International Journal of Human Research and Social Science Studies

ISSN(p): 3050-547X, ISSN(e): 3050-5488

Volume 03 Issue 10 October, 2026

DOI: https://doi.org/10.55677/ijhrsss/13-2026-Vol03I10

Page No : 986-994

Consent Fatigue in Precision Marketing and Personal Information Compliance in Coffee Brands: Can Library Information Literacy Education Serve as A Consumer-Side Correction Mechanism?

Chen Chenwei

School of Economics and Management, Yunnan Open University

ABSTRACT: Precision marketing ecosystems depend on continuous extraction of user consent, yet empirical research documents a growing phenomenon of consent fatigue in which users routinely click "I agree" without reading privacy notices, eroding the substantive voluntariness upon which consent-based personal data regulation rests. This paper examines coffee brands—particularly their loyalty apps, mobile ordering platforms, and IoT-enabled personalization systems—as a paradigmatic site where high-frequency, low-stakes data collection interactions generate repeated consent requests and amplify fatigue. Drawing on interdisciplinary scholarship from law, human–computer interaction, consumer behavior, and library and information science (LIS), the paper develops a three-layer framework of consent failure: structural (dark patterns and interface design), psychological (privacy fatigue and cynicism), and educational (privacy literacy deficits). It argues that regulatory enforcement and corporate self-regulation alone cannot compensate for the consumer-side information asymmetry, and proposes that library information literacy education—reconceptualized as privacy literacy instruction—can serve as a corrective mechanism by building consumers' procedural knowledge, critical evaluation skills, and behavioral self-efficacy. The paper concludes with a four-module pedagogical curriculum and discusses boundary conditions, limitations, and directions for future empirical research.

Corresponding Author:
Chen Chenwei

Published Online:
October 30, 2026

License:
This is an open access article under the CC BY 4.0 license:
https://creativecommons.org/licenses/by/4.0/

KEYWORDS:
consent fatigue, privacy fatigue, precision marketing, personal information compliance, coffee brands, library information literacy, privacy literacy, consumer protection

Cite the Article: *Chenwei, C.(2026). Consent Fatigue in Precision Marketing and Personal Information Compliance in Coffee Brands: Can Library Information Literacy Education Serve as A Consumer-Side Correction Mechanism?. International Journal of Human Research and Social Science Studies,3(10),986-994. https://doi.org/10.55677/ijhrsss/13-2026-Vol03I10*

INTRODUCTION

Every day, consumers encounter dozens of requests to consent to data collection. A coffee shop app asks for location tracking; a loyalty program requests access to contacts; a mobile ordering platform requests camera and microphone permissions. Each individual request appears minor—a click, a toggle, a checkbox. Yet accumulated across hundreds of digital touchpoints, these requests produce what scholars increasingly describe as consent fatigue: a cognitive and emotional state in which users disengage from privacy decisions, default to acceptance, and abandon meaningful evaluation of what they are agreeing to (Richards & Hartzog, 2019; Tang et al., 2021).

Coffee brands occupy a distinctive position in this ecosystem. Unlike social media platforms whose core product is advertising, coffee retailers sell a physical consumable—but their digital loyalty and ordering systems have made them de facto data companies. Starbucks' Deep Brew artificial intelligence platform processes over 100 million transactions per week across 30,000 stores worldwide (Elias, 2021), while Luckin Coffee and competing third-wave brands in China have built their business models around app-exclusive ordering, personalized promotions, and granular user profiling. Each transaction within these systems requires the consumer to have previously consented to terms of service, privacy policies, and data processing practices that most people cannot meaningfully parse.

The regulatory architecture of personal data protection—from the European Union's General Data Protection Regulation (GDPR) to China's Personal Information Protection Law (PIPL), enacted in 2021—rests heavily on consent as the legal basis for processing. Yet a growing body of empirical evidence demonstrates that consent, as currently implemented, fails to deliver informed, voluntary, and revocable permission. Instead, it has become a performative ritual in which users click through notices to access services they want, while companies check a compliance box (Nouwens et al., 2020; Utz et al., 2019).

This paper addresses a question that has received insufficient attention at the intersection of marketing ethics, data protection law, and library and information science (LIS): Can library information literacy education serve as a consumer-side correction mechanism for consent fatigue in precision marketing? The argument proceeds in three steps. First, it synthesizes the literature on consent fatigue, dark patterns, and the privacy paradox to establish that the problem is not merely individual irrationality but a structural asymmetry between platforms and users. Second, it analyzes coffee brand data practices as a concrete site where consent failure is particularly visible because of the high frequency and low stakes of each interaction. Third, it examines the emerging field of privacy literacy instruction in academic and public libraries and proposes a pedagogical framework through which information literacy education can counteract fatigue by building consumers' procedural knowledge, critical evaluation capacity, and behavioral self-efficacy.

