at the first consent level - Temu is going beyond what the regulation demands. Users who don't navigate into the preferences layer see symmetric buttons but no recipient names; the vendor list is there, behind one more click. Berens et al. (2024) would classify 'Avvis alle' as a compliant, low-cognitive-demand label.

That Temu - a platform that has faced European Commission scrutiny under the DSA - operates the most GDPR-compliant consent design of the four platforms is the most

analytically striking finding at Layer 1. Regulatory compliance at the consent interface and commercial design intent at the product page are entirely decoupled.

eBay

eBay's consent interface loads as a banner at the bottom of the page, not blocking anything. Three options: 'Accept All' as a blue filled button, 'Decline All' as a white button with blue outline, and 'Customise my choices' as a plain text link. Rejecting everything is one click from the banner. You can scroll and interact with the page without touching the consent interface at all.

"Decline All' is present at the top level - Nouwens et al.'s (2020) first criterion is met. Their second criterion is where this design has a problem: 'Accept All' is a filled blue button, 'Decline All' is outlined at the same size. Nouwens et al. specifically identified filled button styling as a driver of higher consent rates, because the filled convention reads as the intended primary action. The label wording is fine - Berens et al. (2024) would classify 'Decline All' as compliant and low in cognitive demand - but the visual treatment works against the label.

One notable feature of the first-level banner: it states '24 third-party companies' - an explicit count without named companies at the first level. The preferences layer names only Meta and Google as the companies eBay sells data to. The discrepancy between a headline count of 24 and a named list of 2 is worth flagging as a possible design rhetoric element. The non-blocking bottom-bar format allows page interaction before consent is given, which may reduce the salience of the decision for users who scroll past it.

Apple Online Store

The Apple Online Store presented no cookie consent dialogue during either session - not on page load, not after scrolling, not at any point in the unauthenticated visit. No opt-out mechanism appeared. Neither of Nouwens et al.'s (2020) criteria applies here because there's no interface to evaluate them against.

The analytical complexity here is specific to Apple. Apple's global brand is built substantially on privacy advocacy - 'Privacy. That's iPhone' and 'Privacy is a fundamental human right' are active brand propositions. That the platform making these claims provides zero privacy choice on its Norwegian web storefront creates a sharp

internal contrast. A first-time visitor receives no choice regarding cookie consent - which either confirms their prior that Apple tracks nothing (the brand promise read as literal assurance) or violates it (the absence of consent read as indifference). Both readings coexist in the user population, and neither is stable.

Session B raised a possible explanation worth noting. Anyone who uses Apple hardware - iPhone, Mac - will have already been walked through a data consent flow during device setup. From Apple's commercial perspective, the web consent mechanism may be redundant; the primary data relationship is established at the device level, not the browser level. If that's the reasoning, the absent banner is a deliberate architecture decision rather than an oversight. That reading is speculative, and it doesn't change the GDPR picture: specific consent at the point of web data collection is still required, and it's still absent.

Cross-Platform Comparison

The four platforms represent four distinct approaches to regulatory trust, none of which maps straightforwardly onto the regulatory requirement they share.

Table 1: Layer 1 - Regulatory Trust Dimensions Across Platforms

Dimension	Amazon	Temu	eBay	Apple
Reject option at top level	No	Yes - 'Avvis alle'	Yes - 'Decline All'	No
Visual symmetry (accept/reject)	N/A	Yes - identical orange buttons	Partial - filled vs outlined	N/A
Default state (non-essential)	ON (account setting)	OFF	OFF	N/A
Steps to reject all	3-4 (post-login)	1	1	N/A
Third-party disclosure at first level	No	No (named in second layer)	Count only (24 companies)	No
Nouwens et al. score	0/2	2/2	~1.5/2	0/2

The clearest finding at Layer 1 is the split between platforms that face active regulatory scrutiny and those that do not. Temu - under DSA oversight and facing EC investigations into its data practices - operates the most GDPR-compliant consent design of all four.

Amazon and Apple - two of the three highest-valued companies in the world - present no consent mechanism at all. The compliance ordering is the inverse of what commercial scale and regulatory capacity would predict. This isn't incidental. It suggests that Layer 1 design is primarily a response to enforcement pressure, not a principled commitment to user autonomy. Where enforcement is credible, consent interfaces improve. Where it isn't - or where platform scale provides regulatory insulation - consent design is treated as optional.

The pattern matters beyond individual compliance scores. A consent interface is the first interaction a user has with a platform's stance on their data. A platform that provides no choice at that moment communicates something about how it handles user agency in general - and that impression persists into Layer 2 and Layer 3 processing.

5.2 Layer 2: Institutional Trust - Payment and Checkout

Amazon

Amazon's institutional layer contains strong mechanisms, but they are not the most visible signals on the page. The A-to-z Guarantee - a legally binding commitment under which Amazon reimburses buyers from its own funds if a seller fails to deliver - is present but not prominently headlined at the checkout decision point. The 'Fulfilled by Amazon' (FBA) badge, which signals that Amazon has taken logistical responsibility for the order, appears in the product buy box. These are the two costliest signals in Spence's (1973) terms: both require real contractual obligations that fraudulent actors cannot sustain.

The signals that dominate visually are weaker by Pavlou and Gefen's (2004) framework. 'Amazon's Choice' badge signals editorial authority with undisclosed algorithmic criteria - it is design rhetoric by Head and Hassanein's (2002) definition, present on the product page without an identifiable certifying body. '50+ bought in past month' is social proof with a deliberately vague denominator. Payment logos (Visa, Mastercard, Amazon Pay) appear after login - a first-time visitor on an initial, low-trust visit never reaches these institutional signals before having to decide whether to create an account.

The FBA label makes a specific claim: Amazon has absorbed logistical risk from the third-party seller, meaning the platform's guarantee extends to that order. On non-FBA third-party listings that label is absent and so is that guarantee, leaving seller ratings as the

only institutional indicator. A buyer on an FBA listing and a buyer on a non-FBA listing are dealing with structurally different risk profiles, even when the product page looks similar.

Temu

The checkout page presents 'Alle data er beskyttet' (All data is protected) with a lock icon - a self-stated claim with no external certifying body, functioning as design rhetoric in Head and Hassanein's (2002) sense. 'Stjerneselger' (Star Seller) and '#43 Toppvurdert i Lyd og radio' (Category Top-rated) are internally assigned algorithmic badges with undisclosed criteria. '4.2K+ solgt' (sold count) gives a vague aggregate figure. No third-party security seals appear that a general European consumer would recognise. Every signal on this page originates from Temu itself.

Two stronger signals do appear: 'Leveringsgaranti - Refusjon for ethvert problem' in the global site header, and a 90-day free return policy at checkout. Both would carry real commitment costs if genuinely enforced - the question is whether enforcement is realistic in cross-border e-commerce where the actual sellers are China-based. Session B also flagged something worth considering: when a page stacks as many assurance signals as Temu's does - badges, lock icons, guarantee language, sold counts - there's a risk of tipping into credibility inflation. A surface that needs to assert its trustworthiness this insistently may actually signal that it expects not to be trusted.

Temu also erases individual seller identity. Products are sold by 'forhandleren' (the retailer) - no seller is named by company. The platform absorbs seller identity into its own brand surface. This is structurally different from Amazon: Temu removes the seller while Amazon names the seller alongside its own guarantee.

eBay

eBay's institutional architecture is built at the seller level rather than the platform level. The eBay Money Back Guarantee is legally binding: eBay bears financial liability if a seller fails to deliver, and it extends to third-party seller listings. This is the load-bearing strong mechanism. But it is communicated through brand association rather than prominently headlined on the product page. The dominant visual signals are weak by

Pavlou and Gefen's (2004) framework: seller feedback percentage (98.2% positive), '16 watchers', '5 available · 15 sold', and '104 VIEWED TODAY'.

Ba and Pavlou (2002) found that sellers with higher feedback ratings achieve measurably higher prices on eBay - the reputation signal carries real market weight, not just nominal presence. The listing design makes that priority legible: the feedback score (98.2% positive, 1,568 ratings) sits at the same typographic level as product title and price, more prominent here than on any other platform in this study. The Money Back Guarantee sits beneath all of that as the legally binding floor, covering eBay's liability regardless of what any individual seller does.

'104 VIEWED TODAY' is the weakest element at this layer - an unverifiable metric with no disclosed methodology. The more notable signal is the 'Sweetwater Sound' store banner: Sweetwater is a recognised US audio specialist and this kind of retailer association doesn't show up on any of the other three platforms. Session B's checkout observation: eBay presents only transactionally necessary information at that step, stripping most trust cues. It's a clean checkout rather than a reassurance-heavy one.

Apple Online Store

Apple's institutional layer is the strongest of the four platforms, operating through a fundamentally different mechanism. Apple is a direct seller only - no third-party sellers exist on apple.com. The platform bears full statutory warranty liability under EU/EEA consumer law. AppleCare+ is a priced contractual warranty extension. The 14-day return policy is a legal obligation. These are all costly signals in Spence's (1973) terms - Apple cannot deploy them without accepting legal and financial liability that a fraudulent actor cannot replicate.

Third-party payment logos (Apple Pay, credit cards) appear only at the checkout step, not on the product configuration page. On Amazon or eBay those logos carry active trust work; at Apple they confirm what's already assumed. More notable at this layer are the carrier deal badges on the product configuration page: specific NOK value ranges tied to named Norwegian carriers - Telenor and Telia both appear. Real telecom contracts with named companies are among the more verifiable institutional signals on the page.

AppleCare+ is priced as a product, not offered as a reassurance. Amazon and Temu both foreground buyer protection as a free benefit - something the platform gives you. Apple puts warranty extension behind a paywall. The commercial logic is different: Apple isn't trying to reduce perceived risk through a guarantee headline, because brand authority has already done that work. The statutory minimum is the floor, and the floor is treated as sufficient.

Cross-Platform Comparison

Amazon, eBay, and Apple all have legally binding mechanisms at Layer 2 - the A-to-z Guarantee, the Money Back Guarantee, and statutory warranty respectively. In none of the three cases is that mechanism the most visually prominent element at the decision point. What sits at the top of the visual hierarchy in each case is weaker material: social proof counts, algorithmic badges, self-stated assurances.

Table 2: Layer 2 - Mechanism Strength vs. Mechanism Prominence

Platform	Dominant signal type	Strongest mechanism	Mechanism strength	Strong mechanism prominence
Amazon	Social proof + FBA badge	A-to-z Guarantee	Strong (legally binding)	Low - product page, small print
Temu	Algorithmic badges + lock icon	90-day return / delivery guarantee	Weak-moderate	Low - header, fine print
eBay	Seller feedback score	Money Back Guarantee	Strong (legally binding)	Low - brand association only
Apple	Brand identity	Statutory warranty (direct seller)	Strong (legal obligation)	N/A - no competitor for institutional authority

Apple is the only platform where the strongest mechanism is also the entire institutional identity. The brand cannot be separated from the legal liability. For the other three, the gap between the visual surface and the underlying legal protection is analytically significant: users are presented with weak mechanisms as the primary trust evidence, while strong mechanisms operate in the background.

5.3 Layer 3: Interface-Level Trust - Product Page

Amazon

Amazon's product page is the prototype that the other three platforms are measured against - not because it is the best-designed page in this study, but because it is the most widely imitated. The three-panel layout (image left, product information and buy box right, reviews below) is the dominant Western e-commerce convention. Miniukovich and Figl's (2023) prototypicality research identifies schema-matching as the strongest direct predictor of perceived trustworthiness - and Amazon's layout matches the schema it helped define.

The initial viewport on the observed listing holds approximately twelve distinct elements: product images, title, star rating (4.7 with 2,424 verified reviews), price, fulfilment badges, and a purchase-frequency signal ('50+ bought in past month'). The element count is similar to Temu's but the organisation differs: each item follows from the previous in roughly the sequence a purchase decision runs through, title to quality signal to price to action. On Temu, badges and urgency signals sit at the same level as product details and compete with them.

Fogg et al. (2003) found design look to be the primary credibility channel, but Amazon's above-the-fold credibility doesn't operate through visual polish - it operates through platform recognition. The dark navy navigation, 'Amazon' brand repeated in every badge, and the FBA label create trust through institutional familiarity rather than aesthetic quality. Below the fold, the 'From the manufacturer' editorial section switches to a wider-spaced, image-led format. First-impression credibility comes from platform recognition; once you scroll, deeper product credibility is delegated to seller-provided content, and that varies.

