



Law & Ethics for Digital Product Management

PMDE EEP

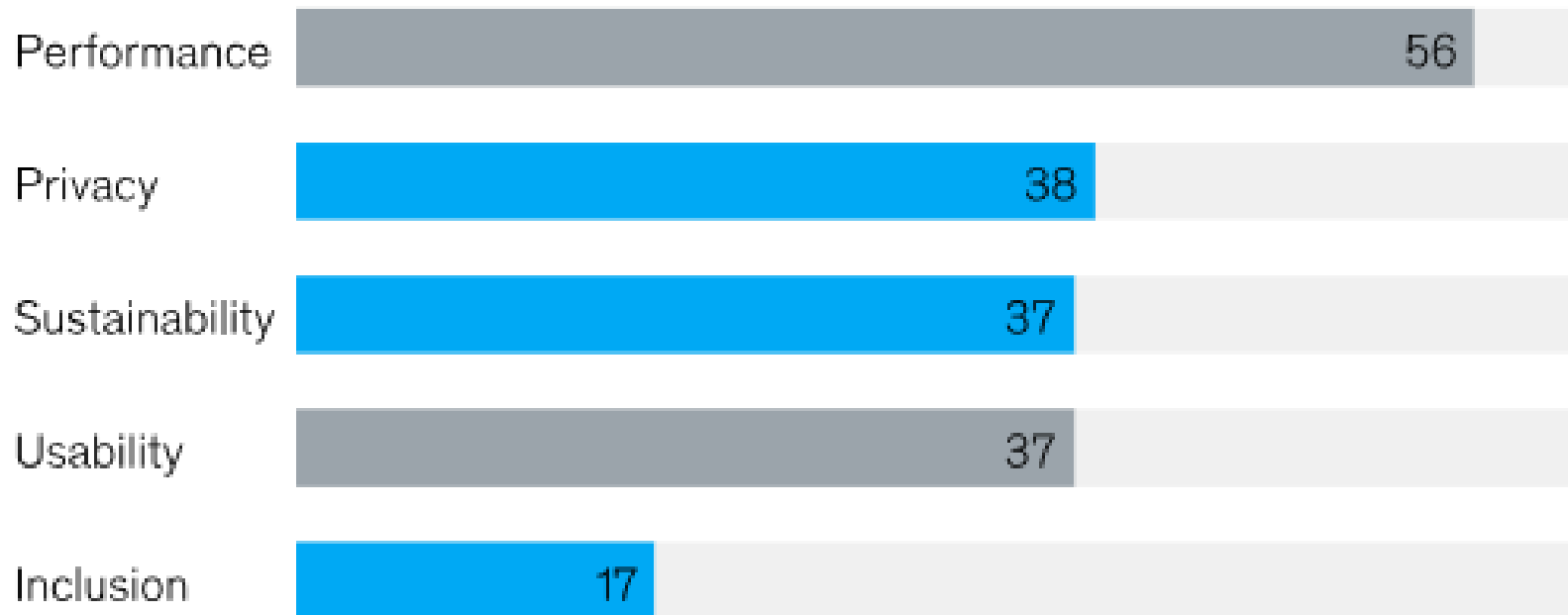
NEENA PANDEY, IIMV

The Latest Concerns

- Stages of Product Development
 - Product development – Privacy: data collection, usage and sharing
 - User-interaction design - Habit-forming products
 - Marketing of products - Dark Patterns
- Type of Digital Products
 - Content-based products – Privacy & Moderation; Copyright
 - AI-based products – Privacy, Bias, and Explainability, Hallucinations

Responsibility dimensions' ranking (Source: McKinsey Report)

Share of respondents who rank the following dimensions as one of their top two product-development priorities, % (n = 52)



Problem addressing sustainability issue

(Source: McKinsey Report)

Share of respondents who cite the following as challenges to incorporating sustainability into the development process, % (n = 52)

Limited capability building, tools, and shared understanding of what “good” looks like

35

No central policy on sustainability dimensions

24

No link to performance metrics

23

Subjective metrics

18



Personal Data Privacy

- Personal data classification
- Reasonable expectation – consumer awareness
- Consent Framework - boilerplate
- Obligation of Data Fiduciaries

What is Personal Data?