The contribution of this paper is threefold. Conceptually, it bridges three disliteratures that rarely converse: privacy law and psychology, retail and marketing studies, and LIS education. Empirically, it draws on verified findings from field experiments on consent interfaces, surveys of privacy fatigue, and evaluations of library privacy literacy workshops. Practically, it offers a curricular blueprint that librarians, marketing ethics educators, and consumer protection advocates can adapt to specific contexts.

LITERATURE REVIEW

The Pathology of Digital Consent and Consent Fatigue

Consent has become the foundational legitimating principle of the digital economy. Terms of service, privacy policies, cookie banners, permission dialogs, and loyalty program onboarding flows all invoke consent as if it were a uniform, unproblematic act of authorization. Yet Richards and Hartzog (2019), in their influential analysis of "the pathologies of digital consent," argue that the practical conditions under which digital consents are obtained fall far short of the legal and ethical ideal of knowing and voluntary agreement. They identify multiple pathologies: unwitting consent (users do not know what they are agreeing to), coerced consent (consent is bundled with access to essential services), and incapacitated consent (users lack the time, expertise, or attention to evaluate complex privacy terms). The further a consent practice departs from three conditions—infrequent choice, vivid and imaginable harm, and correct incentives for deliberate decision-making—the more pathological it becomes.

The phenomenon Richards and Hartzog describe has been operationalized in the privacy literature as privacy fatigue. Distinct from privacy concern—the cognitive appraisal of risk—privacy fatigue is an emotional and attitudinal response characterized by emotional exhaustion and cynicism toward privacy protection. Tang et al. (2021), surveying 426 mobile app users, found that privacy fatigue has a stronger effect on disclosure intention than privacy concern itself, and that neuroticism positively predicts fatigue while agreeableness and extraversion show divergent effects. Tian et al. (2022), using propensity score matching on mobile social media users, demonstrated that cynicism reverses the normally positive relationship between privacy concern and protection behavior, while emotional exhaustion weakens the intention to protect privacy. In other words, the more people worry about privacy, the more exhausted and cynical they become—and the less likely they are to act on that concern.

This finding helps explain the long-noted privacy paradox: the gap between consumers' stated desire for privacy and their actual behavior of readily disclosing personal information. Bandara et al. (2020), through semi-structured interviews with online shoppers, found that the paradox is not a matter of hypocrisy or irrationality but of psychological distance from privacy harms, perceived social benefits of disclosure, and learned helplessness in the face of complex data practices. Svirsky (2019), in a series of online experiments, documented information avoidance: even users willing to pay nearly an hour's wages for privacy will give away their data for small bonuses if given the opportunity to avoid seeing the privacy consequences of their choices. Cofone and Robertson (2018) similarly argue that behavioral biases and information overload render formal consent mechanisms ineffective, requiring structural rather than purely informational interventions.

Compounding these psychological factors are structural design choices known as dark patterns—user interface designs that nudge or manipulate users toward less privacy-protective choices. Nouwens et al. (2020), scraping consent management platform designs across the top 10,000 UK websites, found that only 11.8% met minimal legal requirements, and that removing the opt-out button from the first screen increased consent rates by 22–23 percentage points. Utz et al. (2019), running field experiments with over 80,000 users, showed that seemingly minor decisions about notice position, choice type, and framing substantially alter consent outcomes. Habib et al. (2022) evaluated 12 consent interface variants with over 1,100 participants and found that fully blocking interfaces with in-line options and persistent change-permission buttons best balance usability and privacy. Gray et al. (2021) and Machuletz and Böhme (2020) further demonstrated that default selection of "accept all," asymmetric button emphasis, and bundling of multiple purposes systematically bias consent outcomes. Soe et al. (2020), analyzing 300 cookie consent notices from online

news outlets, documented a taxonomy of circumvention-by-design dark patterns that effectively nullify the intent of GDPR consent requirements.

Precision Marketing, Personal Data Compliance, and the Coffee Brand Context

Precision marketing—also called behavioral targeting or programmatic advertising—relies on the continuous collection, analysis, and exchange of personal data across the digital advertising ecosystem. Veale and Zuiderveen Borgesius (2022) provide a detailed analysis of real-time bidding (RTB) systems, arguing that adtech architecture is structurally difficult to reconcile with European data protection law: GDPR requires prior consent for RTB, transparency requirements are nearly impossible for publishers and RTB companies to meet, and the system incentivizes insecure data processing. Galli et al. (2022) extend this critique to the regulation of consent in targeted advertising more broadly, concluding that informed consent, as currently operationalized, provides weak consumer protection because of information asymmetry, power imbalances, and the complexity of adtech data flows.

Tiwari et al. (2024), analyzing India's Digital Personal Data Protection Act of 2023 in global context, note that the post-cookie landscape is pushing companies toward first-party data architecture and consent managers as mechanisms to address consent fatigue. Yet they caution that consent managers themselves risk becoming another layer of the compliance theater unless they are designed to facilitate genuine, granular, and revocable consent rather than to streamline maximum-data collection.