On the observed listing, no countdown timers or scarcity notices appeared. '50+ bought in past month' is social proof with a vague denominator. 'Amazon's Choice' has no disclosed criteria and functions as design rhetoric in Head and Hassanein's (2002) sense. The FBA-accelerated checkout requires account creation, but Amazon's marketplace structure surfaces competing offers on the same product page - the commercial incentive is to be the best host rather than obstruct comparison.

Temu

Seven persuasive cues are identifiable in the initial viewport: 'NESTEN UTSOLGT' (ALMOST SOLD OUT), struck-through RRP of 488 kr against a current price of 345 kr,

‘4.2K+ solgt’ (sales count), ‘Stjerneselger’ (Star Seller), ‘#43 Toppvurdert’ (category ranking), ‘Vårens utvalg’ (Spring selection), and ‘Populære valg’ (Popular choices). No other platform in this study comes close to that count. Three fall into Mathur et al.’s (2019) dark pattern taxonomy: ‘NESTEN UTSOLGT’ is scarcity manipulation, the struck-through RRP is reference price manipulation (it may not reflect any actual prior market price), and the sales count is social proof inflation with no disclosed methodology.

The page’s basic structure is recognisable as e-commerce - image left, information and buy button right. But the badge overlays, orange-and-red promotional colour palette, and stacked scarcity framing push it away from the clean Western product page schema. Miniukovich and Figl (2023) found prototypicality to be the strongest direct predictor of trustworthiness. Apple’s product page departs significantly from standard e-commerce conventions - that should, by the framework, reduce perceived trustworthiness. It doesn’t, because brand recognition overrides the schema-mismatch effect. Prototypicality predicts trustworthiness well for platforms users haven’t encountered before, but once a brand carries enough cultural weight, users don’t evaluate the interface against schema expectations. The absent reviews are the clearest instance: on a seller no one has heard of, zero reviews raises questions. On Apple, users come to the page with a trustworthiness judgment already formed.

There are no persuasive cues on this page because the brand doesn’t need them. The urgency signals and social proof present on the other three platforms are compensating for something - lower brand recognition, weaker institutional signals, or a user who might otherwise hesitate. Apple’s product page doesn’t have that problem, and the design reflects it. Fogg et al. (2003) found design look to be the primary credibility channel; on this page it’s doing all the trust work.

Cross-Platform Comparison

Putting the four pages side by side makes the strategic differences hard to miss - these aren’t variations in execution, they’re different bets about what builds purchase confidence.

Amazon’s page is dense with institutional signals - verified reviews, recognised badges, FBA label, familiar layout - and the trust impression comes from recognising the platform as one that has passed some implicit quality bar. Temu’s page is dense with persuasive cues: high cue count, urgency framing, price manipulation, social proof inflation. The trust

impression - to the extent it exists - comes from purchase momentum rather than quality evidence. eBay deploys peer validation: moderate density, seller-centric layout, feedback scores as the primary trust credential. Apple deploys aesthetic authority: very low density, no social proof, premium design restraint. The trust impression comes from brand recognition expressed through design quality.

Table 3: Layer 3 - Visual Density and Prototypicality

Platform	Elements above fold (approx.)	Prototypicality	Persuasive cue count	Dominant trust strategy
Amazon	~12	High	2 (vague social proof, Amazon's Choice)	Institutional density
Temu	~18	Medium-low	7	Persuasion density
eBay	~10	Medium	2-3 (viewer counts, sold count)	Peer validation
Apple	~5	Medium-low	0	Aesthetic authority

The inverse correlation between persuasive cue density and institutional mechanism strength documented at Layer 2 extends into Layer 3. Temu, with the most persuasive cues, has the weakest institutional layer. Apple, with zero persuasive cues, has the strongest. Amazon and eBay occupy the middle of both dimensions. This correlation supports the trust compensation argument developed in Chapter 6: platforms with weak institutional mechanisms compensate through high-density persuasion at the interface level.

Miniukovich and Figl's (2023) structural equation models put prototypicality as the strongest direct predictor of perceived trustworthiness, ahead of both aesthetics and usability. Table 3 puts Amazon at high prototypicality, eBay at medium, and Temu and Apple both at medium-low. Following the model literally, Amazon should score highest on trustworthiness at the interface layer, with Temu and Apple at the bottom. That prediction holds for three of the four platforms but breaks down for Apple. Apple's medium-low prototypicality score does not produce low perceived trustworthiness - it produces the opposite. Miniukovich and Figl's (2023) framework would predict that Apple's low prototypicality should reduce perceived trustworthiness. The data from Chapter 5 goes the

other way: zero persuasive cues, no reviews, and a non-standard layout correlate with the highest perceived credibility of the four platforms.

Prototypicality predicts trustworthiness through schema-matching: the more a site resembles what users expect from a trustworthy site of that type, the higher their trustworthiness rating. Miniukovich and Figl (2023) note that this effect is category-dependent, and the Apple case suggests it is also familiarity-dependent. Apple users bring a pre-formed trustworthiness judgment to the product page that doesn't depend on schema conformity - the brand recognition substitutes for schema-matching before any interface evaluation begins. What reads as arrogance on an unknown platform (no reviews, no urgency signals, no third-party endorsements) reads as confidence when the brand is globally recognised. This is not a case of trust compensation - Apple is not offsetting a weakness with a strength elsewhere. It is a case where the preconditions for prototypicality to function as a trust predictor do not hold. Prototypicality operates on the assumption that users have no strong prior schema for this specific vendor. For Apple, that assumption fails. The implication for the Layer 3 analysis is that prototypicality is the correct primary criterion for Amazon, Temu, and eBay - platforms whose Layer 3 trust must be built in the moment of first encounter - but secondary to brand-carried trust schemas for a platform like Apple, where the interface layer confirms rather than creates the trust impression.

6 Discussion

Chapter 5 establishes four trust architectures with distinct profiles across the three layers. Amazon runs no regulatory consent mechanism but strong institutional protections. Temu runs the study's most GDPR-compliant consent design alongside its most aggressive interface-level persuasion. eBay builds on seller reputation across all three layers. Apple builds on brand authority expressed through institutional liability and design restraint. This chapter works through three analytical moves from those findings: what the cross-layer interactions reveal about how the layers actually function together, how trust compensation operates and where it breaks down, and what the four platform archetypes suggest for design practice.

6.1 Interactions Between Trust Layers

The framework predicts that the three layers will interact, and the comparative analysis makes it possible to say what those interactions actually look like across the four platforms. The theoretical grounding comes from McKnight et al.'s (2002) distinction between institution-based trust and trusting beliefs - not additive quantities but qualitatively different perceptions that can converge, diverge, or work at odds with one another.

Apple and Temu provide the clearest contrasting cases. Apple's three layers are in tight alignment: no regulatory consent mechanism, very strong institutional liability as a direct seller, and zero persuasive manipulation at the interface level. All three layers carry the same signal - that Apple doesn't need to prove itself. The absence of a cookie banner and the absence of product reviews express the same underlying logic. The consistency isn't incidental; it follows from treating brand authority as a given rather than something the interface needs to construct.

Temu shows the opposite: direct cross-layer tension. Layer 1 is the most GDPR-compliant consent design of the four platforms - symmetric buttons, one-click rejection, advertising cookies off by default. Layer 3 contains the study's highest dark pattern density. The platform with the most privacy-respecting consent dialogue has the most manipulative product page. These layers do not reinforce each other; they contradict. A user who encounters Temu's consent design first and draws conclusions from it about the platform's commercial intentions would be wrong. The two layers are designed by different logics - regulatory compliance pressure at Layer 1, conversion optimisation at Layer 3 - and the resulting tension is visible in the interface.

Amazon shows substitution. Layer 1 is absent: no cookie consent for Norwegian visitors, tracking on by default. Layers 2 and 3 are both strong: the A-to-z Guarantee and Fulfilled-by-Amazon badge at the institutional level, high prototypicality and verified reviews at the interface level. Layers 2 and 3 together carry the trust work that Layer 1 would ordinarily contribute. The substitution is not complete - a user who specifically cares about privacy consent would not be reassured by strong buyer protection - but it is extensive enough to sustain engagement for most users most of the time.

eBay shows moderate reinforcement within its own architecture. The mild visual asymmetry in the consent design (filled Accept vs outlined Decline) is consistent with the marketplace's market-driven trust strategy throughout. The Money Back Guarantee backstops seller reputation just as seller reputation backstops platform credibility. All three layers reflect the same peer-validation model - none of them undercut the others, and the consistency, while producing no single layer of exceptional strength, produces a coherent overall impression.

6.2 Trust Compensation and Asymmetry

Perhaps the most novel analytical claim of the framework is that deficits in one layer can be partially compensated by strengths in another - and that the limits of that compensation are where the analysis gets most interesting. Trust compensation isn't trust: it describes a structural condition in which continued engagement is sustained despite - not because of - trust at one or more layers.

Luguri and Strahilevitz (2021) ran a randomised experiment exposing participants to mild dark patterns, aggressive dark patterns, or none. Users in the mild condition were more than twice as likely to subscribe to a dubious third-party service as those in the control; users in the aggressive condition were nearly four times as likely. But the aggressive condition also produced a backlash effect: participants were more aware that something manipulative had happened and more hostile to the platform as a result. Liu and Gómez-Cruz (2025) followed that backlash through to a stable equilibrium: Temu users who recognise the manipulation, resent it, and continue using the platform because leaving would cost them more. Their term for it is platform cynicism, and it describes continued use without trust - which is a different thing from trust compensation, and a less stable one.

Amazon is the clearest trust compensation case in this study. Its Layer 1 absence is a genuine regulatory deficit - tracking on by default, opt-out buried in account settings, no consent mechanism surfaced to the unauthenticated visitor. This is not a minor asymmetry; it is the complete absence of the consent interface that Nouwens et al.'s (2020) framework and GDPR require. Yet Layer 2 is very strong - A-to-z Guarantee, Fulfilled-by-Amazon, 30-day returns - and Layer 3 is high prototypicality with 2,424 verified reviews on the observed listing. A consumer is maximally protected as a buyer on Amazon despite having

no privacy choice surfaced at the visit level. The compensation is structural: transactional security is doing trust work that regulatory transparency is not doing.

Temu's situation is different and more fragile. What Temu faces is not compensation - it is coexistence of strong regulatory compliance and aggressive commercial manipulation with no mediation between them. Users who encounter both layers are left with contradictory information about what kind of platform they are dealing with. Liu and Gómez-Cruz's (2025) platform cynicism is the outcome: continued use without trust, sustained by price rather than confidence. Platform cynicism is a stable equilibrium, but it is a precarious one. It holds as long as price advantage persists and as long as no competitor offers equivalent pricing with less manipulative design. The arrival of comparable-price competitors or sustained DSA enforcement pressure are the two most plausible routes out of that equilibrium.

Apple illustrates why the concept of compensation requires careful framing. Layer 1 is absent at apple.com/no - no consent mechanism. But Apple's Layer 2 is independently so strong (full statutory liability as direct seller, no third-party seller uncertainty) and Layer 3 so free of manipulation that the Layer 1 absence does not register as a deficit in the same way it does for Amazon. Whether this constitutes compensation or simply strategic irrelevance of Layer 1 is an analytical question. The practical difference is this: for Amazon, a user who specifically values privacy consent would experience a real gap that Layers 2 and 3 partially offset. For Apple, the same user might not register the absence at all, because the brand proposition already carries a privacy implication. The gap exists legally; its experiential weight depends on what the user brings to the interaction.

6.3 Platform Trust Archetypes

Looking across the four platforms, what emerges isn't variation along a single trust quality dimension - it's four structurally distinct trust architectures, each reflecting a different commercial model, brand strategy, and relationship to user autonomy.

Amazon: Systemic trust

Amazon's architecture works through density and redundancy. The regulatory layer reflects the platform's scale and regulatory exposure in its consent design. The institutional layer stacks strong mechanisms - legally binding buyer protection, credit card infrastructure - on top of a large ecosystem of weaker ones: seller ratings, review counts,

fulfilment badges. The interface layer is information-heavy and structurally typical of general e-commerce, with review volume and recency as the primary trust signals. The layers reinforce each other: each one supplies information the others help contextualise. The main vulnerability is review integrity. It is the mechanism most exposed at the interface level and most open to gaming.

