Fractured Awareness: Why Platform Privacy Systems Are Accepted More Than They Are Understood

Omar Haggag[1][a], John Grundy[1][b] and Mohan Baruwal Chhetri[2][c]
[1]*HumaniSE Lab, Department of Software Systems and Cybersecurity, Faculty of IT, Monash University, Australia*
[2]*CSIRO's Data61, Australia*
{*omar.haggag, john.grundy*}*@monash.edu, mohan.baruwalchhetri@data61.csiro.au*

Keywords: Fractured Awareness, Software Engineering, Privacy, Digital Platforms, Consent Architecture, Australia

Abstract: Public debate about digital privacy is often framed around a familiar dilemma: while concern about surveillance and data misuse continues to grow, individuals nonetheless continue to participate extensively in platform ecosystems that rely on large-scale data extraction. This phenomenon is commonly referred to as the *privacy paradox*. However, attributing the paradox solely to individual behaviour neglects the structural conditions within which privacy decisions take place. This paper investigates how transparency mechanisms are implemented across major digital platforms and how these implementations shape the environments in which users must interpret and make decisions about the data-collection, use, and sharing practices that underpin platform privacy. We conduct a multi-layer analysis of three platform ecosystems: Meta (Facebook and Instagram), TikTok, and YouTube, examining the structural complexity of privacy policies and the architecture of consent interfaces used to communicate data practices. Our analysis shows that transparency mechanisms frequently produce a condition we describe as *fractured awareness*. Privacy disclosures are structurally complex and often distributed across multiple documents, while consent interfaces require substantial interaction effort to locate or modify privacy settings. Together, these characteristics impose high informational and interactional costs on users attempting to understand platform data practices. This study contributes to software engineering research by reframing privacy transparency as a socio-technical property of digital systems rather than solely a legal or behavioural issue. By analysing how regulatory disclosure requirements are translated into software artefacts such as policies and consent interfaces, the paper highlights how platforms can satisfy formal transparency obligations while still limiting meaningful user comprehension. These findings suggest that addressing privacy challenges requires treating transparency not only as a regulatory requirement but also as a design and engineering problem within large-scale digital platforms.

1 INTRODUCTION

Digital platforms increasingly rely on large-scale data infrastructures that capture, infer, and monetise information about users' behaviour. Social media and video platforms such as Facebook and Instagram (Meta), TikTok, and YouTube continuously collect behavioural signals to personalise content, optimise advertising systems, and train large-scale recommendation algorithms. Empirical measurement studies have demonstrated the scale and persistence of tracking infrastructures across the web and mobile ecosystems, revealing extensive third-party data collection and behavioural profiling mechanisms (Acar et al., 2014; Englehardt and Narayanan, 2016; Binns et al., 2018).

At the same time, public concern about digital surveillance and data exploitation has grown substantially. Surveys across multiple countries show that individuals are concerned about how their personal data is collected and used, yet continue to engage extensively with platforms that rely on large-scale data extraction (Acquisti et al., 2015; Auxier and Rainie, 2019; Rainie and Duggan, 2016). This apparent contradiction has often been described as the *privacy paradox* (Barnes, 2006; Norberg et al., 2007). However, research increasingly suggests that privacy decision-making occurs within complex socio-technical environments characterised by information asymmetries, opaque data infrastructures, and interface designs that shape how users encounter privacy controls (Nissenbaum, 2010; Solove, 2013; Haggag et al., 2021).

[a] https://orcid.org/0000-0003-2346-3131
[b] https://orcid.org/0000-0003-4928-7076
[c] https://orcid.org/0000-0002-6138-7742

In practice, most users encounter privacy governance through software artefacts such as privacy policies, consent prompts, and configuration interfaces embedded within digital platforms. Studies in usable privacy and human-computer interaction show that individuals often rely on incomplete mental models of platform data flows when making privacy decisions (Lin et al., 2012; Felt et al., 2012; Balebako et al., 2015). These interactions frequently occur through interface prompts or configuration choices that must be evaluated quickly and under conditions of uncertainty (Egelman et al., 2008; Wang et al., 2013).

Modern privacy regulation largely relies on disclosure-based governance. Frameworks such as the European Union's *General Data Protection Regulation* (GDPR) and Australia's *Privacy Act 1988* require organisations to inform users about how personal information is collected, used, and disclosed through mechanisms such as privacy policies and consent notices (Office of the Australian Information Commissioner, 2023). These transparency obligations are intended to enable informed decision-making about personal data practices (Cate, 2010; Solove, 2013). However, empirical research consistently shows that privacy policies are rarely read and are often difficult to interpret. For example, McDonald and Cranor estimated that reading the privacy policies encountered during a typical year of web use would require hundreds of hours annually (McDonald and Cranor, 2008). As a result, disclosure mechanisms frequently function as formal compliance artefacts rather than effective communication tools (Martin, 2018; Schneier, 2015; Cate, 2010).

From a software engineering perspective, these disclosure mechanisms are implemented through system components such as consent flows, privacy dashboards, and configuration interfaces. These artefacts are typically developed within product environments that prioritise behavioural metrics such as engagement and retention. Research on dark patterns and manipulative interface design demonstrates how consent architectures can influence behaviour through default settings, asymmetric options, and increased interaction costs for privacy-protective choices (Gray et al., 2018; Mathur et al., 2019; Narayanan et al., 2020; Machuletz and Böhme, 2020; Haggag et al., 2022).

