The Unintended Impact of the Draft EU ePrivacy Regulation on Cybersecurity

BSA | The Software Alliance (BSA), the leading advocate for the global software industry, believes the European Commission's proposal for an ePrivacy Regulation (ePR) will play an important role in preserving the principle of the confidentiality of communications. However, we are concerned that, as proposed, the **draft ePR is overly restrictive and could lead to several unintended and negative consequences for the EU digital economy, particularly with respect to cybersecurity.** Please find below a set of examples that highlight the potential impact of the draft ePR:

Cybersecurity Business Examples (Articles of concern: 5, 6 and 8)

Reporting significant incidents: Under the Network and Information Security (NIS) Directive, digital service providers (DSPs) are mandated to notify competent authorities of incidents that have a significant effect on the continuity of their services.

» **Article 6 would not make this possible:** Article 6 of the ePR only allows e-Communications and Over-the-Top (OTT) providers to process electronic communications data for the purpose of maintaining or restoring the security of networks and services. All other NIS Directive covered sectors cannot benefit from this exception because they do not fall within the scope of Article 6. Moreover, Article 6 does not include any general permissions for processing obligations laid down in Union or Member State law — including obligations entailing reporting to national regulators.

Processing metadata to detect botnets: When thousands of devices emit the same type of message simultaneously, it is likely the sign of botnet activity, such as a distributed denial of service (DDoS) attack. Such an attack is visible in internet traffic metadata patterns because all devices emit the same type of data packets targeting the same recipient(s). By analyzing and observing such metadata over public networks, cybersecurity providers can detect and eliminate botnets.

» **Articles 5 and 6 would not make this possible:** Article 5 of the ePR prohibits anyone from "processing" electronic communications data unless they are an end-user (e.g., a consumer speaking to another consumer or business over a communication service) or are expressly permitted to process data under grounds set out in the ePR. Article 6 sets out those grounds, but only permits processing by electronic communication service (ECS) and electronic communication network (ECN) providers. Cybersecurity providers that are not end-users, ECSs or ECNs (e.g., a third-party cybersecurity provider) will not be permitted to process the data.

more >>

The draft ePR is overly restrictive and could lead to several unintended and negative consequences for the EU digital economy, particularly with respect to cybersecurity.

Processing content data to detect malware: Malware is often distributed via electronic communications such as email or instant messaging. It can take various shapes, including malicious files sent as attachments and links pointing to compromised websites. By inspecting the content of electronic communications before they are delivered to a recipient, cybersecurity providers can detect and block the sending of malware.

» **Articles 5 and 6 would not make this possible:** Third-party cybersecurity providers will not be classified as "end-users" under Article 5 and will not be able to benefit from the grounds set out in Article 6 because they will not be classified as ECSs or ECNs. Even if they were to fall within the parameters of Article 6, the requirement of "double end-user consent" would be unworkable because it would require obtaining consent from the malicious actor.

Processing terminal equipment data: To ensure the integrity of networks and systems, legitimate cybersecurity providers execute a multitude of actions, including inspecting digital certificates, sending vulnerability patches, and monitoring diagnostic data to detect malfunctions. By sending, accessing and collecting data from terminal equipment, device vendors and third-party cybersecurity service providers are able to ensure that the ecosystem is safe from vulnerabilities.

» **Article 8 would not make this possible:** Article 8 places a strict consent requirement on all third-party cybersecurity providers prior to being able to access a device or terminal. Such a requirement is neither workable for non-personal devices (e.g., industrial control system components) nor for all personal devices (e.g., smart boilers, smart shutters, smart lightbulbs, etc.) because they often do not have a suitable interface to seek and express consent. The security of the Internet of Things ecosystem cannot be managed solely at the device level. Instead it must be managed at the network level. Subjecting the ability to manage and secure billions of devices to the capacity and willingness of users to express consent will erode the EU's cyber-resilience.

Solutions

To ensure that the draft ePR does not undermine the EU's cyber-resilience, the Regulation should be amended in the following manner:

» **Article 5:** The scope of the draft Regulation should be clarified and limited to data *"in transmission"* across publicly available communications networks.

» **Article 6:** The processing of electronic communications metadata (Art. 6(2)) and content data (Art. 6(3)) for network and information security purposes needs to be explicitly permitted. This permission must apply not only to entities in scope (i.e., ECSs and ECNs) but to any other third parties with a legitimate interest. This permission should extend entirely to protecting the network and information security of users and third parties and not be limited to "self-defence."

» **Article 8:** Accessing the storage and computing capabilities of devices (Art. 8(1)) along with collecting and processing the data emitted by devices (Art. 8(2)) for network and information security purposes needs to be explicitly permitted. This permission should apply to third parties with a legitimate interest without the need for user consent.