Temu: Tension-first trust

Temu's regulatory history in Europe is worth unpacking before the interface analysis. After the European Commission listed it as a very large online platform under the DSA in April 2023 - citing illegal product listings and data handling concerns - the platform was delisted in October 2024 when its active user count dropped below the 45 million threshold, and relisted again in March 2025. For roughly five months of that period Temu was operating without the formal DSA oversight obligations that applied to the other three platforms in this study. The consent interface observed at the time of this study was the most GDPR-compliant of all four platforms - symmetric buttons, one-click rejection, advertising cookies off by default. The product page presented at least seven distinct persuasive cues, including scarcity framing ('NESTEN UTSOLGT'), reference price manipulation, and multiple algorithmic badges with undisclosed criteria. The two layers run directly against each other. Liu and Gómez-Cruz (2025) interviewed Temu users and found people openly describing the platform as untrustworthy while continuing to buy from it - price was the reason given for staying, not any positive evaluation of the platform itself.

eBay: Reputation-centred trust

eBay's trust architecture is built at the seller level rather than the platform level. Seller reputation, aggregated across transactions, is the primary trust instrument - the mechanism Ba and Pavlou (2002) documented and quantified. That puts eBay in a structurally different position from the other three platforms: its credibility rests on a weak mechanism by Pavlou and Gefen's (2004) definition, one that is market-driven rather than legally guaranteed and therefore more exposed to manipulation of feedback scores. The interface layer reflects eBay's C2C context by integrating seller identity directly into the product page - a feature absent from the other three.

Apple: Aesthetic-institutional trust

Apple's trust architecture doesn't separate brand credibility from institutional credibility - they're the same thing. Third-party payment logos appear at checkout because they have to; they don't carry the trust work. Tractinsky, Katz, and Ikar (2000) showed that aesthetic ratings predicted usability ratings both before and after use, while actual usability didn't move aesthetic ratings in return - the relationship runs one way. Robins and Holmes (2008) found the same pattern holds at the content level: identical text rates higher for credibility under better visual presentation. What that means for a product page with Apple's design quality is that credibility is established through the aesthetics before a user consciously processes any institutional signal. Miniukovich and Figl (2023) found prototypicality to be the strongest predictor of trustworthiness in their structural equation models, outweighing aesthetics and usability as independent predictors; Apple's product page is a textbook match for the premium brand retail schema their study used. The ATT rollout in 2021 committed Apple publicly to privacy as a product value, not just a legal posture - a consent design of the kind Nouwens et al. (2020) documented would undercut that in a way that would be hard to miss. The structural vulnerability is the inverse of this strength: the architecture only holds for users who already trust Apple. A first-time visitor with no prior brand exposure receives no consent mechanism, no social proof, and no institutional signals beyond the brand name itself - which, for that user, means nothing.

6.4 Implications for Interaction Design Practice

The Layered Trust Signals framework has practical implications for designers working on commercial interfaces - beyond its analytical application in research. Three design principles follow from the framework's findings.

First: trust architecture is a design choice, not something that emerges by accident. Each of the four platforms made distinct, coherent choices about which layers to invest in and how to configure their interactions. Designers who don't make these choices deliberately will still make them - but the result will reflect the pressures of the design process (conversion optimization, regulatory minimum compliance, aesthetic trend-following) rather than any intentional trust strategy.

Second, layer strength does not transfer across layers. Temu put substantial investment into interface-level persuasion and got platform cynicism rather than trust - the other two layers were too weak for the interface layer to compensate. Apple shows what the other

direction looks like: three layers reinforcing the same proposition, with no layer undermining what the others are doing.

Third, regulatory trust isn't separable from commercial trust. Cookie consent design is typically treated as a compliance exercise, separate from the platform's core commercial design. The analysis suggests the opposite: a consent interface that signals disrespect for user autonomy contaminates the institutional and interface trust signals that follow it. Designers who treat regulatory compliance as a constraint to minimise - rather than as a trust-constructing opportunity - are undermining their own commercial interest in user credibility.

Three specific observations from Chapter 5 ground these principles in observed practice. First, Amazon's Layer 1 absence demonstrates that platforms can sustain conversion without regulatory consent design - but only when Layers 2 and 3 are strong enough to carry the compensating weight. The implication for designers is that cookie consent is not a standalone compliance task; its design quality has consequences for everything that comes after it. Second, Temu's cross-layer tension demonstrates the cost of designing each layer independently. A compliance team producing a GDPR-respecting consent interface and a conversion team producing a dark-pattern product page create a coherent response to two different business pressures - but the result is an interface that sends contradictory signals about what the platform actually values. Third, Apple's Layer 3 restraint demonstrates that the absence of persuasive manipulation is itself a trust mechanism. Designers who treat urgency signals and social proof cues as standard e-commerce furniture should consider that their presence is not neutral - they communicate something about a platform's confidence in its own product, and that communication is received.

7 Contribution and Originality

Five contributions follow from this work. Together, they address the fragmentation in the existing literature and offer a design-applicable analytical framework that currently doesn't exist.

The main research question - how trust signals are structured across regulatory, institutional, and interface levels in contemporary e-commerce platforms - is answered through the comparative analysis in Chapter 5. Each sub-question maps to a section of that analysis: cookie consent design addresses how regulatory trust is constructed or undermined (Section 5.1); payment and checkout pages address how third-party signals function as trust-transfer mechanisms (Section 5.2); product page structure addresses how visual design influences perceived credibility (Section 5.3); and the cross-layer interactions, developed in Chapter 6, address how those layers interact and compensate for one another. The five contributions below follow from those findings.

1. The Layered Trust Signals framework

The main contribution is the Layered Trust Signals framework itself: a design-oriented analytical model that identifies three structurally distinct levels at which trust is constructed in e-commerce interfaces and defines the analytical dimensions relevant to each. Unlike prior trust models that work within a single research domain - institutional trust theory, visual credibility research, or dark pattern scholarship - this framework integrates across disciplines into a unified instrument for comparative interface analysis. It gives interaction designers a vocabulary for discussing trust as a layered design problem rather than a single-construct outcome. In this study, applying the framework revealed findings that neither a dark pattern audit nor a credibility assessment would have produced alone: specifically, that Temu's Layer 1 design and Layer 3 design are designed by entirely different logics and that Amazon sustains conversion without any Layer 1 mechanism at all - both findings are only visible when all three layers are analysed together.

2. The concept of trust compensation

Trust compensation describes the cross-layer dynamics that occur when a deficit in one layer is partially offset by strength in another. The concept isn't present in the existing trust literature, which tends to treat trust dimensions either as additive components of a single construct or as independent variables in separate research programs. Trust compensation, as defined here, isn't the same as high overall trust - it's a structural condition in which engagement is sustained despite trust deficits at one or more layers, with platform cynicism as its limiting case. The concept has implications beyond e-commerce, wherever interfaces are designed to sustain engagement despite legitimate reasons for skepticism. The Chapter 5 analysis gives this concept empirical grounding: Amazon's complete Layer 1 absence is

partially compensated by strong Layers 2 and 3; Temu's cross-layer tension between GDPR-compliant consent and dark-pattern product pages represents the failure mode, where compensation tips into platform cynicism.

3. Comparative characterization of platform trust architectures

The four platforms represent four different answers to the question of how trust is built in an e-commerce interface: systemic trust (Amazon), tension-first trust (Temu), reputation-centred trust (eBay), and aesthetic-institutional trust (Apple). These are not just stylistic differences. Each reflects a set of architectural decisions with traceable consequences for how trust works, and where it fails. The Apple archetype is the analytically least expected: the platform with zero social proof, zero urgency signals, and medium-low prototypicality by Miniukovich and Figl's (2023) standard is also the platform that generates the most automatic trust impression. That finding identifies a boundary condition for prototypicality as a trust predictor - one the framework is now positioned to name.

4. A replicable observation protocol

The observation protocol developed in Chapter 4 and reproduced in Appendix A is designed to be reusable. It is a structured procedure for analysing trust construction in e-commerce interfaces - applicable to other platforms, other time periods, and other regulatory contexts. Its dimensions come from specific empirical literature, which makes it more systematic than an impressionistic credibility audit and gives other researchers a defined starting point for replication or extension.

5. Synthesis of fragmented research

By pulling together foundational trust theory, signalling theory, dark pattern research, visual credibility scholarship, and platform-specific contextual research into a single analytical frame, this thesis does the integrative work that Soleimani (2022) identifies as absent from the field. Interaction designers who need to make decisions across all three trust layers at once have, until now, had no single resource to draw on. The literature is fragmented across disciplines and focused within individual domains.

8 Limitations and Future Research

8.1 Limitations of This Study

Non-empirical scope

The focus here is on how trust is designed, not how it's experienced. The framework identifies design features the literature associates with trust construction or undermining, but doesn't verify that users of these four specific platforms actually respond to them as the literature predicts. Individual variation in prior experience, cultural background, and dispositional trust - what McKnight et al. (2002) call 'disposition to trust' - can't be addressed through interface analysis alone. The claims made are theoretical inferences grounded in empirical literature, not findings from primary data collection.

Snapshot analysis

E-commerce interfaces are subject to continuous modification through A/B testing, regulatory pressure, and competitive dynamics. The analysis reflects interfaces as observed on a specific date and may not accurately represent those interfaces at other points in time. This is a structural limitation of interface analysis as a method, and it's one motivation for the longitudinal approaches outlined in the future research section below.

Scope of case selection

The four platforms were selected for structural diversity, but they don't cover the full range of e-commerce contexts. Vertically specialised retailers, subscription platforms, mobile-native applications, and non-Western platforms all fall outside this study's scope. The trust architectures identified here may not generalise to those contexts, and the observation protocol may need adapting for platforms with substantially different interaction models. More specifically, the framework itself has only been applied to general-purpose retail platforms - it has not been tested on service-based, subscription, or public-sector interfaces, and its three-layer structure assumes a checkout-based transaction model that may not hold in those contexts. That is a constraint on the contributions claimed in Chapter 7, not a direction for future research alone.

Western and European user perspective

The analysis is conducted from a European perspective and applies Western e-commerce prototypicality schemas as its evaluative standards. As Jinchen, Yini, and Kexing (2024) demonstrate, design conventions that read as low-prototypicality or manipulative in Western markets can be entirely standard and familiar in other cultural contexts. The Temu analysis, in particular, requires cross-cultural contextualization that this study can only partially provide - a fuller account would compare the platform's reception across user populations with varying levels of prior exposure to Chinese e-commerce conventions.

Researcher as an analytical instrument

Qualitative interface analysis is inherently interpretive. The observation protocol structures the analysis around theoretically grounded dimensions and reduces the risk of arbitrary interpretation, but it doesn't eliminate the researcher's influence on which features are foregrounded and how they're characterised. Inter-rater reliability assessment - standard in content analysis research - wasn't conducted in this study. Future applications of the observation protocol in empirical research contexts should address this.

8.2 Directions for Future Research

- Empirical validation: user testing in which participants interact with the four platforms and provide trust assessments at each stage would allow the framework's analytical claims to be tested against actual user responses. That would move it from an analytical instrument toward a predictive model.
- Longitudinal tracking: the observation protocol applied repeatedly to the same platforms would show how trust architectures respond to regulatory pressure, competitive moves, and reputational damage - and whether the four archetypes identified here hold over time or shift.
- Mobile interface analysis: mobile e-commerce interfaces work under different constraints - particularly for cookie consent (where screen space forces extreme design choices) and product pages (where limited real estate can amplify the effects of visual density). The observation protocol would need to be adapted for mobile contexts.
- Extension to non-commercial domains: the three-layer framework is not inherently about retail. Public service platforms, healthcare portals, and civic technology applications all face the same problem of constructing trust through design -

through regulatory compliance, institutional affiliation, and visual presentation. Testing the framework in those contexts would reveal where it generalises and where e-commerce-specific assumptions need to be dropped.

- Cross-cultural replication: applying the framework to the same platforms used by users in different cultural contexts - for example, comparing European and East Asian interface versions - would address the cultural limitation identified above and provide a basis for cross-cultural trust architecture comparison.