Coffee brands occupy a distinctive niche in this landscape because they combine physical retail with intensive digital data practices. The case of Starbucks is illustrative. What began as a simple loyalty card program has evolved into a sophisticated digital ecosystem: the Starbucks Rewards app had 22.9 million active users in the United States by 2019, with mobile orders making up 26% of US sales (Elias, 2021). The company's Deep Brew AI platform leverages data from 100 million weekly transactions to optimize store locations, supply chains, inventory management, and personalized marketing. The app requests location data, purchase history, payment information, device identifiers, and—in some markets—biometric payment verification. Each of these data flows requires consent, typically obtained through a bundled terms-of-service agreement during app onboarding.

Lim et al. (2024) document what they call the "Starbucks effect": the use of customers' first names on orders increases store preference and service satisfaction, but this positive effect is mitigated or reverses under conditions where privacy concerns arise—even when the customer is only asked for a first name and could provide a fake one. This finding underscores the tension inherent in coffee brand personalization: the very practices that build brand loyalty and customer experience also generate privacy vulnerabilities, and the consent mechanisms intended to authorize those practices are precisely the ones suffering from fatigue.

In the Chinese context, the PIPL, effective November 2021, establishes consent as a foundational principle of personal information processing, alongside transparency, purpose limitation, and data minimization. Song (2023) argues that the Chinese regime differs from the EU model in that state power takes precedence over both individual consent and corporate obligations, with details of enforcement remaining underspecified. Zhou et al. (2024), examining 13 Chinese online platforms before and after PIPL implementation and interviewing 30 users, found persistent non-compliance in privacy policies—particularly regarding risk assessments for sensitive data—and discovered that over half of interviewees believed the government could access their personal data without explicit consent. This perception further undermines the perceived efficacy of consent: if users believe their data will be accessed regardless of their choices, the incentive to engage critically with consent requests diminishes, reinforcing fatigue and disengagement.

Privacy Literacy and the Library as Information Infrastructure

If consent fatigue is both a psychological and a structural problem, education appears as an obvious—though insufficiently theorized—response. The library and information science (LIS) field has a long tradition of information literacy instruction, and in recent years a subfield of privacy literacy instruction has emerged. Cooke (2018), introducing a special issue of IFLA Journal on privacy and libraries, frames privacy as a core value facing unprecedented threats in the big data era and positions libraries as uniquely trusted institutions for helping patrons navigate information ecosystems.

Hartman-Caverly and Chisholm (2020), surveying academic libraries in the United States, document the rationales, topics, methods, and barriers associated with privacy literacy instruction. They identify a conceptual model of privacy as preserving zones of informational agency and trace the history of privacy culture in US libraries from the ALA Library Bill of Rights of 1939 to contemporary surveillance concerns. Their survey finds that while many librarians recognize the importance of privacy instruction, barriers include limited training, lack of curricular integration, and uncertainty about how to assess learning outcomes.

The Digital Shred project, documented by Hartman-Caverly et al. (2023), provides a concrete model. This multi-institutional privacy literacy workshop, first offered in person in 2019 and moved online during the COVID-19 pandemic, draws on concepts of reputation management, behavioral surplus, data doubles, data governance, and information security damage assessment. Using active and inclusive learning pedagogy, the workshop engages participants in hands-on exercises that demystify data collection practices. Formative assessment feedback suggests that participants value the theory-informed, personalized approach and report increased motivation to manage their privacy.

Umar (2021) argues that privacy literacy should be integrated into digital media literacy education more broadly, emphasizing skills such as understanding personal data flows, analyzing the benefits and risks of information sharing, and practicing

conscious communication. Fulkerson et al. (2016) revisit the role of metacognition and metaliteracy in the ACRL Framework for Information Literacy for Higher Education, arguing that the Framework's emphasis on reflective practice and social participation provides a natural home for privacy literacy: metaliterate learners understand themselves as both consumers and creators of information, and they reflect on the ethical implications of their information behaviors.

The question of whether privacy literacy education actually changes behavior is addressed by Boerman et al. (2023), who conducted a longitudinal three-wave experiment in the Netherlands (N = 1,000 at wave 1) testing three intervention strategies derived from Protection Motivation Theory: increasing threat awareness, training effective protection behavior, and addressing privacy fatigue. Their findings are instructive: the training strategy—teaching concrete skills—increased self-efficacy and response efficacy, immediately increased all privacy protection behaviors, and had lasting effects on tracking blocking and deletion behavior. The threat-awareness and fatigue-focused strategies did not produce their anticipated effects, though the fatigue strategy had a short-term positive effect on cookie rejection. This suggests that procedural, skill-based education is more effective than simply raising anxiety or telling people to care more.

Thomas (2022), reviewing research on public libraries and online privacy protection, concludes that libraries are well-positioned to serve as community privacy educators because of their longstanding ethical commitment to patron privacy, their trusted non-commercial status, and their existing infrastructure for digital literacy instruction. Yet significant gaps remain: most research focuses on academic libraries in North America, and little attention has been paid to how privacy literacy education might function in non-Western contexts or how it might specifically address consent fatigue in commercial transactions.

