e-Privacy proposal: A roadblock to innovation

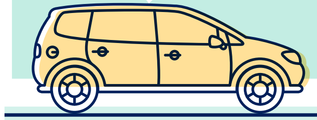
AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Questions?
Maika Föhrenbach
Policy Adviser, AmCham EU
MFO@amchameu.eu
amchameu.eu

Data-driven innovation

is a key driver of economic growth and societal well-being

EUROPEAN DATA ECONOMY



The General Data Protection Regulation (GDPR) provides a strong EU framework for ensuring trust and safety in the use of digital technologies

Currently under implementation

The European Commission e-Privacy proposal outlines rules on confidentiality of electronic communications. However, the business community is concerned that its **restrictive** nature and **overly broad scope could hinder innovation in the data economy**

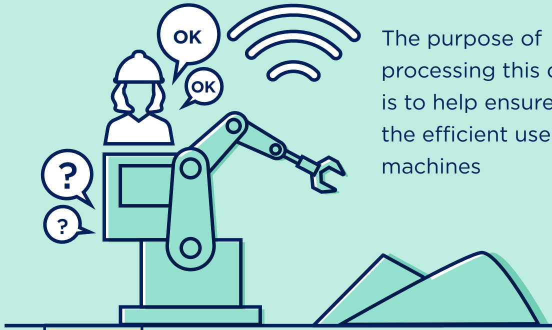
3 MAJOR OBSTACLES

Scope

Problem: Requiring consent from the end user in machine-to-machine (M2M) communication interrupts workflow and threatens safety

Scenario: Nora works in construction

The machines she operates have sensors, which today automatically transmit information about their functioning to the manufacturer



The purpose of processing this data is to help ensure the efficient use of machines

UNDER E-PRIVACY

Nora needs to give consent for the machine to send data via the sensors. If consent is not given, it puts **maintenance and safety** efforts **at risk** and **undermines** the construction site's **efficiency**

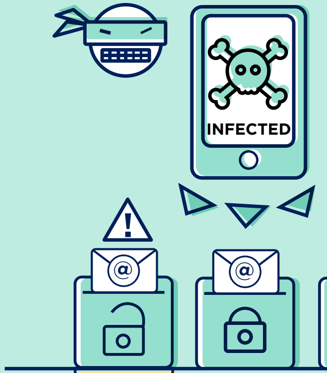
Recommendation:
Exclude M2M communication from the scope of the e-Privacy proposal

Legal processing

Problem: The e-Privacy proposal rules would limit companies from processing important metadata and content

Scenario: Lukas' smartphone is compromised and infected by cybercriminals

Without Lukas knowing, his smartphone is sending malicious emails to his contacts



Under the GDPR, security teams may process metadata and content data of a personal device in legitimate interest to prevent the cyber threat

UNDER E-PRIVACY

Processing this data would not be allowed in most cases by providers of electronic communications networks and services, leading to **weaker security** and **privacy protection for the user**

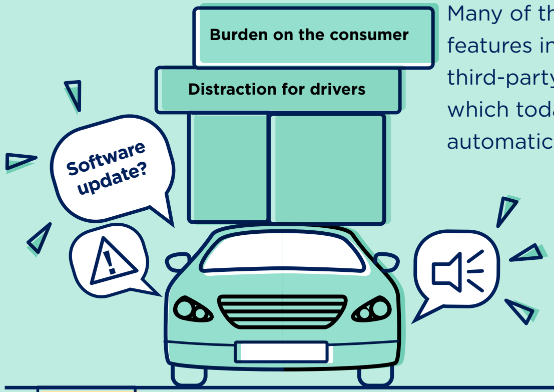
Recommendation:
Align proposal with GDPR framework and the flexibility it provides

Consent rules

Problem: Overly strict consent requirements place a burden on the consumer

Scenario: Eva just bought a new car

Her new car has features that enhance safety and driver experience



Many of these features integrate third-party software which today update automatically

UNDER E-PRIVACY

To maintain proper functioning of the car, Eva must continuously provide consent for each third party software update. This places the **burden** on Eva and puts the **functioning** of the car **at risk**

Recommendation:
We need flexible rules that make sense to consumers based on the sensitivity of data, not the provider of the service