References

- Ba, S., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behaviour. *MIS Quarterly*, 26(3), 243–268. <https://doi.org/10.2307/4132332>
- Berens, B. M., Bohlender, M., Dietmann, H., Krisam, C., Kulyk, O., & Volkamer, M. (2024). Cookie disclaimers: Dark patterns and lack of transparency. *Computers & Security*. <https://doi.org/10.1016/j.cose.2023.103507>
- Fogg, B. J., Soohoo, C., Danielson, D. R., Marable, L., Stanford, J., & Tauber, E. R. (2003). How do users evaluate the credibility of Web sites? A study with over 2,500 participants. *Proceedings of DUX 2003*. ACM. <https://doi.org/10.1145/997078.997097>
- Gefen, D., Karahanna, E., & Straub, D. W. (2003). Inexperience and experience with online stores: The importance of TAM and trust. *IEEE Transactions on Engineering Management*, 50(3), 307–321. <https://doi.org/10.1109/TEM.2003.817277>
- Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The dark (patterns) side of UX design. *Proceedings of CHI 2018*. ACM. <https://doi.org/10.1145/3173574.3174108>
- Head, M., & Hassanein, K. (2002). Trust in e-commerce: Evaluating the impact of third-party seals. *Quarterly Journal of Electronic Commerce*, 3(3), 307–325.
- Hu, X., Wu, G., & Zhang, C. (2010). The effects of web assurance seals on consumers' initial trust in an online vendor. *Decision Support Systems*, 48(2), 407–418. <https://doi.org/10.1016/j.dss.2009.10.004>
- Jamalifard, M., Russell-Rose, T., & Brignull, H. (2024). Exploring deceptive patterns: Insights from eye tracking, EMG and sentiment analysis. *Proceedings of BCS HCI 2024*. <https://doi.org/10.14236/ewic/BCSHCI2024.20>

- Jinchen, J., Yini, S., & Kexing, P. (2024). E-commerce platform mobile interface experience design from a cross-cultural perspective. *Cross-Cultural Design*. Springer. https://doi.org/10.1007/978-3-031-60904-6_19
- Kocyigit, E., Rossi, A., & Lenzini, G. (2023). Towards assessing features of dark patterns in cookie consent processes. *Privacy and Identity Management*. Springer. https://doi.org/10.1007/978-3-031-31971-6_13
- Lindgaard, G., Fernandes, G., Dudek, C., & Brown, J. (2006). Attention web designers: You have 50 milliseconds to make a good first impression! *Behaviour & Information Technology*, 25(2), 115–126. <https://doi.org/10.1080/01449290500330448>
- Liu, S., & Gómez-Cruz, E. (2025). “Temu is evil, but I still use it”: Platform cynicism in platform capitalism. *New Media & Society*. <https://doi.org/10.1177/14614448251365269>
- Luguri, J., & Strahilevitz, L. J. (2021). Shining a light on dark patterns. *Journal of Legal Analysis*, 13(1), 43–109. <https://doi.org/10.1093/jla/laaa006>
- 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). <https://doi.org/10.1145/3359183>
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review*, 20(3), 709–734. <https://doi.org/10.5465/amr.1995.9508080335>
- Mayayise, T. O. (2024). Investigating factors influencing trust in C2C e-commerce environments. *Data and Information Management*, 8(1). <https://doi.org/10.1016/j.dim.2023.100056>
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce. *Information Systems Research*, 13(3), 334–359. <https://doi.org/10.1287/isre.13.3.334.81>
- Miniukovich, A., & Figl, K. (2023). The effect of prototypicality on webpage aesthetics, usability, and trustworthiness. *International Journal of Human-Computer Studies*, 177. <https://doi.org/10.1016/j.ijhcs.2023.103103>

- Miniukovich, A., Figl, K., & Ernst, C. (2024). The effects of webpage prototypicality, aesthetics, and complexity on eye fixations and company perception. *Information Systems and Neuroscience*. Springer. https://doi.org/10.1007/978-3-031-58396-4_24
- Nie, L., Zhao, Y., Li, C., Luo, X., & Liu, Y. (2024). Shadows in the interface: A comprehensive study on dark patterns. *Proceedings of the ACM on Software Engineering*. <https://doi.org/10.1145/3643736>
- Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. *Proceedings of CHI 2020*. ACM. <https://doi.org/10.1145/3313831.3376321>
- Papenmeier, F., Halama, J., & Reichert, C. (2025). Accepting cookies: Nudging, deceptive patterns and personal preference. *Computers in Human Behavior*. <https://doi.org/10.1016/j.chb.2025.108641>
- Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with institution-based trust. *Information Systems Research*, 15(1), 37–59. <https://doi.org/10.1287/isre.1040.0015>
- Peña-García, N., Losada-Otálora, M., Auza, D. P., & Cruz, M. P. (2024). Reviews, trust, and customer experience in online marketplaces. *Frontiers in Communication*. <https://doi.org/10.3389/fcomm.2024.1460321>
- Robins, D., & Holmes, J. (2008). Aesthetics and credibility in web site design. *Information Processing & Management*, 44(1), 386–399. <https://doi.org/10.1016/j.ipm.2007.02.003>
- Soleimani, M. (2022). Buyers' trust and mistrust in e-commerce platforms: A synthesising literature review. *Information Systems and e-Business Management*, 20, 1–32. <https://doi.org/10.1007/s10257-021-00545-0>
- Spence, M. (1973). Job market signalling. *The Quarterly Journal of Economics*, 87(3), 355–374. <https://doi.org/10.2307/1882010>
- Tractinsky, N., Katz, A. S., & Ikar, D. (2000). What is beautiful is usable. *Interacting with Computers*, 13(2), 127–145. [https://doi.org/10.1016/S0953-5438\(00\)00031-X](https://doi.org/10.1016/S0953-5438(00)00031-X)

Wang, J., Shahzad, F., Ahmad, Z., Abdullah, M., & Hassan, N. M. (2022). Trust and consumers' purchase intention in a social commerce platform. *SAGE Open*. <https://doi.org/10.1177/21582440221091262>

Appendix A: Observation Protocol

The following protocol was applied systematically to each of the four platforms examined in Chapter 5. Dimensions are derived from the theoretical framework developed in Chapter 3.

Layer 1 - Regulatory Trust: Cookie Consent

1. Reject availability: Is a 'reject all' or equivalent option present at the top level of the consent dialogue, without requiring navigation into a sub-menu?
2. Button hierarchy: Are the accept and reject options presented with equivalent visual weight - equivalent size, colour prominence, and positional emphasis?
3. Label wording: What are the exact labels used on the accept and reject options?
4. Granularity: Does the interface offer category-level consent controls (e.g. analytics, marketing, functional) accessible at the first level of interaction?
5. Steps to reject: How many distinct interaction steps are required to reject all non-essential cookies?
6. Default state: Are any non-essential cookie categories pre-selected by default?

Layer 2 - Institutional Trust: Checkout and Payment

7. Payment logos: Which payment provider logos are displayed, and at what point in the checkout flow are they made visible?
8. Buyer protection: Is a buyer guarantee or money-back promise displayed? How specifically is the commitment described, and how prominent is it?
9. Return policy: Is the return policy visible on or near the checkout page without requiring navigation away?
10. Seller identity: Is the seller's identity clearly displayed and distinguished from the platform identity?
11. Assurance seals: Are third-party certification or security seals present? Are the certifying bodies recognisable to a general European consumer?

12. Mechanism strength: Are the dominant institutional mechanisms weak (market-driven, e.g. ratings) or strong (legally binding, e.g. buyer guarantees with defined commitments)?

Layer 3 - Interface-Level Trust: Product Page

13. Visual density: How many distinct interactive or informational elements are visible in the initial viewport without scrolling?
14. Colour strategy: How is colour used - for brand identity, urgency signalling, neutral information organisation, or a combination?
15. Information hierarchy: In what sequence does the page present product name, price, star rating, review count, and product description?
16. Review prominence: Where is the star rating and review count positioned relative to product title and price?
17. Persuasive cues: Are scarcity messages (e.g. 'only 3 left'), urgency countdowns, or social proof indicators (e.g. 'X people bought this today') present?
18. Prototypicality: Does the overall page layout match the conventions of mainstream Western e-commerce product pages for this product category?

Appendix B: Interface Screenshots

Amazon

Figure B.1 - Amazon: Cookie consent / absent dialogue (Layer 1)

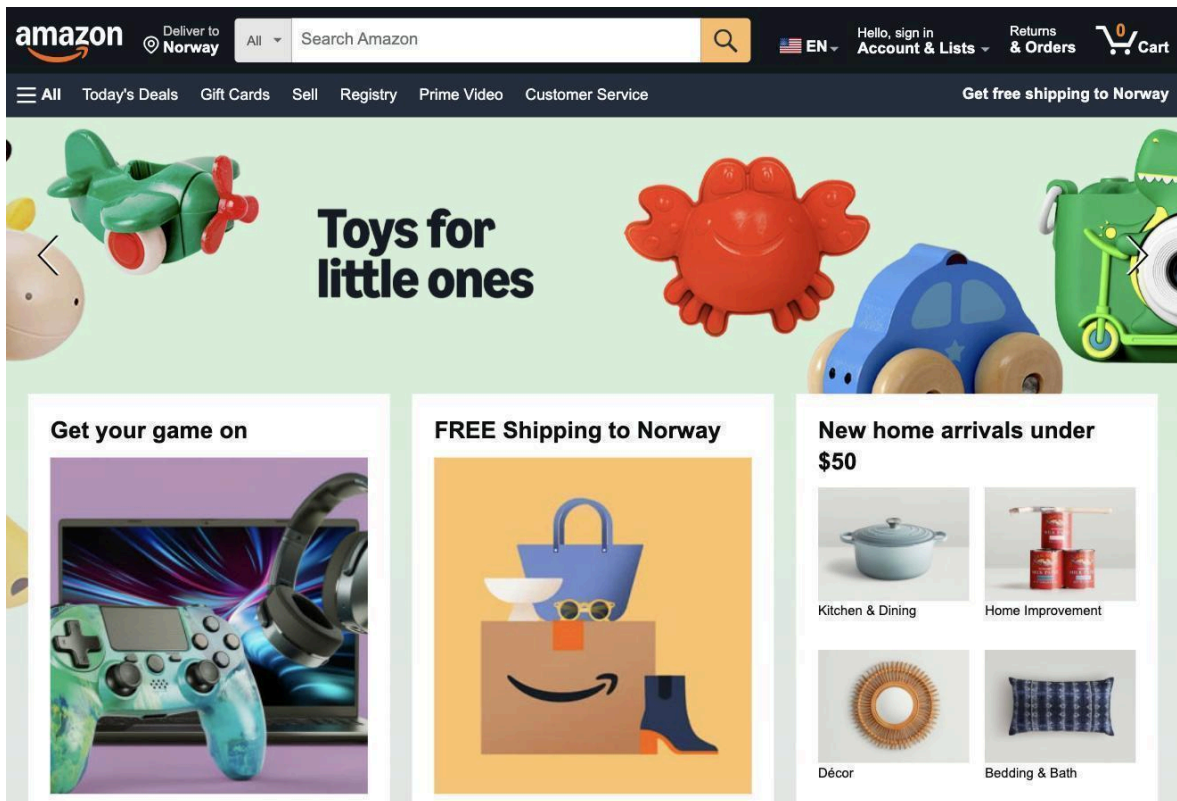


Figure B.1. Amazon: no cookie consent dialogue on first load. amazon.com, Session A, 19 May 2026. Confirms absence of any consent mechanism for unauthenticated visitors. Referenced in Section 5.1.