THEORETICAL FRAMEWORK: TOWARD A CONSUMER-SIDE CORRECTION MECHANISM

The literature reviewed above suggests that consent failure in precision marketing is not attributable to any single cause but arises from the interaction of three layers. The first is structural: interface designs, business models, and adtech infrastructures that systematically bias consent outcomes toward maximum data collection (Nouwens et al., 2020; Veale & Zuiderveen Borgesius, 2022). The second is psychological: privacy fatigue, cynicism, information avoidance, and learned helplessness that cause users to disengage from privacy decisions (Tang et al., 2021; Tian et al., 2022; Svirsky, 2019). The third is educational: a widespread deficit in procedural privacy knowledge—the skills and understanding needed to navigate consent interfaces, configure privacy settings, and assess data practices (Boerman et al., 2023; Hartman-Caverly & Chisholm, 2020).

Regulatory enforcement primarily targets the structural layer. GDPR fines, PIPL enforcement actions, and CCPA/CPRA regulations aim to force companies to design consent mechanisms that are transparent, granular, and freely given. Corporate self-regulation—consent management platforms, privacy by design, first-party data strategies—also operates at the structural level. Yet even well-designed consent interfaces cannot protect users who lack the knowledge, motivation, or attention to engage with them. Conversely, even the most knowledgeable user cannot easily resist a fully blocking dark pattern that has been deliberately engineered to maximize clicks. The three layers interact: structural manipulation produces psychological fatigue, which in turn prevents educational interventions from taking root, because exhausted and cynical users do not seek out or retain privacy knowledge.

This paper proposes that library information literacy education—reconceptualized to include privacy literacy as a core component—can function as a consumer-side correction mechanism that addresses the educational layer and thereby moderates the psychological layer. The argument is not that education can replace regulation or corporate compliance; it cannot. Rather, education can complement structural interventions by building the human capacity needed to make consent mechanisms actually work. Just as freedom of speech requires an educated electorate to function meaningfully, consent-based data protection requires privacy-literate consumers.

The library is a particularly promising site for this intervention for four reasons. First, libraries already have a mandate and infrastructure for information literacy instruction, whether in academic settings (course-integrated instruction, workshops) or public settings (community programs, digital literacy classes). Second, libraries are trusted, non-commercial institutions—patrons do not suspect them of having a stake in maximizing data collection. Third, libraries serve diverse populations across age, socioeconomic, and digital skill levels, which is critical for addressing the digital divide in privacy literacy. Fourth, the LIS profession has an established ethical commitment to patron privacy, codified in the ALA Code of Ethics and IFLA statements, which provides a values foundation for privacy education (Cooke, 2018; Thomas, 2022).

From this framework, three propositions follow. Proposition 1: Privacy literacy education that emphasizes procedural knowledge and skill-building (rather than merely raising awareness of risks) will increase consumers' self-efficacy and willingness to engage with consent interfaces critically. Proposition 2: The effectiveness of such education will be moderated by structural interface design; even knowledgeable users will struggle against aggressively manipulative dark patterns. Proposition 3: Library-delivered privacy literacy education will have greater credibility and reach than industry- or government-delivered programs because of the library's trusted, non-commercial positioning. These propositions provide a research agenda for empirical testing and frame the pedagogical proposal developed later in the paper.

Analysis: Coffee Brand Consent Practices and Compliance Gaps

To illustrate how the three layers of consent failure operate in practice, this section analyzes coffee brand data practices through the lens of the theoretical framework. The coffee retail context is particularly instructive because it involves repeated, low-stakes transactions in which the cumulative data collection footprint is large even though each individual interaction feels trivial.

Consider the typical onboarding flow for a major coffee brand loyalty app. Upon first opening the app, the user is presented with a welcome screen and prompted to create an account using a phone number or email. Immediately, a terms of service and privacy policy agreement appears, typically presented as a scrolling text block with a single "Agree" button at the bottom. The user must also grant permissions: location access (to find nearby stores and enable location-based offers), push notifications (to receive promotional messages), camera access (for scanning payment codes), and sometimes contact list access (to invite friends and earn rewards). Each permission request is a separate consent moment, but they arrive in quick succession, producing what might be termed micro-consent fatigue: the user clicks through each dialog reflexively to reach the functional core of the app—ordering coffee.

Structurally, several dark pattern techniques are common in these flows. The "accept all" default pre-selects all data sharing options; granular controls are buried behind a secondary screen; the "Agree" button is visually prominent while the "Decline" option is subtle or text-only; and consent is bundled—the user cannot access basic ordering functionality without agreeing to marketing communications and data sharing that may not be necessary for the transaction. Nouwens et al. (2020) found that these exact design choices can increase consent rates by more than 20 percentage points, even when users would prefer more restrictive settings.