This paper argues that the interaction between disclosure-based regulation and platform interface design produces a socio-technical condition we describe as *fractured awareness*. In this condition, users express concern about privacy risks while lacking a clear understanding of how platforms collect, infer, and monetise personal information. Rather than emerging from individual irrationality, fractured awareness arises from the interaction between regulatory transparency requirements and the software systems used to implement them. To examine this dynamic, we analyse how transparency requirements under the Australian Privacy Act intersect with the privacy policies and consent architectures of three major platforms: Meta (Facebook and Instagram), TikTok, and YouTube. Our analysis focuses on two dimensions: the structural complexity of platform privacy policies (including document length, readability, and policy structure) and the architecture of consent interfaces (including default settings, interaction costs for opt-out decisions, and the navigational depth required to locate privacy controls). By framing transparency implementation as a software engineering problem rather than solely a legal or behavioural one, this paper highlights how regulatory requirements are translated into technical system artefacts. The main contributions of this paper include:

- Using the concept of *fractured awareness* introduced in our prior work (Haggag et al., 2026), we analyse how platform transparency mechanisms shape the environments in which users encounter and interpret digital privacy disclosures with limited understanding of platform data practices.
- We analyse how privacy transparency requirements under the Australian Privacy Act are operationalised through software artefacts such as privacy policies and consent interfaces.
- Using Meta (Facebook and Instagram), TikTok, and YouTube as empirical cases, we provide a structural analysis of platform privacy policies and consent architectures.
- We demonstrate how policy complexity and interface design jointly create high cognitive and interaction costs for users attempting to understand or manage their privacy settings.
- We argue that *fractured awareness* emerges from the interplay between regulatory disclosure frameworks and software engineering design practices.

2 MOTIVATION

Modern privacy governance assumes that transparency enables informed user choice. Across many jurisdictions, privacy regulation relies on disclosure mechanisms that require organisations to inform individuals about how personal data is collected, processed, and shared. Frameworks such as the European Union's GDPR and Australia's *Privacy Act 1988* operationalise this logic through requirements to publish privacy policies and provide explanations of data handling practices (Cate, 2010; Solove, 2013; Office

of the Australian Information Commissioner, 2023). Within this notice-and-consent model, individuals are expected to evaluate these disclosures and make informed decisions about participation in digital services (Nissenbaum, 2010; Solove, 2013).

However, in practice the effectiveness of disclosure-based governance has long been questioned. Empirical studies show that privacy policies are rarely read and often exceed the cognitive capacity of ordinary users due to complex legal language and fragmented document structures (McDonald and Cranor, 2008; Reidenberg et al., 2015). At the same time, digital platforms have evolved into highly complex socio-technical systems built on large-scale behavioural data collection and algorithmic inference (Helberger et al., 2019). Within such environments, users often encounter privacy governance not through legal texts but through software artefacts such as consent prompts, onboarding flows, and configuration interfaces embedded in platform systems.

This disconnect indicates that the effectiveness of transparency mechanisms depends not only on regulatory disclosure obligations but also on how these obligations are implemented within platform architectures. Rather than treating privacy solely as a legal or behavioural issue, it is therefore necessary to examine how regulatory transparency requirements are translated into software artefacts and interaction pathways within digital platforms.

Our study investigates this translation by analysing how disclosure-based privacy regulation is operationalised within the privacy policies and consent architectures of three major platforms: Meta (Facebook and Instagram), TikTok, and YouTube. We focus on the structural complexity of platform privacy policies and the design of consent interfaces as key artefacts through which users encounter privacy governance. This perspective helps explain the emergence of what we describe as *fractured awareness*: a socio-technical condition in which users express concern about digital privacy while lacking a clear operational understanding of platform data practices. To examine this dynamic, we wanted to answer the following research questions:

- **RQ1:** How are transparency obligations under privacy regulation, particularly the Australian Privacy Act, translated into concrete software artefacts, specifically privacy policies and consent interfaces, across major digital platforms?
- **RQ2:** How does the structural complexity of privacy policies and the design of consent interfaces shape users' capacity to interpret, evaluate, and act on platform data practices?
- **RQ3:** How does the interaction between regulatory disclosure frameworks and platform design and engineering practices contribute to the socio-technical condition of fractured awareness within digital platform ecosystems?

3 METHODOLOGY

Our study examines how regulatory transparency requirements are translated into software artefacts within modern digital platforms. Rather than treating privacy policies solely as legal texts or relying on surveys to analyse user behaviour, we adopt a *regulation-to-implementation traceability approach*. This perspective treats privacy regulation as a set of normative requirements that must be operationalised within platform software architectures. The central premise is that regulatory frameworks do not directly shape user experience. Instead, legal requirements are mediated through technical artefacts such as privacy policies, consent banners, onboarding flows, and privacy configuration interfaces, that together constitute the practical layer through which regulation becomes visible to users. Analysing this translation allows us to investigate how transparency obligations interact with the engineering realities of digital platforms.

3.1 Analytical Perspective

Our methodology integrates three analytical layers:

- **Regulatory Layer**: The transparency obligations articulated in the Australian *Privacy Act 1988* and the Australian Privacy Principles (APPs), which define the formal requirements governing how organisations must disclose the collection, use and sharing of personal information.
- **Platform Implementation Layer**: The software-level artefacts through which these obligations are operationalised, including privacy policies, supporting documentation structures, and the consent interface architectures used to present data-handling practices to users.
- **Interaction Layer**: The user-facing interaction pathways through which individuals encounter these artefacts, navigate disclosure materials, and make privacy-related decisions about data collection, use and sharing within platform environments.

3.2 Regulatory Analysis

The first stage of our methodology analyses transparency requirements within the Australian privacy regulatory landscape. In particular, we focus on the

APPs that establish the core obligations governing how organisations must manage, collect, use and disclose personal information in Australia. Our analysis centres on the principles most directly related to transparency and disclosure: (i) *APP 1* (open and transparent management), (ii) *APP 5* (notification of collection), (iii) *APP 6* (use and disclosure of personal information).

These principles require organisations to inform individuals about how their personal data is collected, processed, and shared. However, the regulation does not prescribe specific constraints on the structure, length, readability, or interaction design of disclosure mechanisms. Consequently, organisations have broad discretion in how privacy policies and consent interfaces are constructed.

