ITI Comments to European Data Protection Board Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive

18 January 2024

The Information Technology Industry Council (ITI) is the premier voice, advocate, and thought leader for the global information and communication technology (ICT) industry. Our member companies include the world's leading innovation companies, with headquarters worldwide and value chains distributed around the globe. ITI member companies represent the breadth of the technology ecosystem, including semiconductor and computer hardware and software companies, network equipment manufacturers and suppliers, cybersecurity providers, and leading Internet services and consumer technology companies.

Privacy and trust are central to our member companies' businesses and global operations. Together with our members, ITI works with governments, regulators, and stakeholders around the world to strengthen and align approaches towards data protection and privacy that safeguard individual rights and promote innovation.

I. Introduction

ITI appreciates the opportunity to provide comments to the proposed European Data Protection Board Guidelines 2/2023 on the Technical Scope of Article 5(3) of the ePrivacy Directive[1] ("the Guidelines").

ITI is concerned that the Guidelines expand a widely accepted interpretation of Article 5(3) that will affect the provision of many different types of online services, and that the Guidelines risk going beyond the original legislative intent of the ePrivacy Directive.

Online identifiers are central to the proper technical functioning of the internet, providing consumers with secure, high-quality service and performance, as well as facilitating and simplifying the consumer online experience. The use and application of cookies and other online identifiers continues to rapidly evolve, with business models adapting to improve transparency and further empower users to safeguard their privacy.

Legislative reforms to the ePrivacy Directive have stalled since 2017. As such, there is a need for the European Commission, co-legislators and regulators to reconsider how to move forward with ePrivacy rules that are workable for both consumers and internet services, and consistent with the EU's General Data Protection Regulation. Efforts to amend or expand the interpretation of Article 5(3) therefore require careful consideration and should take account of wider policy developments, as well as the changing technical requirements for current and future online consumer products and services.

[1] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2023/guidelines-22023-technical-scope-art-53-eprivacy_en

ITI believes that any significant amendments to the generally understood scope of Article 5(3) should form part of a wider legislative discussion on ePrivacy reform, with sufficient opportunity for stakeholder input and debate.

II. Overly broad interpretation of key terms

"Gaining Access" and "Storage"

The Guidelines expand the current interpretation of what constitutes "gaining access", bringing within scope any software instruction requesting information from an end-user's terminal equipment. The Guidelines also expand the interpretation of "storage" to include information stored by any entity on the end-user's terminal equipment or "produced through processes and programs executed on the terminal equipment".

These changes, coupled with EU data protection authorities' narrow reading of the Article 5(3) consent exemption (for "technical storage or access…strictly necessary…to provide the service"[2]), would mean that important routine internet services, which do not have direct contact with end-users, would be required to obtain consent from end-users. This includes services such as certain content delivery networks, cybersecurity services, and other services that rely on IP-peering or other forms of cross-customer analysis to maintain performance, ensure security and detect fraud. This could also lead to situations whereby end-users unknowingly disable these critical features.

Furthermore, the Guidelines' open-ended interpretation of "gaining access" to include information automatically transmitted, e.g. via a communication protocol, could be read to include any form of communication over the internet, potentially vastly increasing consent requirements for end-users.

"Information", "Terminal Equipment", and "Electronic Communication Network"

Additionally, the EDPB outlines criteria for "information", "terminal equipment", and "publicly available electronic communication services in public communication networks". In our view, each of these criteria, in addition to "gaining access" and "storage", is too broad and does not take into consideration an assessment of the level of privacy risk but rather aims to cover all use cases. As currently drafted, this risks going against industry best practice and disrupting the provision of important services as set out above.

III. Specific concerns relating to IoT Devices and Cybersecurity

An expanded interpretation of Article 5(3) may have significant implications for different Internet of Things product functions. Such functions implement a wide range of processing operations, such as reporting configuration information, submitting error reports and the near-constant monitoring of the operational state of the device or software in question. This moves the conversation to

[2] Article 29 Working Party, WP 294, Opinion 04/2012 on Cookie Consent Exemption, adopted on 7 June 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

software security, which is a completely different set of concerns, best practices, and considerations.

Consent may be difficult, impracticable, or even impossible to obtain in this instance as well as for other use cases set out in the Guidelines, especially for B2B companies. Additionally, the proposed guidelines present a problem for “web audience measurement”, that in certain cases is not used for any profiling purposes.

Additionally, the EDPB highlights use cases where Article 5(3) may or may not apply and states the rule does not apply if information is processed locally and does not leave a device but does apply in essentially every other use case, including URL and pixel tracking, tracking based on IP and using unique or persistent identifiers. The EDPB does not consider how these technologies can be used to protect users’ privacy and the integrity of the user’s equipment. For example, in cybersecurity, pixel tracking can be used as an authentication measure to ensure the person logging into a system is who they say and not an adversary. A wider consultation process on ePrivacy reform is required to ensure that organizations and consumers can continue to use the best-in-class cybersecurity measures to protect themselves from bad actors.

IV. Conclusion

Absent a wider debate on ePrivacy reform, ITI respectfully requests introducing language to limit the proposed expanded scope of Article 5(3), in particular regarding the interpretation of “gaining access” and “storage”. If this is not possible, we would welcome a more detailed consideration of how the Guidelines would affect the provision of the many critical online services that fall outside of the “strictly necessary” exemption and the related impact on the consumer online experience.

This could include an assessment of whether the original processing goals set out in Article 5(3), coupled with the Guidelines’ strict interpretation, remain fit for purpose in light of technological developments, and given that today’s products and services increasingly rely on the exchange of technical information with end-user devices as part of their overall broader functionality. This includes cutting-edge content delivery networks and cybersecurity services, as well as routine performance monitoring of devices and services, such as for troubleshooting, debugging and quality assurance purposes.

ITI remains available to discuss these issues further with the EDPB, and we also look forward to continuing to work with the EU and stakeholders at the international level towards a more joined-up, pragmatic global approach to the use of online identifiers.