Psychologically, the coffee context amplifies fatigue through what might be called the small-transaction problem. Unlike a social media platform, where users may have some awareness of trading data for a free service, a coffee purchase feels like a straightforward commercial exchange: money for a product. The idea that ordering a latte involves consenting to behavioral profiling, location tracking, and cross-device advertising attribution is not salient to most consumers. Each individual data request feels trivial—what harm could sharing my coffee order history cause?—and the cumulative effect of hundreds of such trivial consents is a detailed behavioral profile that drives precision marketing. Bandara et al. (2020) identified this as psychological distance: privacy harms feel abstract and distant, while the immediate benefit of faster ordering and reward points feels concrete and immediate.

The educational layer is equally visible. Most consumers do not know what Deep Brew-style AI systems do with their purchase data, what data brokers receive their information through adtech exchanges, or how to adjust app-level permissions after initial onboarding. They cannot distinguish between data necessary for fulfilling the order (payment method, delivery address) and data collected for marketing purposes (preference profiling, location tracking, device fingerprinting). When users do attempt to exercise their GDPR or PIPL rights—to access, correct, or delete their data—they often find the process confusing, time-consuming, or effectively obstructed by companies that make data deletion harder than data collection (Zhou et al., 2024).

The compliance gap analysis under both GDPR and PIPL reveals the consequences. Under GDPR, consent must be freely given, specific, informed, and unambiguous; bundled consent and pre-checked boxes are explicitly non-compliant. Yet field studies consistently find widespread non-compliance in commercial consent interfaces (Nouwens et al., 2020; Utz et al., 2019). Under PIPL, consent must be obtained for each specific processing purpose, and sensitive personal information requires separate consent; yet Zhou et al. (2024) found that post-PIPL privacy policies on major Chinese platforms still showed inadequate risk assessments and unclear purpose specification. Coffee brands, as high-frequency consumer touchpoints, are both subject to these regulations and frequent sites of compliance failure.

This analysis makes clear why a purely regulatory or corporate response is insufficient. Even if every coffee brand perfectly complied with consent requirements—which they do not—consumers would still need the knowledge and motivation to engage with those consent choices meaningfully. Conversely, even the most privacy-literate consumer cannot easily opt out of data collection if every competing coffee brand requires app-based ordering and bundles consent as a condition of purchase. The consumer-side correction proposed in this paper operates at the intersection: it cannot fix structural problems, but it can help individuals navigate them more effectively, and collectively, privacy-literate consumers create market and regulatory pressure for better design.

DISCUSSION: CAN LIBRARY INFORMATION LITERACY EDUCATION SERVE AS A CONSUMER-SIDE CORRECTION?

The analysis above suggests that consent fatigue in coffee brand precision marketing arises from the interaction of structural, psychological, and educational factors. The question now is whether library information literacy education can meaningfully address the educational layer and thereby serve as a consumer-side correction mechanism. This section examines the mechanisms through which privacy literacy education might work, the boundaries of what it can accomplish, and the conditions under which it is most likely to be effective.

The core mechanism is the transformation from passive consent-clicking to critical information evaluation. Traditional information literacy instruction teaches students to evaluate sources, identify bias, and understand how information systems work.

When extended to privacy literacy, these skills map directly onto consent challenges: evaluating privacy policies as information sources, identifying persuasive design techniques (dark patterns) as a form of bias, and understanding the data ecosystems behind precision marketing as information infrastructure. Fulkerson et al. (2016) argue that the ACRL Framework's metaliteracy approach—which emphasizes metacognition, social participation, and the learner as both consumer and creator of information—is particularly well-suited to this extension. A metaliterate consumer does not just click "Agree"; they reflect on what they are agreeing to, why the interface is designed the way it is, and what alternatives they have.

Boerman et al.'s (2023) longitudinal experiment provides empirical support for this mechanism. Their finding that skill-based training—not threat awareness or fatigue management—was the only intervention that produced lasting behavior change suggests that privacy literacy education should focus on procedural knowledge: how to adjust app permissions, how to use privacy-enhancing technologies, how to read a privacy policy, how to submit a data access request. This aligns with Filipczuk's (2022) experimental finding that procedural privacy knowledge—knowing how to control one's privacy—has a greater impact on consent decisions than factual knowledge about data collection practices. The implication is that library privacy literacy workshops should be hands-on and skill-oriented rather than purely informational or anxiety-provoking.

The library's trusted, non-commercial positioning is a critical advantage. When a coffee brand's app includes an in-app tutorial about privacy, users rightly suspect that the tutorial will minimize risks and maximize data sharing. When a government agency publishes privacy guidance, users may perceive it as authoritarian or disconnected from their daily concerns. Libraries, by contrast, have a longstanding reputation as neutral, user-centered institutions whose mission is to empower individuals rather than to sell products or enforce regulations. Thomas (2022) notes that the ALA Code of Ethics has protected patron privacy since 1939, and this historical commitment provides a foundation of trust that commercial or government privacy education programs cannot easily replicate.