This regulatory analysis identifies a gap between normative transparency obligations and the absence of technical or architectural guidance governing how these obligations should be implemented. This gap motivates our examination of how platforms translate regulatory requirements into artefacts such as policies, consent prompts, and privacy configuration interfaces.

3.3 Platform Selection

To examine how regulatory transparency is implemented in practice, we analyse three major digital platforms: *Meta* (Facebook and Instagram), *TikTok*, and *YouTube*. These platforms were selected because they represent some of the most widely used digital services globally and within Australia, and because their business models rely heavily on behavioural data collection and algorithmic recommendation systems.

Privacy policy texts were extracted from each platform's Australian site as of December 2025 and served as the primary artefacts for structural and readability analysis. Consent interfaces and privacy-configuration architectures were analysed through direct interaction with each platform using an iOS device in January 2026. This analysis involved documenting onboarding consent prompts, tracing navigation pathways to privacy controls, and recording the interaction steps required to modify or withdraw consent settings.

3.4 Platform Artefact Analysis

The second stage of our methodology examines how transparency requirements are operationalised through two categories of platform artefacts.

- **Privacy Policy Structures**: We analyse privacy policies as the primary documentation artefacts through which platforms disclose their data-handling practices. To assess their informational complexity, we extract a set of structural indicators, including:
  - Policy word count
  - Estimated reading time
  - Document layering and internal cross-referencing
  - Readability metrics using the Flesch-Kincaid Grade Level (FKGL) (Flesch, 1948; Kincaid et al., 1975)
  - Density of technical and legal terminology

  FKGL estimates the educational level required to understand a text and is computed as:

$$FKGL = 0.39\left(\frac{\text{total words}}{\text{total sentences}}\right) + 11.8\left(\frac{\text{total syllables}}{\text{total words}}\right) - 15.59$$

  These indicators capture the informational burden placed on users attempting to understand platform data practices.
- **Consent Interface Architectures**: This study examines how privacy decisions are operationalised through interface design. Consent mechanisms were analysed by reviewing platform onboarding flows and the privacy-configuration interfaces through which users view, modify, or withdraw consent.

  Our analysis focuses on interactional characteristics including:
  - Default data-collection settings
  - Interaction steps required to modify privacy preferences
  - Navigation depth needed to locate privacy controls
  - Symmetry between acceptance and rejection options
  - Visibility of data-processing explanations within the interface

  These indicators capture the interactional costs associated with exercising privacy control within platform environments.

3.5 Composite Consent Complexity Metrics

To capture the structural complexity of consent interfaces, we construct two derived indicators: the *Consent Cognitive Load Index (CCLI)* and the *Consent Navigation Entropy (CNE)*. Together, these metrics approximate the cognitive and navigational effort required for users to understand and modify privacy settings within platform interfaces.

- **Consent Cognitive Load Index (CCLI).** The CCLI estimates the interactional complexity of consent mechanisms by aggregating four observable interface characteristics:

$$CCLI = D + N + G + S \tag{1}$$

  where:

– D represents the number of decision points presented to the user (e.g., toggles, prompts, or consent choices);
– N denotes the navigation depth required to reach privacy configuration controls;
– G captures the number of consent or data-processing categories presented within the interface;
– S reflects the number of settings groups affecting tracking, advertising, or data personalisation.

Higher CCLI values indicate greater interaction complexity and increased cognitive effort required to interpret and manage privacy settings.

- **Consent Navigation Entropy (CNE).** The CNE metric captures the structural variability of navigation pathways through which users can reach privacy controls. It is defined as:

$$CNE = P \tag{2}$$

where P denotes the number of distinct navigation paths leading to the same privacy-configuration location.

Higher CNE values signal more fragmented interface structures in which users may encounter multiple alternative routes to the same privacy controls. Such variability increases the difficulty of forming a coherent mental model of where privacy-related decisions can be managed.

4 RESULTS

This section presents the empirical results of our analysis combining privacy policy structural metrics with consent-interface characteristics across Meta (Facebook/Instagram), TikTok, and YouTube (Google). We examine how transparency obligations in the Australian privacy regulatory landscape are translated into platform artefacts that are experienced by users.

Figure 1 illustrates the regulation–implementation pathway, illustrating how transparency requirements under the Australian Privacy Act are translated into platform artefacts such as privacy policies and consent interfaces, and how these artefacts are ultimately encountered by users.

4.1 Privacy Policies Exceed Realistic Reading Expectations

The structural analysis reveals substantial variation in privacy policy length across the examined platforms. The Meta privacy policy contains approximately 21,248 words, corresponding to an estimated

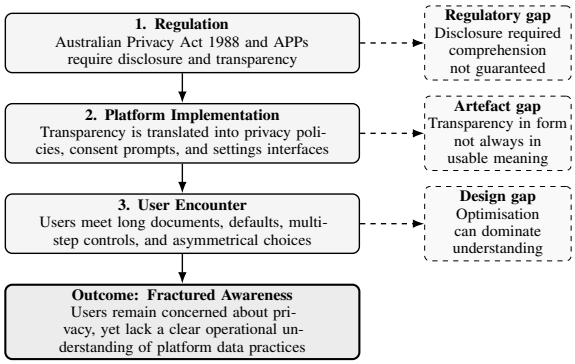

Figure 1: Regulation-implementation pathway of fractured awareness, showing how Australian privacy regulation translates into platform privacy policies and consent interfaces.

reading time of 106.2 minutes at 200 words per minute. YouTube's policy contains 14,520 words (approximately 72.6 minutes), while TikTok's policy contains 7,246 words (approximately 36.2 minutes). Even the shortest document therefore requires sustained attention. Moreover, once cross-referenced documents and hyperlinks are taken into account, the effective effort required to understand a platform's complete policy environment increases even further.