Figure B.2 - Amazon: Account-level opt-out in settings (Layer 1 supplementary)

All

amazon for shopping

Free Shipping Zone

Today's Deals

Buy Again

Mathias's Amazon.com

Browsing History -

Gift Cards

Customer Service

Get free shipping to Norway

Help & Customer Service

All Help Topics

Security and Privacy

Amazon and Your Personal Information

Additional State-Specific Privacy Disclosures

How Amazon Uses Your Personal Information

How Amazon Collects Your Personal Information

How Amazon Protects Your Personal Information

Manage Your Personal Information

Interest-Based Ads

EU-US Data Privacy Framework, UK Extension, and Swiss-US Data Privacy Framework

About Cookies

California Supply Chain Transparency Act Statement

Human Rights and Environmental Grievances

Law Enforcement Information Requests

Request your personal information

Communications from Amazon.com

Legal Policies

Your Security

Report Unsolicited Packages or Brushing Scams

How to keep your account safe and secure

How to Obtain Amazon Transaction Records After Identity Theft

Customer Service History

Find more solutions

Search our help content

Q Search our help content

Security and Privacy

Cookies

Last updated: January 1, 2020

We use cookies, pixels, and other technologies (collectively, "cookies") to recognize your browser or device, learn more about your interests, and provide you with essential features and services and for additional purposes, including:

- Recognizing you when you sign-in to use our services. This allows us to provide you with product recommendations, display personalized content, recognize you as a Prime member, enable you to use 1-Click purchasing, and provide other customized features and services.
- Keeping track of your specified preferences. This allows us to honor your preferences, such as whether or not you would like to see interest-based ads. You may set your preferences through [Your Account](#).
- Keeping track of items stored in your shopping basket.
- Conducting research and diagnostics to improve Amazon's content, products, and services.
- Preventing fraudulent activity.
- Improving security.
- Delivering content, including ads, relevant to your interests on Amazon sites and third-party sites (see the [Interest-Based Ads notice](#) for how we use cookies in serving interest-based ads).
- Reporting. This allows us to measure and analyze the performance of our services.

Amazon's cookies allow you to take advantage of some of Amazon's essential features. For instance, if you block or otherwise reject our cookies, you will not be able to add items to your Shopping Cart, proceed to Checkout, or use any Amazon products and services that require you to sign in.

Approved third parties may also set cookies when you interact with Amazon services. Third parties include search engines, providers of measurement and analytics services, social media networks, and advertising companies. Third parties use cookies in the process of delivering content, including ads relevant to your interests, to measure the effectiveness of their ads, and to perform services on behalf of Amazon.

You can manage browser cookies through your browser settings. The 'Help' feature on most browsers will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie, how to block cookies, and when cookies will expire. If you block all cookies on your browser, neither we nor third parties will transfer cookies to your browser. If you do this, however, you may have to manually adjust some preferences every time you visit a site and some features and services may not work. Some mobile operating systems may further limit the use of cookies and similar technologies; your choices do not override those more limited settings on such mobile devices.

See our [Privacy Notice](#) for more information about the types of information we gather.

Was this information helpful?

Yes No

Quick solutions

Your Orders
Track or cancel orders

Returns & Refunds
Exchange or return items

Manage Prime
Cancel or view benefits

Payment Settings
Add or edit payment methods

Carrier Info
Shipping carrier information

Figure B.2. Amazon: account-level opt-out in privacy settings, accessible only after login. amazon.com, Session A, 19 May 2026. Demonstrates that the opt-out is located in account settings rather than surfaced at the point of entry. Referenced in Section 5.1.

Figure B.3 - Amazon: Checkout / payment page (Layer 2)



Sign in or create account

Enter mobile number or email

Continue

By continuing, you agree to Amazon's [Conditions of Use](#) and [Privacy Notice](#).

[Need help?](#)

Buying for work?

[Create a free business account](#)

[Conditions of Use](#) [Privacy Notice](#) [Help](#)
 © 1996-2026, Amazon.com, Inc. or its affiliates



Deliver to Mathias
 Blomsterd... 5258

EN
Hello, Mathias
Account & Lists
Returns & Orders
Cart

All
[alexa for shopping](#)
Free Shipping Zone
Today's Deals
Buy Again
Mathias's Amazon.com
Browsing History
Gift Cards
Customer Service
Sell
Prime Video
Get free shipping to Norway

Shopping Cart

[Deselect all items](#)

☒


JBL Flip 6 - Portable Bluetooth Speaker, powerful sound and deep bass, IPX7 waterproof, 12 hours of playtime, JBL PartyBoost for multiple speaker pair...

FREE International Returns

☐ This is a gift [Learn more](#)

Style: Flip 6

🛒
1
+

[Delete](#) | [Save for later](#) | [Compare with similar items](#) | [Share](#)

Subtotal (1 item): **\$88.99**

Your Items

No items saved for later [Buy it again](#)

No items

Subtotal (1 item): \$88.99

☐ This order contains a gift

Proceed to checkout

 Enjoy fast, **FREE** delivery on eligible items with a 30-day trial for \$0

Try Prime FREE

Free Shipping on International Top Sellers for you



HOTNOW Short USB ...

★ ★ ★ ★ ☆ 1,616

\$8⁹⁹ (\$3.00/count)

Delivery Thu, Jun 11

Add to cart



TOSOWOONG Arbuti...

★ ★ ★ ★ ☆ 5,569

\$25⁰⁰

(\$14.79/fluid ounce)

Delivery Thu, Jun 11

The price and availability of items at Amazon.com are subject to change. The Cart is a temporary place to store a list of your items and reflects each item's most recent price. [Learn more](#)

Do you have a gift card or promotional code? We'll ask you to enter your claim code when it's time to pay.

Figure B.3. Amazon: checkout / payment page showing payment methods and order summary (before and after login). amazon.com, Session B, 19 May 2026. Shows payment provider logos and fulfilment information at the checkout step. Referenced in Section 5.2.

Figure B.3a - Amazon: Buyer protection display (Layer 2)

Product information

Additional details

Sound Quality

Connectivity

Battery details

Warranty & Support

Amazon.com Return Policy: Amazon.com Voluntary 30-Day Return Guarantee: You can return many items you have purchased within 30 days following delivery of the item to you. Our Voluntary 30-Day Return Guarantee does not affect your legal right of withdrawal in any way. You can find out more about the exceptions and conditions [here](#).

Product Warranty: For warranty information about this product, please [click here](#)

Feedback

Would you like to [tell us about a lower price?](#)

Item details

Power

Measurements

Compatibility

Power Source

Audio Hardware

Figure B.3a. Amazon: buyer protection display at checkout showing the A-to-z Guarantee and return policy. amazon.com, Session B, 19 May 2026. Documents placement and prominence of the platform’s legally binding buyer guarantee. Referenced in Section 5.2.

Figure B.4 - Amazon: Product page above the fold (Layer 3)

amazon

Deliver to Norway

Electronics

Search Amazon

EN

Hello, sign in Account & Lists

Returns & Orders

Cart

All

Today's Deals

Gift Cards

Sell

Registry

Prime Video

Customer Service

Get free shipping to Norway

Home Audio & Theater

Premium Audio

Headphones

Home Theater Systems

Speakers

Wireless Audio

Stereo System Components

Accessories

Electronics > Portable Audio & Video > Portable Speakers & Docks > Portable Bluetooth Speakers

JBL

Flip 6

Portable Bluetooth Speaker, powerful sound and deep bass, IPX7 waterproof, 12 hours of playtime, JBL PartyBoost for multiple speaker pairing for home, outdoor and travel (Red)

Visit the JBL Store

4.7 (2,424)

Amazon's Choice

50+ bought in past month

NOK825⁶²

FREE International Returns

NOK 581.43 Shipping & Import Charges to Norway

Details

Sales taxes may apply at checkout

Buy used: NOK 825.62

NOK 300.04 delivery June 10 - 18

Deliver to Norway

Used: Like New | Details

Sold by Power Up Deals

Fulfilled by Amazon

Add to cart

Add to List

Other sellers on Amazon

Used (2) from NOK825⁶²

Figure B.4. Amazon: product page above the fold for the observed JBL speaker listing. amazon.com, Session B, 19 May 2026. Shows the three-panel layout, star rating, review count, FBA badge, and social proof signal. Referenced in Section 5.3.

Figure B.5 - Amazon: Review / ratings section (Layer 3)

↑ Top About this item Similar Product information From the Brand **Review** JBL Flip 6 - Portable Bluetooth Speaker, powerful sound and...

★★★★★ 4.7 out of 5
2,424 global ratings

5 star 86%
4 star 7%
3 star 3%
2 star 1%
1 star 3%

How customer reviews and ratings work ▼

JBL Flip 6 - Portable Bluetooth Speaker, po...
★★★★★ 21,602
NOK 868.65 ✓prime [Shop now](#)
Sponsored

Top reviews from the United States

Sebastian
★★★★★ **Works as intended**
Reviewed in the United States on March 17, 2026
Style: Flip 6 | **Verified Purchase**
Man this speakers the bees knees when it comes to durability, I've dropped it, submerged it, kicked it, rolled it etc. I work in a kitchen so the thing takes a beating. Size is great, music sounds nice, value is perfect, battery lifes good i get about 9 - 10 hours with a full charge. Would recommend.
[Helpful](#) [Report](#)

Brian
★★★★★ **Sounds Great and lasts all day**
Reviewed in the United States on February 11, 2026
Style: Flip 6 | **Verified Purchase**
Sounds amazing, Battery lasts way longer than expected, It's in a backpack perfectly. Im a rock and metal guy and it come out sounding balanced and clear. Connects easy and stays

Subtotal: NOK 82
[Go to cart](#)

Figure B.5. Amazon: review and ratings section for the observed listing. amazon.com, Session B, 19 May 2026. Shows verified review count, rating breakdown, and review recency. Referenced in Section 5.3.

Temu

Figure B.6 - Temu: Cookie consent dialogue, initial state (Layer 1)

Gratis levering Utrolig
Leveringsgaranti Refusjon for ethvert problem
Få Temu-appen

Bestselgende varer 5-stjerner Kategorier Søk i Temu

Bestilling er og ... Norsk bokmål

Innstillinger for personvern og informasjonskapsler

Vi bruker informasjonskapsler og lignende teknologier for å levere tjenesten vår, gi deg den beste opplevelsen, forbedre og annonsere tjenesten, sikre at den er trygg og sikker for brukere og måle effektiviteten av reklamekampanjer. Hvis du velger «Godta alle», godtar du at vi og partnerne vi jobber med lagrer informasjonskapsler og lignende teknologier på enheten din for reklameformål. Du kan også «Avvise alle» informasjonskapsler som ikke er helt nødvendige, eller velge hvilke typer informasjonskapsler du ønsker å godta eller deaktivere ved å klikke på «Tilpass informasjonskapsler» nedenfor eller når som helst under dine personverninnstillinger. For mer informasjon, se våre retningslinjer for informasjonskapsler og lignende teknologier.

[Tilpass informasjonskapsler](#) [Avvis alle](#) [Godta alle](#)

Utvalg 1 stk (1 stk) Vanntett ... 105 kr 22K+ solgt 1 481
Utvalg WB Voldemort Bursda... 31 kr 9,7K+ solgt RRP 36 kr
Oppvaskmaskinmagneter, 1... 20 kr 76K+ solgt Laveste siste pris: 37 kr
Utvalg Håndholdt frøing og jo... 23 kr 81K+ solgt Toppvurdert i Hagever...
Utvalg Golfswingtrenerarmbå... 55 kr 43K+ solgt RRP 57 kr
Bestselgende vare i Golf 768
Utvalg 2 stk Gjenbrukbare Sil... 25 kr 17K+ solgt

Figure B.6. Temu: cookie consent dialogue in initial state on first load. temu.com/no, Session A, 21 May 2026. Shows symmetric accept and reject buttons and initial cookie category state. Referenced in Section 5.1.

Figure B.7 - Temu: Cookie preferences layer showing advertising cookies off by default (Layer 1)

Cookie preference

You can change your cookie settings to accept or refuse certain cookies and similar technologies below. Remember, you can customise your cookie settings at any time in your privacy settings. To learn more about the cookies we use, see our [Cookie and Similar Technologies Policy](#).

^ Essential cookies

Always on

These cookies are necessary and required to provide our Service. For example, we use cookies to display products relevant to your language and region, to ensure the security of our Service, to differentiate users, and to support various functionalities of our website and App. For more details, see our [Cookies and Similar Technologies Policy](#).

^ Advertising cookies

☐

These cookies are used to deliver you personalised advertising including that is appropriate and relevant to your region and language. These cookies are also used to track the advertisements that are shown to you and to assist with advertising measurement and reporting. We use both first-party advertising cookies, and third-party cookies. Advertising cookies are optional. For more details, see our [Cookies and Similar Technologies Policy](#).

First-Party Advertising Cookies

☐

^ Third-Party Advertising Cookies

☐

Confirm my choice

Figure B.7. Temu: cookie preferences layer showing advertising cookies set to off by default. temu.com/no, Session A, 21 May 2026. Documents the default toggle state for advertising cookies at the manage-preferences level. Referenced in Section 5.1.