It is equally important to acknowledge what information literacy education cannot do. First, it cannot compensate for structural power imbalances. A consumer who has been trained in dark pattern recognition still faces a take-it-or-leave-it choice when a coffee brand requires app-based ordering and bundles consent with access. Second, education has diminishing returns under conditions of extreme fatigue. Tian et al. (2022) found that cynicism can completely reverse the relationship between privacy concern and protection behavior; a deeply cynical, exhausted consumer may not seek out or retain privacy education. Third, the digital divide means that those who most need privacy education—older adults, low-income users, less digitally literate populations—may be the least likely to access library workshops. Public libraries are well-positioned to reach these groups, but resource constraints and outreach challenges remain.

These limitations suggest that privacy literacy education is a complement to, not a substitute for, regulatory enforcement and corporate compliance. The most effective approach is a multi-layered one: regulations require companies to design consent interfaces that are fair and transparent; companies implement privacy-by-design practices that minimize data collection; and privacy-literate consumers can engage with the remaining consent choices meaningfully. Education is the consumer-side layer that makes the other two layers actually work, because even a well-designed consent interface is useless if users cannot or will not engage with it.

There is also a feedback loop to consider. As privacy literacy becomes more widespread, consumers collectively create market demand for better privacy practices and provide political support for stronger regulation. Library privacy literacy education thus has both direct effects (empowering individual consumers) and indirect effects (cultivating a more privacy-conscious citizenry). This aligns with the broader role of libraries in democratic society: not merely providing access to information, but building the critical capacities needed for informed participation in an information-saturated democracy.

Pedagogical Proposal: A Privacy Literacy Curriculum for Consumer Empowerment

Building on the theoretical framework and empirical evidence reviewed above, this section proposes a four-module privacy literacy curriculum designed for delivery through academic and public libraries. The curriculum is grounded in the Digital Shred model (Hartman-Caverly et al., 2023), the ACRL Framework (Fulkerson et al., 2016), and the findings of Boerman et al. (2023) that skill-based training produces the most durable behavior change. It is designed to be adaptable to different contexts—academic libraries can integrate it into information literacy courses for business or e-commerce students, while public libraries can offer it as community workshops.

Module 1: Understanding Data Ecosystems and Behavioral Surplus. This module introduces the basic architecture of digital data collection: what data is collected, who collects it, how it flows through adtech ecosystems, and how it is used for precision marketing. Using the coffee loyalty app as a case study, learners trace the journey of a single transaction—from app onboarding, through RTB auctions, to personalized advertising—and identify the different actors (the coffee brand, ad networks, data brokers, analytics providers) involved. Key concepts include behavioral surplus (Zuboff, as discussed in Hartman-Caverly et al., 2023), data doubles, and the difference between first-party and third-party data. The module combines short presentations with a visual mapping exercise where learners draw the data flow from a coffee ordering app to their own social media feeds.

Module 2: Decoding Consent Interfaces and Dark Patterns. This module teaches learners to identify and critically evaluate consent interfaces. Drawing on the taxonomies developed by Nouwens et al. (2020), Gray et al. (2021), and Soe et al. (2020),

learners examine real screenshots of cookie banners, app permission requests, and loyalty program onboarding flows, and identify specific dark pattern techniques: forced action, sneaking, hidden costs, disguised ads, confirmshaming, and asymmetry of choice. The module includes a practical exercise where learners redesign a deliberately manipulative consent flow to make it more transparent and user-centered. This module directly addresses the structural layer of consent failure by building recognition skills.

Module 3: Practical Privacy Management: Tools, Settings, and Habit Formation. This module is the most skill-oriented, consistent with Boerman et al.'s (2023) finding that behavioral training produces the most durable effects. Learners work on their own devices to adjust privacy settings on their phone operating systems, review app permissions, configure ad tracking preferences, set up password managers and two-factor authentication, and learn how to submit data access and deletion requests under GDPR or PIPL. The module emphasizes small, achievable actions rather than overwhelming learners with complex technical tools. A habit-formation component helps learners integrate privacy practices into routine behavior—for example, reviewing app permissions quarterly, declining unnecessary permission requests by default, and reading privacy notices when creating new accounts rather than clicking through automatically.

Module 4: Advocacy and Digital Citizenship. The final module moves beyond individual behavior to collective action. Learners explore their rights under GDPR, PIPL, and other relevant regulations, discuss how to file complaints with data protection authorities, and examine how consumer advocacy groups use privacy literacy as a tool for systemic change. The module also addresses the social dimensions of privacy: how data practices affect marginalized communities, how algorithmic profiling intersects with discrimination, and how libraries can serve as community spaces for privacy advocacy. This module connects individual empowerment to broader digital citizenship, consistent with the metaliteracy emphasis on social participation (Fulkerson et al., 2016).