These findings must be interpreted in light of APP 1.2, which requires entities to take reasonable steps to implement practices and systems that ensure compliance with the privacy principles. However, the Act provides no operational thresholds for readability or practical comprehensibility.

⇒ **Finding:** Although transparency obligations are technically met through the provision of extensive documentation, the volume, complexity, and fragmentation of these materials impose substantial cognitive burdens that make meaningful comprehension improbable for most users.

Figure 2 synthesises these results by illustrating how regulatory disclosure requirements, platform implementation practices, and optimisation-oriented design jointly create conditions for fractured awareness.

4.2 Policies Written at a Postgraduate Reading Level

In addition to sheer length, the linguistic structure of the policies further contributes to their comprehension burden. The FKGL score ranges from 18.2 to 18.9, indicating that the documents require reading skills equivalent to postgraduate-level education. Average sentence length ranges from 22.0 words (TikTok) to 32.7 words (Meta), while technical and legal terminology density ranges from 73.2 to 107.8 specialised

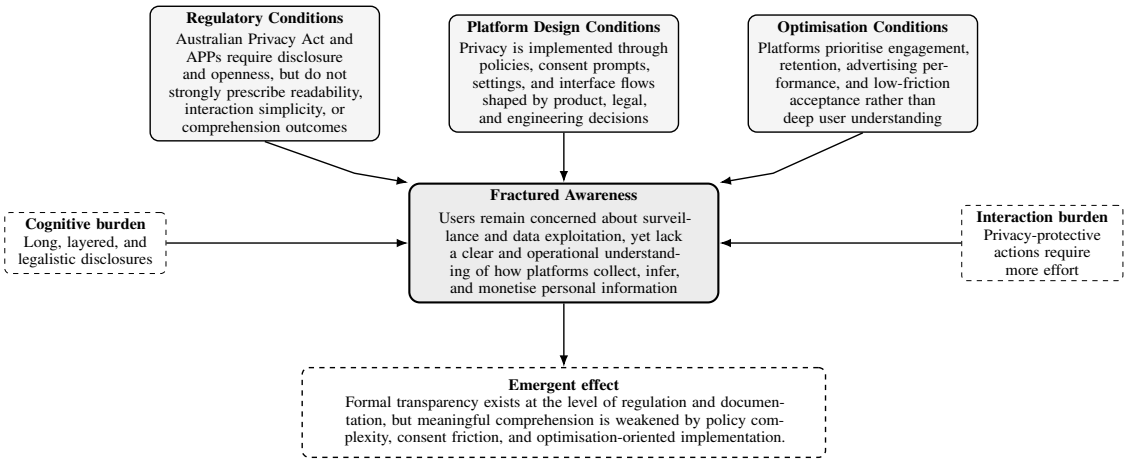

Figure 2: Fractured Awareness Model. The interaction of regulation, platform design, and optimisation creates conditions where privacy concern coexists with limited understanding.

terms per 1,000 words, as shown in Table 1.

This level of linguistic complexity conflicts with the intent of APP 1.4, which requires organisations to clearly express their policies relating to personal information management. While the Act emphasises openness and clarity, it does not establish enforceable readability thresholds or place limits on the use of specialised terminology.

⇒ **Finding:** The linguistic characteristics of platform privacy policies suggest that regulatory transparency requirements are satisfied in a formal, legal sense rather than a functional one, resulting in documents that are legally precise but cognitively inaccessible for most users.

4.3 Transparency Fragmented Across Multiple Documents

A further structural characteristic concerns the fragmentation of policy information across multiple linked documents. Our analysis identified 199 external links within the Meta policy, 73 within TikTok's policy, and 218 within YouTube's privacy documentation. Each platform also employs extensive cross-referencing across secondary policies, with between 14 to 18 linked documents forming part of the overall privacy disclosure ecosystem. Internal anchor links range from 133 (TikTok) to 423 (Meta), indicating highly layered navigation structures as shown in Table 1. Although layered documentation can, in principle, improve modularity, it simultaneously requires users to reconstruct the platform's overall data-processing logic by navigating multiple documents and hyperlinks.

⇒ **Finding:** Transparency is distributed across interconnected documentation networks rather than presented as a unified coherent explanation, requiring users to assemble fragmented pieces of information to understand platform data practices.

4.4 Bundled Consent Reduces Meaningful User Choice

The consent architecture analysis [1] reveals that all three platforms enable core data collection by default at the moment of account creation. Consent prompts appear during onboarding, before users have developed familiarity with platform functions or data flows. In addition, consent is frequently bundled across multiple processing purposes: rather than requesting permission for specific data uses individually, platforms typically combine multiple data-processing purposes under single acceptance interactions.

This practice must be considered in relation to APP 5, which requires organisations to notify individuals about the collection of personal information and the purposes of that collection. However, the Act does not prohibit bundled consent structures nor does it require granular opt-in mechanisms for each specific processing purpose.

[1] Privacy policy text was extracted from publicly available policy documents and analysed using automated readability analysis to compute sentence counts, word counts, and syllable counts. Consent interfaces and privacy configuration architectures were examined through direct interaction with the platforms using an iOS device (Australian App Store distribution) in January 2026.

Table 1: Integrated privacy-policy complexity and consent architecture characteristics across major platforms. Policy metrics are computed from the analysed policy (word counts tokenised from extracted text and reading time estimated at 200 WPM). Interface indicators are derived from structural analysis of platform consent interfaces on an iOS device.

