JOINT INDUSTRY STATEMENT ON SOFTWARE (OS) UPDATE REQUIREMENTS ACROSS EU REGULATORY INITIATIVES

Executive Summary

To achieve various policy goals pertaining to sustainability, cybersecurity and consumer rights, a significant number of regulatory instruments and initiatives have been introduced in the EU proposing to regulate the way operating systems should be updated, upgraded, installed and secured. When evaluated in isolation, each independent regulatory proposal may seek to advance the public interest and convenience. However, when read in conjunction the different provisions do not complement each other, introduce legal uncertainty, stand at odds with each other, threaten to fragment the internal market and in some instances undermine the policy objectives related to the security and safety of end-users.

We are particularly concerned with some of the requirements surrounding the provision of software (OS) updates mandating consumers be entitled to roll back security updates and install OS of their choice. Furthermore, proposals for mandated periods, lack of alignment under different directives and disregard of standard industry practices adds technical complexity for servicing. Releasing operating system updates with the upcoming rules will introduce legal uncertainty and place undue burden on sellers of electronic devices who are required to inform users about

availability of software updates for the different products they sell, and ensure these updates are installed as well as third parties who leverage software to develop programmes and services. And while some directives mandate products to be sold with the latest available version of the digital component installed, others mandate users be enabled to reject and roll back security updates which introduces conflicting requirements and undermines security policies and industry best security practices.

Discussion

With increased innovation, digital connectivity, societal reliance on connected products and expansion of the attack surface, the focus on software updates has increased,[1] including the number of proposed policies. This has resulted in a fragmentation of proposed requirements related to software updates, across regimes underlining different interests, creating untenable regulatory environment and contradiction. This fragmentation is standing in direct tension to achieving the underlining purpose or effectively balancing competing objectives and may lead to broad unintended consequences.

Amongst others, software update-related provisions and requirements are contemplated across the following policy regimes: Radio Equipment Regulation, Product Liability, Safety Regulation, Cybersecurity, Privacy, Sustainability and Eco-Design, Consumer Contracts, the NLF and more.[2] This adds to existing regimes (e.g. GDPR), which may interact with software update requirements, leading to increased conflict. Some of the proposals include contradicting overly prescriptive technical requirements (e.g., requirements on immediate provisioning of updates and rollback requirements).

Reducing this regulatory fragmentation is key to ensure proposals are striking a sound balance between potentially competing principles. Furthermore, this fragmentation presents barriers for the ecosystem, industry, civil society, standard bodies and technical experts to engage on potential proposals and impedes the ability of maintaining regulations that accommodate the needs of evolving technology and landscape, including emerging threats. This regulatory fragmentation is especially challenging given the need to ensure proposals are technical feasible, not overly prescriptive and consider the complexity of ecosystem collaboration needed for effective update provisioning and adoption.

The discussion below on the Eco-Design Regulation for Smartphones and Tablets presents an urgent case study illustrating these concerns – it also highlights an opportunity to consider a broader policy approach towards addressing mutual challenges associated with software update-related provisions.

Concerns with Proposed Update Provisions at Eco-Design Regulation for Smartphones and Tablets

The Ecodesign Regulation's main objective is to develop a policy framework which promotes the manufacturing and sale of energy efficient products in the EU market and reduces the negative

[1] The importance of updates is also underlined in the Cybersecurity Strategy for the Digital Decade.

[2] Partial list includes Eco-Design Regulation for Smartphones and Tablets, Sales of Goods Directive and the Digital Content Directive (EU 2019/771 and 2019/770) regimes, E-Privacy proposal, RED Directive security and privacy provisions, Network and Information Security Directive 2.0, EU Cybersecurity Act (and its implementation) including related certification programs, NLF, and the proposed EU Cyber Resilience Act.

environmental impact of products during their lifecycle. While such a goal is laudable, the corresponding requirements, particularly with regard to software updates, need to be aligned to other current, and upcoming Commission initiatives to avoid legal fragmentation, conflicting expectations on service providers, unintended societal consequences and undermining objectives of other regulations (e.g. securing users), and the inadvertent introduction of barriers to the trade of goods within the internal EU market.

- *Lack of clarity regarding the mandated period of time related to providing security software operating system updates:* We are concerned about the lack of clarity as to when the period begins which is further complicated by the lack of a unified approach to defining update support periods under different EU Directives; we note flexibility is needed to ensure security update periods take into account the various needs of ICT products sectors and technical complexities. Industry best practices is to track the support period from the supported product launch.

- *Rigid timelines or cadence for security & functionality updates:* Quality cannot be assured if deadlines for updates are mandatorily set. Processes to develop updates, prepare them for public release in a manner that increases adoption are highly complex. An eco-system of various businesses cooperate to deliver that seamless and secure user experience. However, continuous complex organizational processes can experience unforeseen or uncontrollable delays. Mandating rigid deployment deadlines does not recognize this complexity and could force immature deployment to the users' detriment. It is also inconsistent with international standards for coordinated vulnerability disclosure and security best practices.

- *Uninstall security updates/ Rollback:*
  Mandating that users be able to rollback to previous versions of the OS is contradictory to the policy under different directives requiring products sold in the market to be installed with the most recent OS version. Not only has there been no empirical data demonstrating how enabling users to revert to a previously installed OS version maximizes the longevity of a product, but the negative consequences of said mandate on the resilience and security of the ecosystem and app compatibility has not been thoroughly studied, vetted and understood.

Conclusion

Our organizations urge EU policymakers to consider the following considerations as they progress with considering update-related requirements:

- Ensure sufficient coordination between the relevant committees
- Reduce regulatory contradiction and duplicity across regimes
- Ensure sufficient consideration of unintended consequences, notably on the security of the ecosystem at large
- Avoid an overly prescriptive approach that does not take into account technical challenges or industry best practices (including the considerations above)

Supporting associations:

AFNUM: Alliance Française des Industries du Numérique

ACT: The App Association

Ametic: Association of Electronics, Information and Communciation Technologies, Telecommunication and Digital Content Companies (Spain)

ANITEC – ASSINFORM: Associazione Italiana per l'Information and Communication Technology

bitkom: Branchenverband der deutschen Informations- und Telekommunikationsindustrie

BSA: The Software Alliance

Developers Alliance

Digital Poland

Elektronikbranschen (Sweden)

FEEI: Fachverband der Elektro- und Elektronikindustrie (Austria)

iSFE: Europe's Video Games Industry

iT Branchen: Danish ICT Industry Association

ITI: Information Technology Industry Council

JEITA: Japan Electronics and Information Technology Industries Association

NLdigital: Trade Association for IST and Telecom Companies in the Netherlands

NUMEUM: Syndicat professionel de l'écosystème numérique in France

sp: Confederation of Industry of the Czech Republik

Technology Ireland/IBEC: Irish Business and Employers' Confederation

techUK: The UK's Technology Trade Association

For more information please contact:

Philippe de Cuetos, AFNUM

Director of technical and regulatory affairs

pdecuetos@afnum.fr