Assessment of the curriculum should use a pre-test/post-test design measuring three outcomes: knowledge (understanding of data ecosystems, consent mechanisms, and privacy rights), attitudes (privacy self-efficacy, intention to protect privacy, reduced cynicism), and behavior (actual permission settings, use of privacy tools, filing of access requests). Long-term follow-up at three and six months would assess retention and habit formation, addressing the gap noted by Boerman et al. (2023) where some effects decayed over time.

Delivery channels should be diverse. Academic libraries can integrate the curriculum into existing information literacy courses for e-commerce, business, and information science students—populations that are particularly relevant because they will either work in precision marketing themselves or teach future marketers. Public libraries can offer the modules as drop-in community workshops, partnering with consumer protection agencies and senior centers to reach vulnerable populations. Online versions of the curriculum can extend reach beyond local communities, though the hands-on nature of Module 3 suggests that in-person or synchronous virtual delivery is most effective for skill-building.

LIMITATIONS AND FUTURE RESEARCH

This paper has several limitations that should be acknowledged. First, it is a conceptual and interdisciplinary analysis rather than an empirical study. The proposition that library information literacy education can correct consent fatigue is grounded in existing evidence from related domains—privacy fatigue research, dark pattern studies, and library privacy literacy evaluations—but has not been directly tested in the specific context of coffee brand precision marketing. Future research should conduct field experiments that deliver the proposed curriculum and measure its effect on consent decision-making in realistic app-onboarding scenarios.

Second, the analysis draws heavily on Western (primarily US and European) scholarship, with some attention to the Chinese context through PIPL-related research. Privacy norms, regulatory frameworks, coffee market structures, and library systems vary significantly across countries, and the proposed pedagogical model may need adaptation for different cultural and institutional contexts. Cross-cultural comparative research would be valuable, particularly in non-Western settings where library traditions, privacy expectations, and digital commerce infrastructures differ.

Third, the paper focuses on coffee brands as a paradigmatic case but does not empirically analyze specific coffee brand apps or their consent interfaces. A systematic content analysis of loyalty app onboarding flows across multiple coffee brands—using the dark pattern taxonomies developed by Nouwens et al. (2020) and others—would provide concrete evidence about the nature and prevalence of consent design practices in this sector.

Fourth, the long-term behavior change effects of privacy literacy education remain understudied. Boerman et al.'s (2023) longitudinal study found that some effects decayed over two months, suggesting that one-time workshops may be insufficient. Future research should explore spaced repetition, micro-learning interventions, and community-based reinforcement models that sustain privacy behaviors over time.

Finally, the paper does not address the role of technological solutions—such as privacy-enhancing technologies, browser-based consent agents, or machine-learning tools that automatically negotiate privacy settings on behalf of users. Filipczuk's (2022) research on agent-based privacy negotiation suggests that technological intermediaries may reduce the burden on users. Future research should examine how information literacy education and technological solutions complement each other: educated users are

better equipped to choose, configure, and trust automated privacy agents, while effective agents reduce the cognitive load that produces fatigue in the first place.

CONCLUSION

Consent fatigue in precision marketing represents a systemic failure at the intersection of technology, business models, regulation, and human cognition. Coffee brands, with their high-frequency, low-stakes digital interactions and sophisticated loyalty app ecosystems, offer a particularly clear window onto this failure. The consent mechanisms that are supposed to empower consumers have become rituals of acquiescence, manipulated by dark patterns, exhausted by repetition, and undermined by a widespread lack of procedural privacy knowledge.

This paper has argued that regulatory enforcement and corporate self-regulation, while necessary, are insufficient on their own. They operate primarily at the structural layer of consent failure and cannot compensate for the psychological and educational layers. Library information literacy education—reconceptualized as privacy literacy instruction—can serve as a consumer-side correction mechanism that builds the procedural knowledge, critical evaluation skills, and behavioral self-efficacy needed to make consent mechanisms actually work. The library's trusted, non-commercial, community-embedded position makes it uniquely suited to deliver this education to diverse populations.

The contribution of this paper is to bring together three literatures that rarely converse—privacy law and psychology, retail and marketing studies, and LIS education—and to propose a concrete pedagogical framework. The four-module curriculum outlined here is grounded in empirical evidence about what works (skill-based training over awareness-raising) and what the barriers are (fatigue, structural constraints, digital divide). It is offered not as a panacea but as one important component of a multi-layered approach to restoring meaningful consent in the digital economy.

For librarians, the implication is that privacy literacy should be recognized as a core component of contemporary information literacy, not as an optional workshop topic. For marketing ethics scholars and practitioners, the implication is that consumer education is not a substitute for fair consent design but a necessary complement. For regulators, the implication is that enforcement action should be paired with public investment in privacy education, delivered through trusted institutions like libraries. Only through this kind of coordinated, multi-layered effort can the pathology of digital consent begin to be treated—one informed click at a time.