Indicator	Meta (Facebook/Instagram)	TikTok	YouTube (Google)
Privacy policy structural complexity			
Policy word count (snapshot)	21,248	7,246	14,520
Estimated reading time at 200 WPM	106.2 min	36.2 min	72.6 min
#Sections (top-level)	12	11	9
Flesch-Kincaid Grade Level (FKGL)	18.9	18.2	18.5
Average sentence length	32.7 words	22.0 words	29.6 words
Technical/legal terminology density	High (73.2 per 1k)	High (107.8 per 1k)	High (81.6 per 1k)
Number of External links (URI links)	199	73	218
Number of Linked / cross-referenced policy documents	15	14	18
Number of Internal hyperlinks / anchors	423	133	275
Layered policy structure (primary + secondary documents)	Yes	Yes	Yes
Clarity of data processing explanations	Moderate	Moderate	Moderate
Overall policy comprehension burden	Very high	High	Very high
Consent architecture and interface characteristics			
Default data collection enabled at account creation	Enabled by default	Enabled by default	Enabled by default
Consent requested during onboarding before user familiarity	Yes	Yes	Yes
Bundled consent covering multiple processing purposes	Extensive bundling	Extensive bundling	Extensive bundling
Granularity of consent categories	Limited category separation	Limited category separation	Moderate category separation
Immediate opt-in interaction cost (clicks to proceed)	1	1	1
Minimum opt-out interaction cost (navigation + confirmation clicks)	6-8	5-7	4-6
Navigation depth to tracking controls (interface layers)	3-4	3-4	2-3
Consent friction ratio (opt-out / opt-in interaction cost)	$\sim$7:1	$\sim$6:1	$\sim$5:1
Number of settings groups affecting advertising or tracking	6-7	4-6	4-5
Linked privacy documents referenced from consent interface	3-5	3-4	4-6
Algorithmic inference transparency regarding profiling logic	Very limited	Very limited	Limited
Data category aggregation under single toggle	Present	Present	Present
Persistence of consent decision once accepted	Persistent until manual change	Persistent until manual change	Persistent until manual change
Ease of locating consent withdrawal controls	Low discoverability	Low discoverability	Moderate discoverability
Interface salience bias favouring acceptance	Strong	Strong	Moderate
Consent Cognitive Load Index (CCLI)	13-15 (High)	11-13 (High)	9-11 (Moderate-High)
Consent Navigation Entropy (CNE)	4 navigation paths	3 navigation paths	3 navigation paths

$\Rightarrow$ **Finding:** Bundled consent collapses multiple data-processing decisions into a single acceptance action, limiting users' ability to make differentiated choices and functioning as a choice-architecture dark pattern that preserves legal compliance while undermining meaningful consent.

4.5 Opt-Out Requires Significantly More Effort than Opt-In

A clear asymmetry emerges when comparing the interaction costs of accepting versus rejecting data processing. Across all three platforms, the initial opt-in interaction cost is minimal, typically requiring only one click to proceed. In contrast, withdrawing or limiting consent requires navigating substantially deeper interface structures. The minimum opt-out interaction cost ranges from 4-6 clicks on YouTube to 6-8 clicks on Meta, with navigation depth extending across 2-3 interface layers for YouTube and 3-4 layers for Meta and TikTok. This produces a Consent Friction Ratio of approximately 5:1 to 7:1, meaning that users must invest significantly more effort to restrict data processing than to accept it.

The integrated metrics in Table 1 further illustrate this structural asymmetry. Across Meta, TikTok, and

YouTube, default configurations enable broad data collection, while privacy-protective settings require deeper navigation and multiple interaction steps. Opt-out pathways are longer, less salient, and peripheral to onboarding flows. As shown in the table, opt-out to opt-in interaction ratios reach approximately 7:1 for Meta, 6:1 for TikTok, and 5:1 for YouTube, accompanied by limited transparency about profiling logic and low discoverability of withdrawal controls.

⇒ **Finding:** Interface structures systematically privilege acceptance pathways over restriction pathways, turning regulatory disclosure into behavioural steering via asymmetric interaction costs.

4.6 Limited Transparency Around Algorithmic Profiling

Our analysis further examined the extent to which platforms explain their algorithmic inference and profiling practices. Across all three ecosystems, transparency regarding profiling logic remains limited. Although policies describe categories of data collected and potential uses such as advertising personalisation, they rarely provide detailed explanations of how behavioural signals are transformed into predictive models or advertising segments.

This gap is particularly significant in light of APP 6, which governs the use and disclosure of personal information. While the Act requires organisations to specify the purposes for which personal information is used, it does not mandate disclosure of algorithmic inference methods, model features, or decision-making logic. Users are informed about what data may be used, but not how the data shapes personalised recommendations, risk scores, or advertising classifications.

⇒ **Finding:** Regulatory transparency obligations centre on high-level statements of data use, leaving the algorithmic processes that transform behavioural traces into inferences and predictions largely opaque to users.

4.7 Consent Interfaces Produce High Cognitive Load

The combined interface metrics provide an aggregate view of consent complexity. The Consent Cognitive Load Index (CCLI) ranges from 13-15 for Meta, 11-13 for TikTok, and 9-11 for YouTube, indicating substantial decision complexity within their respective consent interfaces.

Similarly, the Consent Navigation Entropy (CNE) reveals multiple potential pathways through which users may attempt to modify consent settings. Meta presents four navigation paths, while TikTok and YouTube present three paths each. Such navigation variability increases the likelihood that users encounter inconsistent, circular, or incomplete sequences.

Overall, these results suggest that transparency obligations under the Australian privacy framework are implemented primarily through documentation and interface artefacts. While these artefacts formally satisfy disclosure requirements, their structural complexity and interaction characteristics create conditions in which users may remain concerned about privacy risks while still lacking a clear operational understanding of platform data practices.

⇒ **Finding:** Consent interfaces combine structural complexity with navigational variability, increasing the cognitive effort required for users to form a stable and coherent understanding of platform data practices.

This indicates that disclosure and comprehension are empirically separable. The presence of information does not guarantee that users form accurate or actionable mental models of system behaviour. In this sense, transparency should not be evaluated as a binary attribute, i.e, disclosed versus not disclosed, but as a conversion problem: whether available information can realistically become intelligible knowledge.

