QUESTIONS THAT ANY LABELING SCHEME SHOULD BE CAPABLE OF ANSWERING:

1. What proportion of consumers are expected to change their purchasing behaviour due to the security labeling? [Will this proportion be large enough to influence producers to strengthen the security of their products/ services?]
2. Who decides on the security status labeled? [Is the standard so prescriptive that conformance is obvious and binary? Is it decided by the product/ service producer alone? Is it the producer, validated by an external independent conformance assessor?]
3. How does the labeling capture the scale of the security risks posed by the product/ service? [Does the labeling illustrate some measure of security risk to reflect the stringency of security controls?] Eg.

Medium Risk Medium Controls	High Risk High Controls
Low Risk Low Controls	Medium Risk Medium Controls

4. How are the subjective judgements in the risk assessment captured in the labeling? [Are these moderated by an independent external conformance assessor?]
5. How does the labeling inform customers about the degrading of security status from the point of conformance assessment or latest firmware update? [Would such information be meaningful to the majority of consumers?]
6. What baseline security controls objectives/ controls are product/ services expected to conform with? [Are these the 'Security Measures for "EO-Critical Software"…', as tested by 'Guidelines on Minimum Standards for Developer Verification of Software'?]
7. How are the security risks posed by upstream component suppliers and downstream distribution and maintenance suppliers communicated within the labeling? [Is the risk assumed from suppliers captured in the labeling, rather than just transferred to consumers?]
8. How are the security risks posed by open source software communicated within the labeling? [Again, who handles the risks and how are consumers expected to handle transferred risks?]
9. How might the security labeling reflect the variety of products/ services offered to consumers and their respective security contexts? [From a power station to a connected doorbell?]
10. How might one model the degrading of security status over time? [CVE discovery modelling offers one approach to estimating how long before a technology becomes vulnerable.]
11. If the security status changes over time, how does the labeling communicate this? Eg.

This device does not meet this rating
Security of use before 09/2025
Security of use after 09/2025
Security of use after 09/2030

12. How would a point of purchase security status labeling be altered if the estimate of security status over time was inaccurate and a producer wants to decrease or increase the estimated duration of a security status? [Does this militate against a fixed point-of-purchase labeling? If instead the digital labeling can be updated remotely, would all products/ services be capable of allowing this, and what would happen if the product/ services was not updated?]
13. How might one model the degrading of security status through space? [From a product/ service directly connected to the backbone to one connected to a mesh network with constrained power, processing, data storage, and security functionality.]
14. Should the labeling note a time in the future when user functionality, or security functionality will degrade sufficiently to be limited or the product/ service become inoperable? [Time limited security functionality from initial security assessment or latest firmware release. What about the PII stored on the product/ service, would it be deleted, access to it disabled, or remain open to access without security controls?]
15. How are consumers informed about the meaning of the labeling at point of purchase? [What minimum level of detail is required?]
16. How are those purchasers who buy the product/ service on the secondary market informed of the implications of the labeling? [Does communication about the labeling require secondary registration?]
17. How are users of the product/ service kept up to date with security status without degradation of their privacy rights? [How are purchasers, secondary purchasers, non-purchasing users tracked in a privacy-sensitive way? Purpose limitation of such customer PII may be difficult to enforce.]
18. Would an update require an active response from the consumer, and if so, what if the consumer is not capable of executing this response, does their user functionality or security status degrade more than for those who actively respond? [A warning to scan a QR code for upgrade instructions may be a viable upgrade approach, but may be beyond the capability of a significant minority of consumers.]
19. How might the security labeling be communicated to vulnerable consumers, or those with sensory impairments?
20. How might the security labeling take into account the cultural communication norms of consumers? [Red-Amber-Green Labeling may appear different to an East Asian consumer than to a Western consumer.]
21. How does the labeling communicate that if a user repairs their product, the security status is altered? [This might be more important due to the recent Executive Order on 'Right to Repair'.]
22. How does the labeling communicate the balance in product liability/ consumer protection between the user expecting to buy a perpetual licence to a product/ service, and the reality of a time-limited user/ security functionality? [Does this amount to in-built obsolescence, and how does this relate to the circular economy and the recent Executive Order on 'Right to Repair'?]
23. If the security controls and their testing are too strict and costly to implement, consumers may choose to purchase unregulated products/ services that provide a lower level of security? [Security vulnerabilities introduced by unregulated products/ services could expose regulated products/ services to security threats.]
24. Will the security labeling and the underlying controls become mandatory in order to prevent the legitimate sale of unregulated products/ services?
25. Would a regulator such as the FCC or FTC be mandated to enforce any mandate?
26. Due to their limited power, processing, data storage, and security functionality, will constrained products/ services automatically have a lower graded labeling than unconstrained products/ services? [Would this impair the growth of the mesh-connected aspects of the IOT market?]

Kieran McDonagh MSc LLM CISSP CISA CIPP/E

Principal of Riskscape Law Ltd, London, UK

Member of: ISO PC 317 Privacy by Design for Consumer Goods (alongside Kaitlin Boeckl); BSI IOT/1; and ETSI Cyber