Figure B.8 - Temu: Named third-party vendor disclosure in advertising cookies layer (Layer 1)

^ Third-Party Advertising Cookies

Customise Third-Party Advertising Cookies: You can allow third parties to display advertisements to you, as well as measure and optimise the effectiveness of those advertisements.

ADman Media ads

Adjust

BidMachine ads

Bidease ads

Bing ads

Criteo ads

Digital Turbine ads

Eskimi ads

Facebook ads

Facebook event

Google ads	☐
-------------------	--------------------------

Google firebase analytics	☐
----------------------------------	--------------------------

Index Exchange ads	☐
---------------------------	--------------------------

Lenovo ads	☐
-------------------	--------------------------

LoopMe ads	☐
-------------------	--------------------------

Opera ads	☐
------------------	--------------------------

Outbrain ads	☐
---------------------	--------------------------

Pinterest ads	☐
----------------------	--------------------------

PubMatic ads	☐
---------------------	--------------------------

Smaato ads	☐
-------------------	--------------------------

Snapchat ads	☐
---------------------	--------------------------

Startio ads	☐
--------------------	--------------------------

Taboola ads	☐
TikTok ads	☐
Verve ads	☐
Videoheroes ads	☐
Vungle ads	☐
X ads	☐

Confirm my choice

Figure B.8. Temu: named third-party vendor disclosure in the advertising cookies preferences layer. *temu.com/no*, Session A, 21 May 2026. Shows the list of named advertising partners disclosed at this level of the consent flow. Referenced in Section 5.1.

Figure B.9 - Temu: Checkout / payment page (Layer 2)

 All informasjon vil bli kryptert

Logg på / Registrer deg

Alle data er beskyttet

Gratis levering

Utrolig

Gratis retur

Opptil 90 dager

E-post eller telefonnummer

Fortsett

Problemer med å logge inn?

Eller fortsett på andre måter

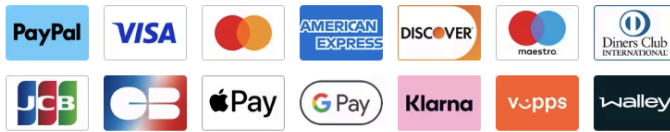




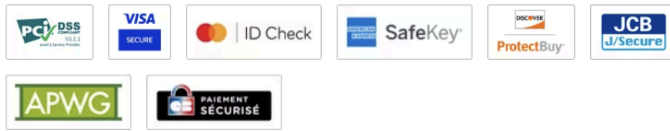


Ved å fortsette godtar du vår [Brukervilkår](#) og erkjenner at du har lest vår [Retningslinjer for personvern](#).

1. Betalingsmåter



2. Sikkerhetssertifisering



Sikkert personvern

Å beskytte personvernet ditt er viktig for oss! Du kan være trygg på at informasjonen din holdes trygg og ukompromittert. Vi selger ikke personopplysningene dine for penger, og vil kun bruke opplysningene i samsvar med våre retningslinjer for personvern og informasjonskapsler for å levere og forbedre våre tjenester til deg.

Lære mer >

Temu kjøpsbeskyttelse

Handle trygt hos Temu og vit at dersom noe skulle gå galt, vil vi alltid hjelpe deg.

Se programvilkår >

Leveringsgaranti

- ✓ Kreditt på 50 kr for forsinkelse
- ✓ Refusjon for 15 dager uten oppdateringer
- ✓ Returner hvis varen er skadet
- ✓ Refusjon for 30 dager uten levering

Finn ut mer >

Temus treplantingsprogram >

Figure B.9a. Temu: buyer protection display showing the delivery guarantee and return policy. *temu.com/no*, Session B, 21 May 2026. Documents placement and wording of the platform's guarantee claims. Referenced in Section 5.2.

Figure B.10 - Temu: Product page above the fold (Layer 3)

Gratis levering > Utrolig

Prisjustering Innen 30 dager

Få Temu-appen

Begynn å selge til millioner av kjøpere på Temu

Bil med nå >

TEMU

Bestselgende varer

5-stjerner

Kategorier

Bluetooth speaker

Hjem > Elektronikk > Lyd og radio > JBL GO ESSENTIAL 2. genera...

JBL

Ankommer NO på så kort tid som **4 virkedager** JBL GO ESSENTIAL 2. generasjon oppgradert høyttaler, Ungdomsversjon av Music Brick 2. generasjon, Lettvekts bærbar trådløs høyttaler for utendørs, løping, sport, trening, fjellklatring, kraftig og kraftfull bass. Ladekabel, koble til mobiltelefon/nettbrett/TV. Passer til hjem, bil, utendørs, camping

Merke: JBL >

4,2K+ solgt | Selges av forhandleren — **Stjerneselger** > 4,8★★★★★

#43 Toppvurdert i Lyd og radio >

345 kr RRP 488 kr Mva. er inkludert

Betal 0 kr i dag > Hva er RRP >

Varens utvalg ✓ Gratis frakt | ✓ Kreditt på 50 kr for forsinkelse >

Farge

[Svart] [Blå] [Rød]

Velg et alternativ

366 anmeldelser | 4,8★★★★★

Alle vurderinger er fra verifiserte kjøp

Delsum 512 kr

Gratis frakt

Kasse (1)

Gå til handlekurv

Velg alle (1)

512 kr

1

Meldinger

Tilbakemelding

Figure B.10. Temu: product page above the fold for the observed speaker listing. temu.com/no, Session B, 21 May 2026. Shows the full set of persuasive cues in the initial viewport, including scarcity framing and reference price manipulation. Referenced in Section 5.3.

Figure B.11 - Temu: Review / ratings section (Layer 3)

366 anmeldelser | 4,8 ★ ★ ★ ★ ★

 Alle vurderinger er fra verifiserte kjøp

Anbefalt ?

Seneste



Людмила Болотова i  13. des 2025



Høytaleren er veldig fin, kobles til raskt, har god kvalitet og gir en lyd av høy kvalitet



ra***hi i  2. okt 2025



Alt er fantastisk, det ser bra ut og har en utrolig god lyd... Jeg er veldig fornøyd.



snt i  14. mai 2026



Perfekt og original! Jeg hadde den dyre JBL 3-versjonen, og dette er den andre. Den er like bra, med klar og kraftig lyd, og den er mindre og enklere å håndtere. Takk til selgeren! 🙏👍



Mamorapeli Ramelamu i  1. mai 2026



 Elsker den! Så lett å ta med seg og så søt. Og kvaliteten er helt perfekt

Se alle vurderinger

Figure B.11. Temu: review and ratings section for the observed listing. *temu.com/no*, Session B, 21 May 2026. Shows star rating, review count, and review display format. Referenced in Section 5.3.

Figure B.12 - Temu: Page footer showing security certifications and accepted payments (Layer 2/3)

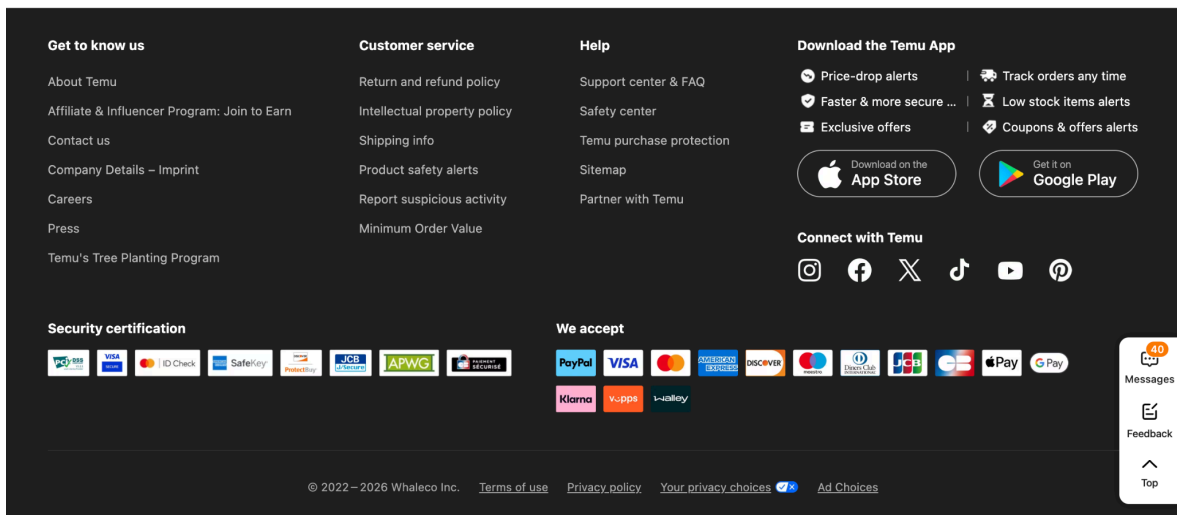


Figure B.12. Temu page footer (temu.com/no), Session B, 26 May 2026. Shows security certification logos, accepted payment methods (PayPal, Visa, Mastercard, Klarna, etc.), and order guarantee links. Referenced in Sections 5.2 and 5.3.

eBay

Figure B.13 - eBay: Cookie consent banner (Layer 1)

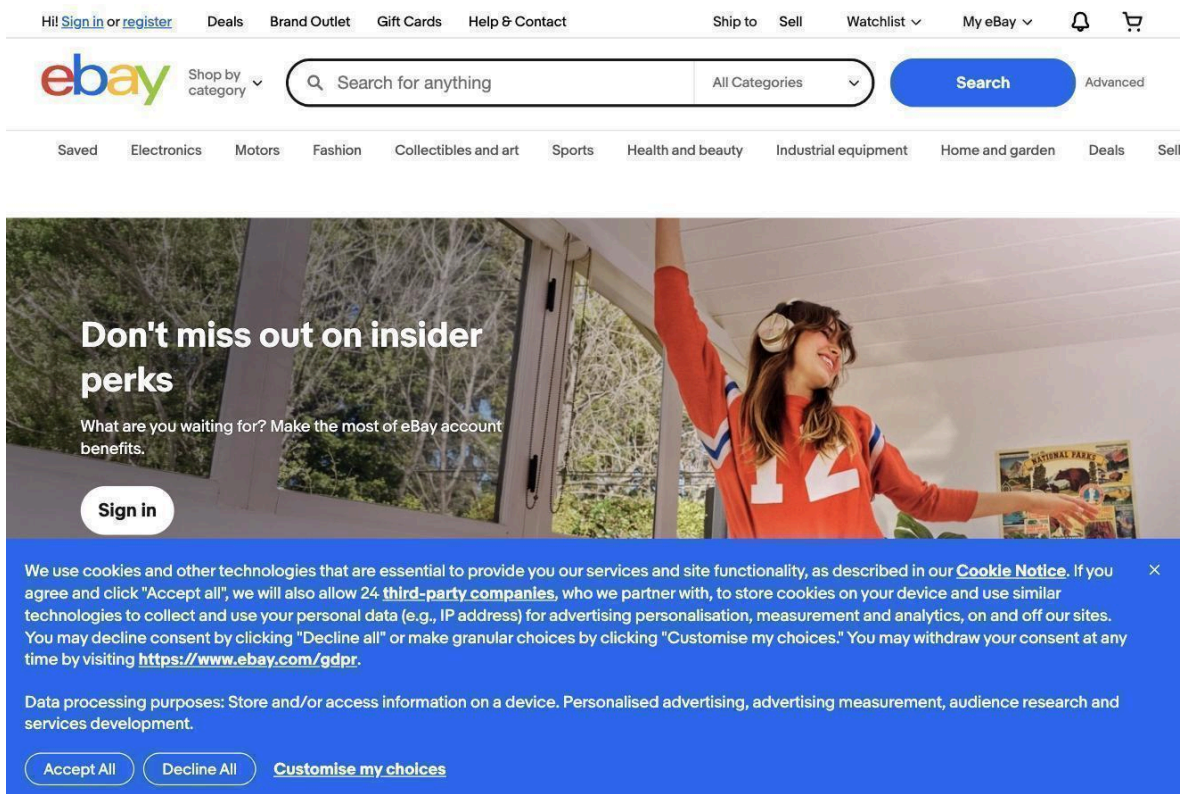


Figure B.13. eBay: cookie consent banner on first load. ebay.com, Session A, 23 May 2026. Shows button hierarchy with filled Accept and outlined Decline options. Referenced in Section 5.1.