- Personal Data – whether the data is related to an identified or identifiable individual
 - Protection of personal data ~ Objective of protecting an individual's identity
 - Developments in data science have changed the understanding of identifiability
- Methods of Removing Identification
 - Anonymization
 - Process of removing identifiers from personal data in a manner ensuring that the risk of identification is negligible
 - Mathematical and technical methods to distort data irreversibly ensure that identification is not possible
 - Pseudonymization
 - Method by which personal identifiers are replaced with pseudonyms
 - Important component of privacy by design
 - Carries a risk of re-identification without specific technical and organizational measures
 - Anonymized Data (no more personal data) vs. Pseudonymized Data (personal data)

Sensitive Personal Data

- Data integral to an individual's identity
- Processing of this data can lead to graver concern, hence stricter rules
- Criteria to 'categorize' data as sensitive:
 - Likelihood of causing significant harm to the individual
 - Expectation of confidentiality to that category of data
 - Significant discernible class of data principals could suffer harm or a similar nature
- Residuary power vested with the DPA (Data Protection Authority)
- *Passwords, Financial data; health Data; Official identifiers including government-issued identity cards; sex life and sexual orientation; biometric & genetic data; transgender status or intersex status; caste or tribe; and religious or political beliefs or affiliations*

Consent

- *Expression of a person's autonomy or control, consequent to allowing another person to legally disclaim liability for acts which have been consented to*
- Enabled through notice – affirmative obligation placed on data fiduciaries
- Advantage of consent – in principle
 - It respects user autonomy
 - Provides a clear basis for the entity to whom the consent is given to disclaim liability, if reqd.
 - Hence, the meaningfulness of consent shall be carefully determined
- Current Operational Framework
 - Complex and boilerplate
 - Unequal bargaining power of parties and ineffective in informed consent

New Consent Framework

- Informed Consent
- Explicit Informed Consent

Privacy by Design Principles

- Proactive and not Reactive
- Privacy as the Default
 - Data minimization, data sharing restriction, unused data purging, Correct usage of opt-in and opt-out options
- Privacy Embedded into Design
 - Encryption, authentication, testing vulnerabilities at every stage
- Full functionality
 - May not need to sacrifice functionality for privacy
 - Not zero-sum, but positive-sum

Privacy by Design

- End-to-end security
 - Security ensure throughout data lifecycle – from collection to deletion
- Visibility & Transparency
 - Communication with customer – Privacy policy, Data breaches
- Respect for User Privacy
 - User-centric – prioritize transparency, allow granting/withdrawal of consent as per user wish (user control of data)

Competitive Edge offered by 'Privacy by Design'

- Indicates seriousness of business towards their CSR
- Cisco's 'Privacy Benchmark' report – high correlation between privacy investments and sales delay
- Quality Software Development
- Product Differentiation - Effective Marketing
- Promotion of Robust Privacy Culture
- Secondary Gains
 - Reduced compliance costs, Certification from global privacy standards, Ease of operations, Enhanced transparency, Goodwill

KPIs for Product Managers

- Data breach incident rates
 - Analyze, reduce, vulnerability assessment
- Privacy policy compliance
 - Organization's, Country's
 - Tracking non-compliance - e.g., Amazon
- Number of customer complaints related to data privacy
- Data subject data-related requests
- Data deletion and retention rates

User content-based Products

- Facebook, Twitter, Blogs etc.
- Legal & Ethical Issues
 - Content moderation – subjectivity, biasedness
 - Copyright violation
 - Deep-fakes
 - Hallucinations
 - Echo-chamber effect

Marketing Dark Patterns

- False Urgency/Scarcity
 - False data on high demand, time-bound pressure
- Basket sneaking
 - Automatic addition of ancillary services; pre-ticked boxes, subscription added to single service purchase
- Confirm Shaming
 - Create a sense of fear, shame, or guilt
- Forced Action
 - Prohibiting a user from continuing with the product/service with the conditions contracted for, unless they upgrade for a higher rate or fees
- Subscription Trap
 - Instruction for subscription cancellation complex, ambiguous, latent, confusing etc.; authorization for auto debits to avail free subscription

Marketing Dark Patterns

- Interface interference
 - 'X' opening up another ad rather than closing it
- Bait & Switch
 - Deceptively serving an alternate outcome in place of a chosen outcome
- Drip Pricing
 - Revealing price elements post-confirmation of purchase
- Disguised advertisement
 - Masking advertisements as other types of content
- Nagging
 - Request overload; insistence on sharing phone numbers etc.

References

<https://www.haveignition.com/kpis-for-product-managers/kpis-for-product-managers-product-data-privacy>

<https://www.privacypolicies.com/blog/privacy-by-design/>

<https://www.dp-institute.eu/en/the-competitive-edge-of-privacy-by-design-in-product-development/>

<https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/responsible-product-management-the-critical-tech-challenge>