⇒ **Finding:** Disclosure does not necessarily generate comprehension. The results reveal a consistent conversion failure in which platform practices are formally disclosed yet remain cognitively inaccessible to most users.

5 IMPLICATIONS FOR RESEARCH AND PRACTICE

The results of this study suggest that fractured awareness cannot be understood solely as a behavioural phenomenon or as a matter of inadequate user education. Rather, it emerges from the interplay between regulatory transparency requirements, software engineering practices, and optimisation-oriented platform design. As such, its implications extend across three domains: privacy regulation, software engineering practice, and socio-technical research on digital governance. This section discusses how these findings challenge existing assumptions about transparency and outlines practical directions for researchers, practitioners, and policymakers.

5.1 Rethinking Transparency as a Software Engineering Problem

Privacy regulation traditionally conceptualises transparency as a documentation requirement. Under the Australian Privacy Act 1988, transparency is primarily operationalised through obligations to provide privacy policies and notifications describing data collection and use. However, our results demonstrate that the practical experience of transparency is mediated not by legal text alone but by the software artefacts through which that text is delivered and received.

Privacy policies, consent prompts, and privacy-settings interfaces are ultimately implemented as user interface components embedded within complex digital systems. Their design therefore falls within the domain of software engineering rather than legal drafting. Our results show policy length, hyperlink fragmentation, and consent-navigation depth are not just characteristics of written documentation but architectural properties of software and interaction designs.

This implies that transparency should be conceptualised as a *software engineering quality attribute*, similar to usability, accessibility, or security. From this perspective, privacy transparency must be evaluated through measurable system characteristics such as interaction cost, information architecture, cognitive load, and navigational entropy.

✓ **Recommendation:** Transparency should be treated as a measurable system property rather than a purely legal requirement. Researchers and software engineers must incorporate transparency metrics into software design processes, system evaluations, and broader software quality frameworks.

5.2 Integrating Privacy Transparency into Software Architecture

Our findings also highlight the role of software architecture in shaping the practical accessibility of privacy controls. Consent pathways, navigation depth, and interaction costs are not incidental interface details but outcomes of architectural decisions about how privacy-management functions are structured. For example, the observed consent friction ratios show that restricting data processing requires significantly more interaction steps than accepting it. This asymmetry indicates that consent management mechanisms are embedded within interface hierarchies optimised primarily for engagement and retention, rather than for user autonomy or informed decision-making.

Historically, software engineering research has prioritised properties such as performance, reliability, and scalability. Privacy transparency, by contrast, has rarely been considered as an architectural concern. The present findings suggest that privacy management mechanisms should be treated as first-class architectural components rather than peripheral configuration interfaces. This requires elevating transparency from a UI-level consideration to a structural design objective embedded throughout the system architecture.

✓ **Recommendation:** Software architects should explicitly model privacy transparency mechanisms as core architectural components, ensuring that consent management, privacy controls, and data-use explanations are integrated into foundational system design rather than added as secondary or peripheral interface layers.

5.3 Disclosure Alone Is Not Enough for Regulation

Our analysis also reveals a structural limitation within current regulatory frameworks. The Australian Privacy Act emphasises openness and disclosure but does not specify concrete operational requirements for readability, structural simplicity, or interaction costs associated with privacy decisions.

As a result, organisations can satisfy regulatory transparency obligations through extensive documentation while still implementing consent interfaces that impose substantial cognitive and navigational burdens on users. This creates a regulatory environment in which formal transparency may coexist with limited practical comprehension.

Regulators have historically relied on disclosure as the primary mechanism for protecting user autonomy. Yet, the results indicate that disclosure is insufficient when transparency artefacts are too complex to meaningfully interpret. In practice, transparency depends not only on providing information but on whether users can feasibly convert that information into an accurate understanding of system behaviour.

✓ **Recommendation:** Privacy regulators should complement disclosure obligations with design-oriented transparency requirements, including readability thresholds, interface symmetry standards, and limits on consent interaction complexity.

5.4 Transparency Needs Measurable System Metrics

Another implication concerns the need for systematic measurement frameworks. The indicators introduced in this study – consent friction ratios, cognitive

load indices, and navigation entropy – demonstrate that transparency and consent architectures can be analysed using quantifiable system properties. Such metrics provide an empirical basis for evaluating whether privacy mechanisms meaningfully support user understanding. They also allow comparative analysis across platforms and regulatory environments.

Currently, privacy research often relies on qualitative evaluations of policy clarity or user perceptions. While valuable, these approaches do not capture the structural characteristics of digital systems that shape user decision environments. Developing robust measurement frameworks would enable regulators, researchers, and platform designers to evaluate transparency in a systematic and reproducible manner.

✓ **Recommendation:** Future research should develop standardised metrics for evaluating transparency artefacts and consent architectures, enabling systematic comparison across platforms and regulatory contexts.

5.5 Towards Human-Centred Privacy Engineering

Finally, the concept of fractured awareness suggests that privacy governance must move beyond documentation-based transparency toward more human-centred approaches. Rather than assuming that users will read and interpret extensive policies, systems should support understanding through interactive explanations, contextual prompts, and simplified data-flow visualisations.

Human-centred privacy engineering treats user understanding as a design objective rather than as an individual responsibility. This shift aligns privacy governance more closely with established principles from human-computer interaction and usability engineering. Potential approaches include progressive disclosure mechanisms, interactive explanations of algorithmic profiling, and real-time visualisations of data use.

✓ **Recommendation:** Platform designers should adopt human-centred privacy engineering approaches that prioritise comprehension through interactive explanations, simplified data-flows, and context-aware transparency mechanisms.