Figure B.13a - eBay: Cookie preferences / manage layer (Layer 1)

Hi! [Sign in](#) or [register](#) Deals Brand Outlet Gift Cards Help & Contact Ship to Sell Watchlist My eBay

ebay Shop by category Search for anything All Categories Search Advanced

Advertising and related preferences

These settings are intended to help our customers in the European Economic Area (EEA) and the United Kingdom control the placement and use of cookies and similar technologies by third-party companies, who we partner with to process your data (including personal data, e.g., IP address) for advertising and content personalisation, measurement and analytics purposes.

What information is being used?

- **IP addresses:** Your IP address is a number assigned by your Internet Service Provider to any Internet connection. It is not always specific to your device and is not always a stable identifier. It is used to route information on the Internet and display online content (including ads) on your connected device.
- **Device characteristics:** Technical characteristics about the device you are using that are not unique to you, such as the language, the time zone or the operating system.
- **Device identifiers:** A device identifier is a unique string of characters assigned to your device or browser by means of a cookie or other storage technologies. It may be created or accessed to recognise your device e.g. across web pages from the same site or across multiple sites or apps.
- **Probabilistic identifiers:** A probabilistic identifier can be created by combining characteristics associated with your device (the type of browser or operating system used) and the IP address of the Internet connection. If you give your agreement, additional characteristics (e.g. the installed font or screen resolution) can also be combined to improve precision of the probabilistic identifier. Such an identifier is considered "probabilistic" because several devices can share the same characteristics and Internet connection. It may be used to recognise your device across e.g. web pages from the same site or across multiple sites or apps.

Figure B.13a. eBay: cookie preferences / manage layer. ebay.com, Session A, 23 May 2026. Shows category-level controls available at the manage-preferences level of the consent flow. Referenced in Section 5.1.

Figure B.14 - eBay: Checkout / payment page (Layer 2)

 Checkout

How do you like our checkout? [Give us feedback](#)
Have an account? [Sign in](#)

Review order

**primecart-uk**
98.2% positive feedback



Flip 6 Bluetooth Portable Speaker System - Black ✓
Colors: Black
GBP 52.47

Quantity
1

Returns accepted

Delivery
Est. delivery: Jun 3 – Jun 17
International Priority Shipping ⓘ
GBP 17.11
Includes international tracking

Import charges ⓘ
No additional import charges at delivery
GBP 20.03

Order Summary

Item (1)	GBP 52.47
Shipping	GBP 17.11
Import charges	GBP 20.03
Order total	GBP 89.61

Confirm and pay

Enter shipping address

 Purchase protected by [eBay Money Back Guarantee](#)

Figure B.14. eBay: checkout / payment page showing payment methods and buyer protection information. ebay.com, Session B, 23 May 2026. Shows payment provider logos and Money Back Guarantee positioning at checkout. Referenced in Section 5.2.

Figure B.14a - eBay: Buyer protection display (Layer 2)

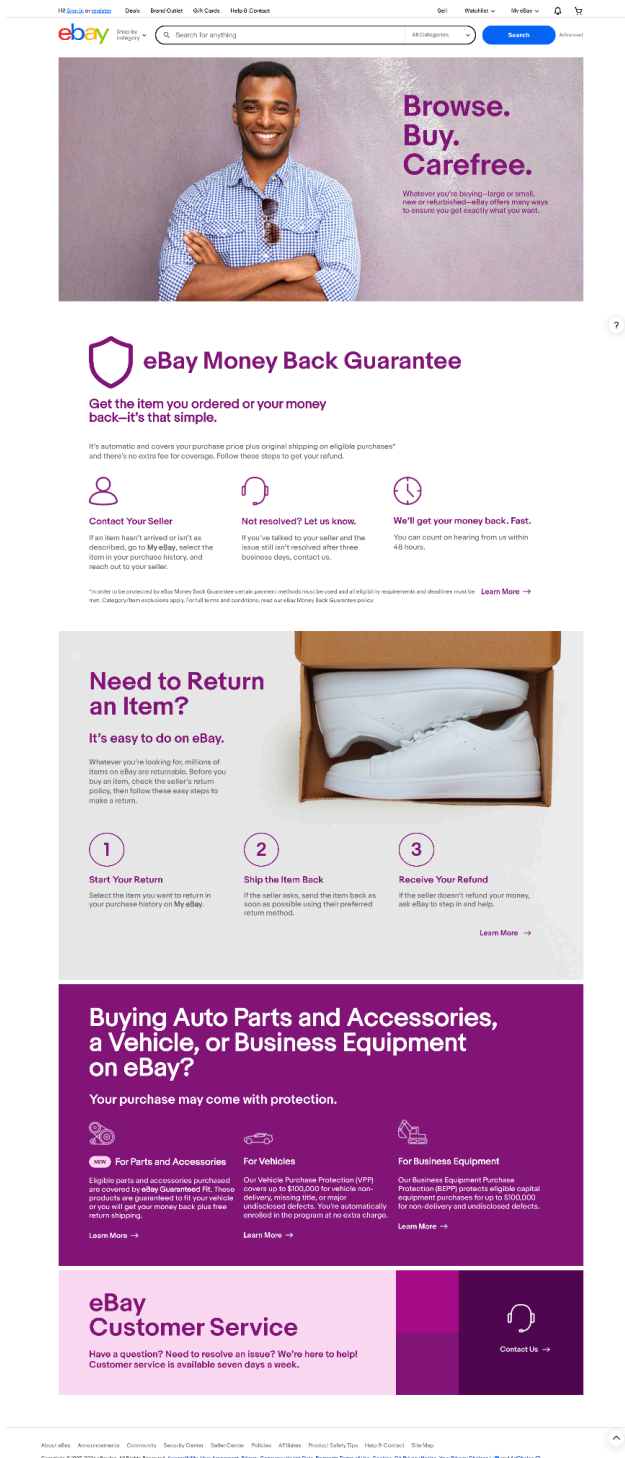


Figure B.14a. eBay: buyer protection display showing Money Back Guarantee messaging. ebay.com, Session B, 23 May 2026. Documents the placement and wording of the platform's legally binding guarantee. Referenced in Section 5.2.

Figure B.15 - eBay: Product page above the fold showing seller reputation block (Layer 3)

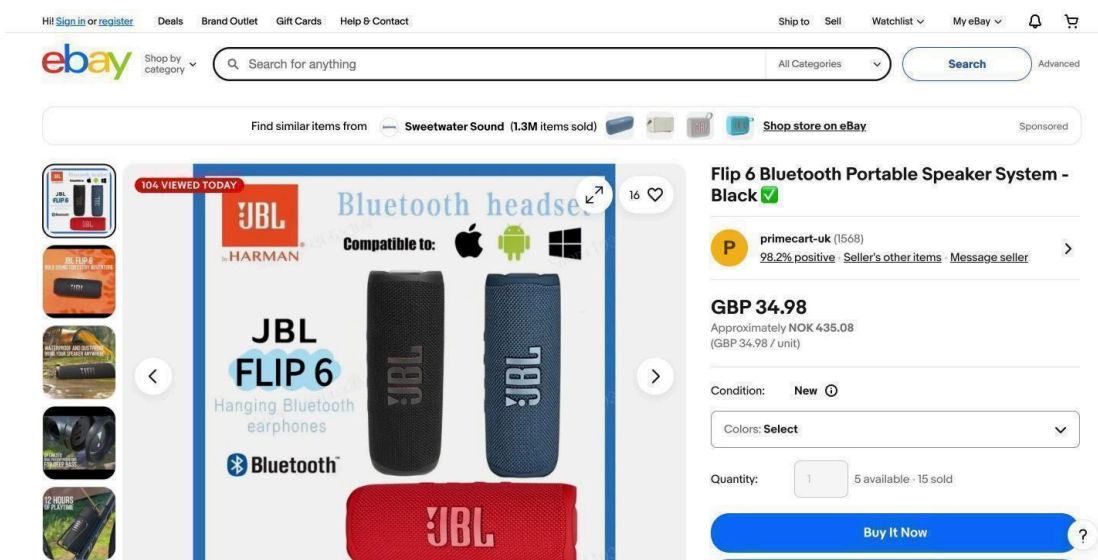


Figure B.15. eBay: product page above the fold for the observed listing, showing the seller reputation block. ebay.com, Session B, 23 May 2026. Shows seller feedback score, watcher count, and sold count at their position in the visual hierarchy. Referenced in Section 5.3.

Figure B.15a - eBay: Review / ratings section (Layer 3)

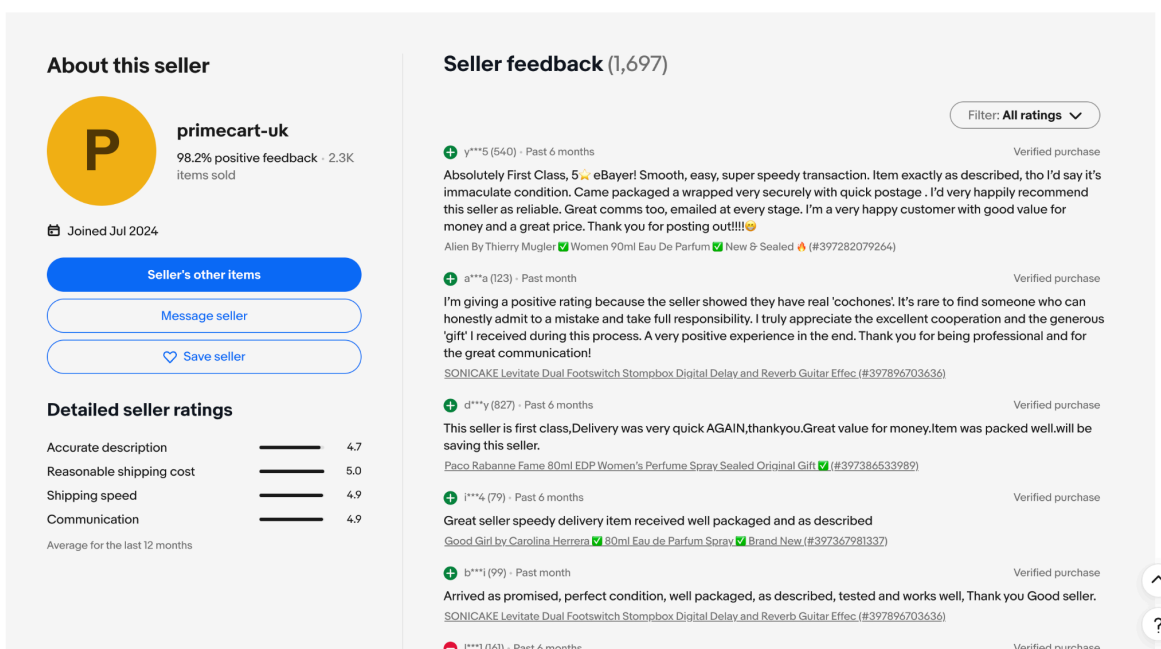


Figure B.15a. eBay: review and ratings section for the observed listing. ebay.com, Session B, 23 May 2026. Shows item rating, review count, and seller feedback integration. Referenced in Section 5.3.

Figure B.16 - eBay: 'This one's trending' social proof cue, workbook record (Layer 3)

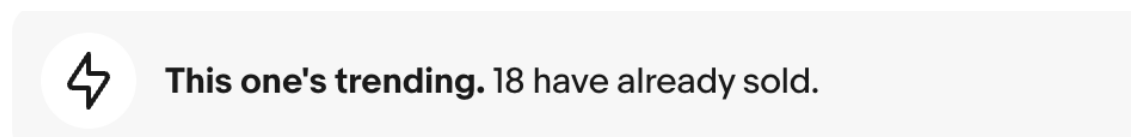


Figure B.16. Observation workbook page (Session B, 26 May 2026) recording the eBay dark pattern check (Q11). Shows 'This one's trending. 18 have already sold.' social proof cue captured verbatim. Referenced in Section 5.3 (Layer 3, eBay persuasive cues).