FUNDING SUPPORT

The paper is supported by the Yunnan Open University (Yunnan Technical College of Industry) Science and Technology Team (Cultivation) "Digital Marketing of Yunnan Small Grain Coffee Brand"(Project No.: 2025YKFP01)

REFERENCES

1. Bandara, R., Fernando, M., & Akter, S. (2020). Explicating the privacy paradox: A qualitative inquiry of online shopping consumers. Journal of Retailing and Consumer Services, 52, 101947.
2. Boerman, S. C., Strycharz, J., & Smit, E. G. (2023). How can we increase privacy protection behavior? A longitudinal experiment testing three intervention strategies. Communication Research, 50(2), 179–208.
3. Cofone, I. N., & Robertson, A. Z. (2018). Consumer privacy in a behavioral world. Hastings Law Journal, 69(5), 1243–1290.
4. Cooke, L. (2018). Privacy, libraries and the era of big data [Editorial]. IFLA Journal, 44(3), 173–177.
5. Elias, E. (2021). Is Starbucks undergoing a transition into the FinTech industry? [Undergraduate thesis].
6. Filipczuk, D. (2022). Consent mechanisms in privacy engineering [Doctoral dissertation, University of Southampton]. ePrints Soton.
7. Fulkerson, D. M., Ariew, S. A., & Jacobson, T. E. (2016). Revisiting metacognition and metaliteracy in the ACRL Framework. Communications in Information Literacy, 10(1), 21–35.
8. Galli, F., Lagioia, F., & Sartor, G. (2022). Consent to targeted advertising. European Business Law Review, 33(4), 567–590.
9. Gray, C. M., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021). Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (pp. 1–18). ACM.
10. Habib, H., Li, M., Young, E., & Cranor, L. F. (2022). Okay, whatever: An evaluation of cookie consent interfaces. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (pp. 1–21). ACM.
11. Hartman-Caverly, S., & Chisholm, A. (2020). Privacy literacy instruction practices in academic libraries: Past, present, and possibilities. IFLA Journal, 46(4), 389–408.
12. Hartman-Caverly, S., Chisholm, A., & Glenn, A. (2023). Digital shred: Case study of a remote privacy literacy collaboration. College & Research Libraries, 84(2), 245–268.

13. Lim, S., van Osselaer, S. M. J., Goodman, J. K., Fuchs, C., & Schreier, M. (2024). The Starbucks effect: When name-based order identification increases customers' store preference and service satisfaction. Journal of Retailing, 100(3), 456–474.
14. Machuletz, D., & Böhme, R. (2020). Multiple purposes, multiple problems: A user study of consent dialogs after GDPR. Proceedings on Privacy Enhancing Technologies, 2020(2), 451–468.
15. Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (pp. 1–13). ACM.
16. Richards, N. M., & Hartzog, W. (2019). The pathologies of digital consent. Washington University Law Review, 96(2), 235–302.
17. Soe, T. H., Nordberg, O. E., Guribye, F., & Slavkovik, M. (2020). Circumvention by design: Dark patterns in cookie consents for online news outlets. In Proceedings of the 11th Latin American Conference on Human-Computer Interaction (pp. 1–8). ACM.
18. Song, R. (2023). Allocating data protection duties the Chinese way. Washington International Law Journal, 32(1), 123–168.
19. Svirsky, D. (2019). Why are privacy preferences inconsistent? (Harvard John M. Olin Center for Law, Economics, and Business Discussion Paper No. 81). Harvard Law School.
20. Tang, J., Akram, U., & Shi, W. (2021). Why people need privacy? The role of privacy fatigue in app users' intention to disclose privacy: Based on personality traits. Journal of Enterprise Information Management, 34(5), 1453–1474.
21. Thomas, S. (2022). Online privacy protection and public libraries: A review of contemporary research. Public Library Quarterly, 41(3), 245–265.
22. Tian, X., Chen, L., & Zhang, X. (2022). The role of privacy fatigue in privacy paradox: A PSM and heterogeneity analysis. Applied Sciences, 12(19), 9702.
23. Tiwari, I. D., Kumari, C., Kumar, A., & Shrivastava, A. (2024). Data privacy and targeted advertising: Marketing compliance under the Digital Personal Data Protection Act, 2023 in the global regulatory landscape. Canadian Journal of Marketing Research, 10, 1–20.
24. Umar, M. (2021). Privacy literacy and digital media literacy: Can digital media literacy be used in protecting user's online privacy? Journal of Media and Communication Studies, 13(1), 1–10.
25. Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed consent: Studying GDPR consent notices in the field. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (pp. 973–990). ACM.
26. Veale, M., & Zuiderveen Borgesius, F. (2022). Adtech and real-time bidding under European data protection law. European Journal of Risk Regulation, 13(3), 545–568.
27. Zhou, M. M. Z., Qu, Z., Wan, J., Wen, B., Yao, Y., & Lu, Z. (2024). Understanding Chinese internet users' perceptions of, and online platforms' compliance with, the Personal Information Protection Law (PIPL). In Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems. ACM.