6 THREATS TO VALIDITY

- **Internal Validity**: One potential threat arises from the manual extraction and analysis of privacy policies and interface structures. Although the structural indicators in Table 1 were derived through systematic inspection, manual coding may introduce interpretation bias, particularly when assessing qualitative attributes such as clarity of explanations. To mitigate this, our analysis focused primarily on measurable structural indicators – word counts, hyperlink counts, navigation depth, and interaction costs – which reduce reliance on subjective interpretation by grounding the analysis in observable system properties. Another potential threat concerns the dynamic nature of digital platforms: privacy policies and interfaces evolve over time, and the analysed artefacts represent only a snapshot at the point of data collection. Subsequent updates may alter policy wording, navigation pathways, or consent mechanisms.
- **External Validity**: This study focuses on three major platform ecosystems – Meta (Facebook/Instagram), TikTok, and YouTube (Google) – selected because they represent widely used global services with large-scale data-driven advertising infrastructures and well-developed privacy documentation. However, the results may not directly generalise to all digital platforms. Smaller platforms, services operating under different business models, or systems deployed in highly regulated sectors may implement different privacy architectures. Similarly, the regulatory analysis is grounded in the Australian Privacy Act and the Australian Privacy Principles, which may differ from regulatory frameworks in other jurisdictions. Despite these limitations, the selected platforms represent some of the most influential data ecosystems globally, and their governance models often shape broader industry practices.
- **Construct Validity**: In this research, the key construct is *fractured awareness*, defined as the condition in which users express concern about data practices while lacking an operational understanding of how data is collected, inferred, and monetised. One potential threat is that policy complexity metrics and interface indicators may not fully capture all dimensions of transparency or user understanding. For example, the presence of long privacy policies does not necessarily imply that no users can understand them. To address this, we employed multiple complementary indicators. Policy complexity metrics (e.g., reading time, hyperlink density, technical terminology) capture the informational burden of documentation. Interface indicators (e.g., navigation depth, consent friction ratio, and consent cognitive load) capture the interactional burden associated with exercising privacy choices.

7 RELATED WORK

Research on digital privacy spans multiple disciplines including human computer interaction, law, information systems, and software engineering. Prior work has examined how individuals make privacy decisions, how transparency mechanisms such as privacy policies and consent interfaces operate in practice, and how platform infrastructures shape data collection and governance. A long-standing body of research investigates the gap between individuals' stated privacy concerns and their disclosure behaviour online, commonly described as the *privacy paradox* (Barnes, 2006; Norberg et al., 2007). Subsequent work suggests that this phenomenon cannot be explained solely by inconsistent preferences. Privacy decisions often occur under conditions of bounded rationality, uncertainty, and incomplete information (Acquisti et al., 2015). Studies in usable privacy further demonstrate that user behaviour is strongly influenced by contextual cues and interface design (Adjerid et al., 2013; Balebako et al., 2015). Large-scale surveys also report that many individuals express concern about digital surveillance while simultaneously reporting limited understanding of how data collection systems operate (Auxier and Rainie, 2019; Rainie and Duggan, 2016).

Another strand of research examines the effectiveness of transparency mechanisms such as privacy policies. Numerous studies show that these documents are frequently difficult to interpret due to complex language and legal terminology (Milne and Culnan, 2004; Reidenberg et al., 2015). McDonald and Cranor's analysis estimated that reading all privacy policies encountered during typical web usage would require hundreds of hours per year (McDonald and Cranor, 2008). Legal scholarship has questioned disclosure-based governance models, arguing that individuals cannot realistically evaluate complex data practices through policy reading alone (Cate, 2010; Solove, 2013).

Research in usable privacy and security has also examined how privacy decisions are shaped through interface design. Users frequently interact with privacy systems through permission dialogs, consent prompts, and configuration interfaces rather than through detailed policy documents. Studies of mobile permissions and privacy warnings demonstrate that users often rely on incomplete mental models of data flows when interpreting these prompts (Felt et al., 2012; Lin et al., 2012). Other work shows locating and configuring privacy controls in platform settings can involve substantial interaction complexity (Habib et al., 2019).

A growing literature further examines how interface design can influence behaviour through so-called *dark patterns*. These manipulative design strategies include asymmetric choice architectures, hidden options, and default configurations that steer users toward decisions that benefit the platform (Gray et al., 2018; Mathur et al., 2019). Empirical studies of cookie consent systems and privacy dialogs introduced after the GDPR demonstrate that many implementations still privilege acceptance over refusal through interface design choices (Degeling et al., 2019; Machuletz and Böhme, 2020).

Finally, privacy must be understood within the broader technical infrastructures of digital platforms. Measurement studies have revealed extensive tracking technologies operating across the web and mobile ecosystems (Acar et al., 2014; Englehardt and Narayanan, 2016). Mobile applications often involve complex third-party data flows that remain difficult for users to observe directly (Binns et al., 2018). At a broader level, scholars have analysed how platform economies rely on large-scale behavioural data collection to support targeted advertising and algorithmic optimisation (Helberger et al., 2019).

Although these research strands provide important insights into privacy behaviour, transparency mechanisms, interface design, and platform infrastructures, they are often analysed separately. This study integrates these perspectives within a socio-technical framework that examines how regulatory transparency requirements are translated into software artefacts. By analysing privacy policy complexity and consent interface structures across major platforms, we highlight how disclosure-based governance can produce environments in which concern about surveillance coexists with limited operational understanding of data practices, a condition referred to as *fractured awareness*.