Apple Online Store

Figure B.17 - Apple: No cookie consent on first load (Layer 1)

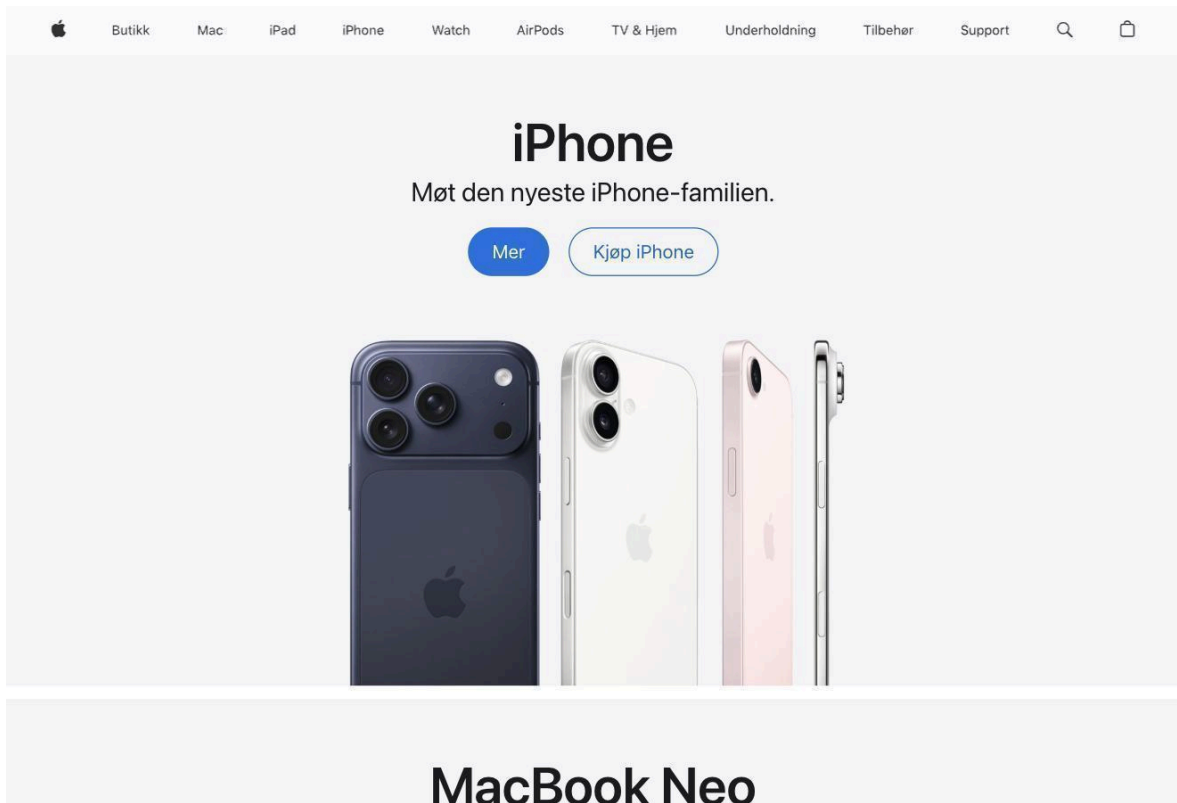


Figure B.17. Apple Online Store: no cookie consent dialogue on first load. apple.com/no, Session A, 26 May 2026. Confirms absence of any consent mechanism for first-time visitors. Referenced in Section 5.1.

Figure B.17a - Apple: Privacy settings / manage layer (Layer 1)

Apple's Use of Cookies

Apple's websites and online services may use "cookies." Cookies enable you to use shopping carts and to personalize your experience on our sites, tell us which parts of our websites people have visited, help us measure the effectiveness of ads and web searches, and give us insights into user behavior so we can improve our communications and products.

If you want to disable cookies in the Safari web browser, go to Preferences and then to the Privacy pane and choose to block cookies. On your iPad, iPhone, or iPod touch, go to Settings, then Safari, and then to the Cookies section. For other browsers, check with your provider to find out how to disable cookies.

Because cookies are used throughout our websites, disabling them may prevent you from using certain parts of the sites.

The cookies used on our websites have been categorized based on the guidelines found in the ICC UK Cookie guide. We use the following categories on our websites and other online services:

Category 1 — Strictly Necessary Cookies

These cookies are essential to enable you to browse around our websites and use their features. Without these cookies, services like shopping baskets and e-billing cannot be provided.

Category 2 — Performance Cookies

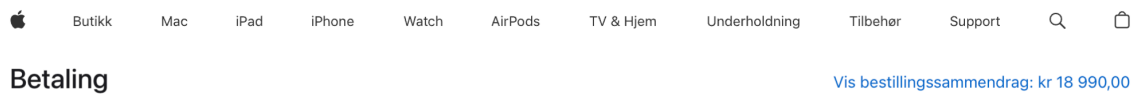
These cookies collect information about how you use our websites — for instance, which pages you go to most. This data may be used to help optimize our websites and make them easier for you to navigate. These cookies are also used to let affiliates know if you came to one of our websites from an affiliate and if your visit resulted in the use or purchase of a product or service from us, including details of the product or service purchased. These cookies don't collect information that identifies you. All information these cookies collect is aggregated and therefore anonymous.

Category 3 — Functionality Cookies

These cookies allow our websites to remember choices you make while browsing. For instance, we may store your geographic location in a cookie to ensure that we show you our website localized for your area. We may also remember preferences such as text size, fonts, and other customizable site elements. They may also be used to keep track of what featured products or videos have been viewed to avoid repetition. The information these cookies collect will not personally identify you, and they cannot track your browsing activity on non-Apple websites.

Figure B.17a. Apple Online Store: privacy settings / manage layer accessible from the site footer. apple.com/no, Session A, 26 May 2026. Shows the privacy preference controls available through the footer link. Referenced in Section 5.1.

Figure B.17b - Apple: Checkout / payment page (Layer 2)



Hvordan vil du betale?

[Logg på](#) med Apple-kontoen din for å bruke saldoen din.

Kreditt- eller debetkort
Visa, Mastercard, AMEX

Skriv inn kortinformasjonen din:

Kreditt- eller debetkortnummer

Utløper MM/ÅÅ

CVV

Fakturaadresse

☒ Bruk leveringsadressen min.

Figure B.17b. Apple Online Store: checkout / payment page. *apple.com/no*, Session B, 26 May 2026. Shows Apple Pay and credit card options at the checkout step. Referenced in Section 5.2.

Figure B.18 - Apple: Product configuration page above the fold (Layer 2/3)

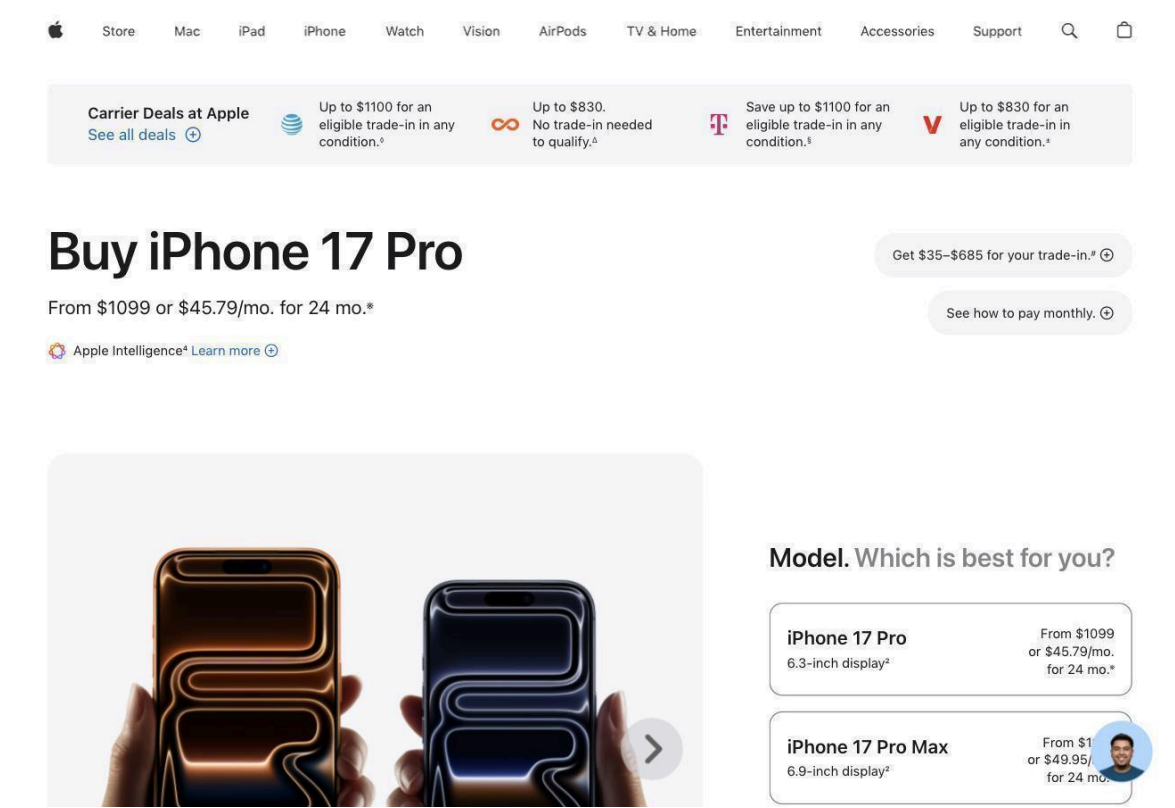


Figure B.18. Apple Online Store: product configuration page above the fold. apple.com/no, Session B, 26 May 2026. Shows minimal element count, premium visual treatment, and carrier deal badges. Referenced in Section 5.3.

Figure B.19 - Apple: Page footer showing legal notices and privacy links (Layer 1/2)

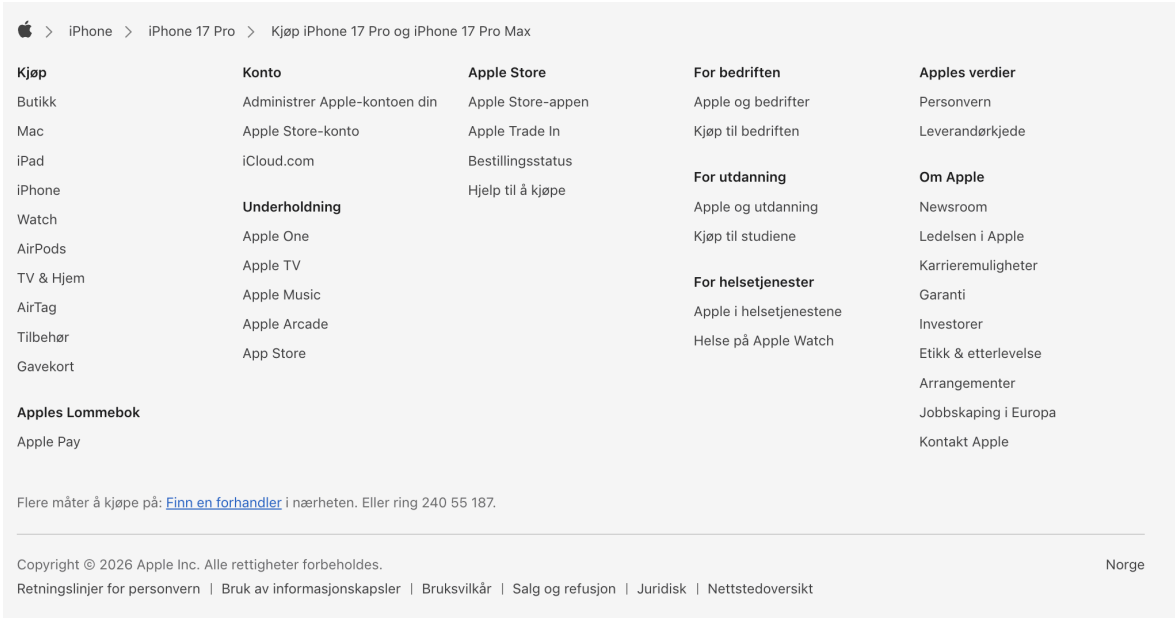


Figure B.19. Apple Online Store footer (apple.com/no), Session B, 26 May 2026. Contains site navigation, privacy policy link, terms of use, and EU consumer rights references ('Salg og refusjon', 'Juridisk'). Referenced in Section 5.2: return policy appears here rather than at the product configuration level.