8 SUMMARY

Our study examined a persistent paradox in digital privacy research: individuals frequently report concern about surveillance and data misuse, yet participation in data-intensive platform ecosystems continues to grow. Rather than treating this coexistence of concern and participation as a behavioural contradiction, our findings suggest it reflects a structural condition embedded within modern digital platform systems. Through the combined analysis of privacy policy complexity, consent interface structures, and regulatory transparency requirements, our study identifies a socio-technical configuration we describe as *fractured awareness*. Individuals recognise the existence of digital surveillance and express concern about it, yet the mechanisms through which data is collected, inferred, and monetised remain difficult to interpret

in practice. Transparency mechanisms exist, but their structural complexity and interactional demands impose informational and navigational costs that limit meaningful understanding. From a software engineering perspective, this highlights an underexplored class of socio-technical risks. Systems may satisfy formal regulatory requirements while still generating conditions that obscure how underlying data infrastructures operate. Addressing this challenge requires moving beyond transparency as a documentary obligation toward transparency as an engineering property that can be evaluated through interface design, system architecture, and interaction costs.

ACKNOWLEDGEMENTS

Haggag is supported by a National Intelligence Post-doctoral Fellowship. Grundy and Haggag were supported by ARC Laureate Fellowship FL190100035 and Discovery Project DP200100020.

REFERENCES

Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A., and Diaz, C. (2014). The web never forgets: Persistent tracking mechanisms in the wild. In *CCS*.

Acquisti, A., Brandimarte, L., and Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221):509–514.

Adjerid, I., Acquisti, A., Brandimarte, L., and Loewenstein, G. (2013). Sleight of hand? studying the influence of privacy policy presentation on consumer behavior. In *SOUPS*.

Auxier, B. and Rainie, L. (2019). Americans and privacy: Concerned, confused and feeling lack of control over their personal information.

Balebako, R., Schaub, F., Adjerid, I., Acquisti, A., and Cranor, L. F. (2015). Beyond information seeking: Understanding privacy decisions. In *SOUPS*, pages 197–215.

Barnes, S. B. (2006). A privacy paradox: Social networking in the united states. *First Monday*, 11(9).

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., and Shadbolt, N. (2018). Third party tracking in the mobile ecosystem. In *Proceedings of the Web Science Conference*.

Cate, F. H. (2010). The failure of fair information practice principles. *Consumer Protection in the Age of the Information Economy*, pages 341–378.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., and Holz, T. (2019). We value your privacy... now take some cookies: Measuring the gdpr's impact on web privacy. *Proceedings on Privacy Enhancing Technologies*, 2019(3):32–48.

Egelman, S., Cranor, L. F., and Hong, J. (2008). You've been warned: An empirical study of the effectiveness of web browser phishing warnings. In *CHI*, pages 1065–1074.

Englehardt, S. and Narayanan, A. (2016). Online tracking: A 1-million-site measurement and analysis. In *CCS*.

Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., and Wagner, D. (2012). Android permissions: User attention, comprehension, and behavior. In *SOUPS*.

Flesch, R. (1948). A new readability yardstick. *Journal of Applied Psychology*, 32(3):221–233.

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., and Toombs, A. (2018). The dark (patterns) side of ux design. In *CHI*, page 534.

Habib, H., Pearman, S., Wang, Y., Ghanem, R., Acquisti, A., and Cranor, L. F. (2019). An empirical analysis of data deletion and opt-out choices on 150 websites. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*.

Haggag, O., Grundy, J., Abdelrazek, M., and Haggag, S. (2022). A large scale analysis of mhealth app user reviews. *Empirical Software Engineering*, 27(7):196.

Haggag, O., Grundy, J. C., and Chettri, M. B. (2026). Click, scroll, consent: Uncovering australia's privacy knowledge crisis. In *Proceedings of the International Conference on Software Engineering (ICSE)*, Rio de Janeiro, Brazil.

Haggag, O., Haggag, S., Grundy, J., and Abdelrazek, M. (2021). Covid-19 vs social media apps: does privacy really matter? In *2021 IEEE/ACM 43rd International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS)*, pages 48–57. IEEE.

Helberger, N., Pierson, J., and Poell, T. (2019). The political power of platforms. *Internet Policy Review*, 8(4).

Kincaid, J. P., Fishburne, R. P., Rogers, R. L., and Chissom, B. S. (1975). Derivation of new readability formulas for navy enlisted personnel. Technical report, U.S. Naval Air Station Memphis.

Lin, J., Liu, B., Sadeh, N., and Hong, J. (2012). Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the ACM Conference on Ubiquitous Computing (UbiComp)*, pages 501–510.

Machuletz, D. and Böhme, R. (2020). Multiple purposes, multiple problems: A user study of consent dialogs after gdpr. *Proceedings on Privacy Enhancing Technologies*, 2020(2):481–498.

Martin, K. (2018). Privacy interest, privacy loss, and mitigation. *Washington Law Review*, 93:1077–1116.

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., and Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11k shopping websites. In *CHI*, volume 3, pages 1–32.

McDonald, A. M. and Cranor, L. F. (2008). The cost of reading privacy policies. In *I/S: A Journal of Law and Policy for the Information Society*, volume 4, pages 543–568.

Milne, G. R. and Culnan, M. J. (2004). Readability of privacy policies. *Journal of Public Policy & Marketing*, 23(1):19–32.

Narayanan, A., Mathur, A., Chetty, M., and Kshirsagar, M. (2020). Dark patterns: Past, present, and future. *CACM*, 63(9):42–47.

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.

Norberg, P. A., Horne, D. R., and Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, 41(1):100–126.

Office of the Australian Information Commissioner (2023). Australian privacy principles guidelines.

Rainie, L. and Duggan, M. (2016). The state of privacy in america.

Reidenberg, J. R., Breaux, T., Cranor, L., French, B., Grannis, A., Graves, J. N., Liu, F., Norton, N., Ramanath, R., and Schaub, F. (2015). Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Technology Law Journal*, 30:39–88.

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton & Company.

Solove, D. J. (2013). Privacy self-management and the consent dilemma. *Harvard Law Review*, 126:1880–1903.

Wang, Y., Leon, P. G., Acquisti, A., and Cranor, L. F. (2013). Privacy nudges for social media: An exploratory facebook study. In *Proceedings of the World Wide Web Conference Companion*.