ANNEX 2
Background on outstanding M2M/IoT issues concerning the proposed ePrivacy Regulation

This paper provides more detailed background to explain the text proposals contained in Annex 1, focusing on key grey areas that remain in consideration of the European Commission's non-paper on ePrivacy and new technologies.[1]

Solutions to the issues described below, as suggested in Annex 1, are essential to enabling existing and future M2M and IoT use cases. The development of AI based on such use cases is also vital for Europe's future economic competitiveness.

This paper refers extensively to guidance from data protection authorities (DPAs) as well as to court cases. It is complemented by examples of M2M/IoT scenarios to illustrate our points.

Definitions

The Commission's non-paper states that the scope remains unchanged for the transmission of M2M services (Art. 6) under the ePrivacy Regulation (ePR) compared to the ePrivacy Directive. As a consequence, the non-paper reinstates that only transmission is covered by Art. 6 as opposed to processing on the server of the M2M service provider, which does not fall within the ePR's scope.

While we welcome these basic parameters, their application to concrete use cases is not always clear-cut and the examples provided in the Commission's non-paper do not address less straightforward but deciding aspects.

In summary, the ePR's application to 'transmission' means that Art. 6 will only apply insofar as the data processing in question is carried out in the context of a publicly available electronic communications service (ECS). Understanding whether any given processing activity can be conceived to fall within this definition is therefore key.

a) ECS

It is worth recalling that while the ECS definition was laid down 17 years ago, its parameters are still being debated in at least two ongoing CJEU cases.[2] Importantly, both such CJEU cases revolve around the element of 'conveyance of signals on electronic communications networks.'

Even though the explicit recognition of 'interpersonal communications services' in the new telecoms framework is helpful to exclude some M2M/IoT use cases,[3] the same fundamental questions around the definition of 'conveyance of signals' still stand and are key to understanding whether Art. 6 would apply. Such questions include:

[1] WK 510/2019 INIT.

[2] C-142/18 and C-193/18.

[3] The new EECC definition of ECS (Art. 2(4)) now explicitly includes 'interpersonal communications services,' which captures online services providing 'direct interpersonal and interactive' communications 'between a finite number of persons, whereby the persons initiating or participating in the communication determine its recipient(s).' Many M2M/IoT use cases do not fall within this definition because they lack the 'interpersonal' element. The Council has sought to more explicitly cover this under the ePR's Recital 11a, specifying that the ePR wouldn't apply 'when the entity providing the communications channel is at the same time a communicating party.'

- Can services supplied via the servers of M2M/IoT service providers, by transmitting data using the internet protocol suite, in themselves be regarded as 'conveyance of signals'?
- In the event that the M2M/IoT service provider conveys signals itself or the conveyance of signals by internet access services is in any event attributable to it, can such M2M/IoT service, irrespective of any additional functions of the service, also consist 'wholly or mainly' in the conveyance of signals?
- Even if the ECS definition does not in principle include M2M/IoT services supplied over the open internet and which do not themselves provide internet access, can the ECS definition exceptionally apply where the M2M/IoT service provider simultaneously operates a number of its own internet-connected electronic communications networks that can be used, inter alia, for the purposes of the M2M/IoT service?
- Can the criterion of 'normally provided for remuneration' also apply when the service is financed in part or in full by third parties, e.g. public budgets, rather than paid for directly by the person to whom the service is provided?

Far from being theoretical, all the above questions have been the subject of Member State enforcement and are currently being tried before the CJEU.[4]

b) Publicly available

Ultimately, the ePR's application rests on the interpretation of how a given service is construed from a technology and business perspective. Whether a service is 'available to the public' is a key factor to determine whether the regulation applies.

The Commission has reinstated that Art. 6 – and, for that matter, Art. 8 – only applies insofar as the communication happens, directly or indirectly, via publicly available networks. The Commission states that this would normally exclude private networks such as connected factories.[5]

However, the definition of 'publicly available' has itself been subject to much interpretation. For example, BEREC indicates that in principle any ECS that is available to any user who wants to use such service or network should be considered to be publicly available. This includes virtual private networks (VPNs), which are typically provided to anyone who wishes to use the service.[6]

DPAs themselves have stated that 'in practice, the notions of "public communications network" and "electronic communications services" are very often unclear. Services are increasingly becoming a mixture of private and public elements and it is often difficult for regulators and for stakeholders alike to determine whether the ePrivacy Directive applies in a given situation.'[7]

To add to this, the ePR expands its scope to 'wireless networks accessible by anyone in public and *semi-private* spaces,' including where the communications service is 'ancillary to other services.'[8] This brings into scope many use cases where M2M communications are ancillary to other services and are

[4] See in particular C-193/18.

[5] Example 2 on p. 4, WK 510/2019 INIT.

[6] See p. 5, BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules.

[7] P. 4, Article 29 Working Party Opinion 2/2008 on the review of Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive).

[8] Recital 13 ePR, emphasis added. While this language has been introduced to cover processing under Art. 8(2), it does make more general points about the applicability of the entire ePR. Note that the emphasis on the ancillary aspect mirrors the ePR's expanded definition of 'interpersonal communications service' in Art. 4(2).

deployed in public or semi-public environments such as hospitals, smart cities, connected public transport and transport infrastructure.[9]

Who is the end-user?

An 'end-user' is a legal entity or natural person using or requesting a publicly available electronic communications service who is not at the same time providing public communications networks or publicly available electronic communications services.[10]

In many M2M/IoT use cases, this creates an obligation to obtain consent from both the individuals or entities subscribing to a service and the individuals actually using a given service or device, as illustrated by this example:

> [A] car rental service installs a smart vehicle tracking device in its rental cars. Although the car rental service will be considered the owner/subscriber of the device/tracking service, the individual renting the car qualifies as the device user. [The ePrivacy Directive] then requires the device manufacturer to (at least) obtain the consent of the device user, in this case the individual renting the car.[11]

Moreover, the processing of M2M/IoT data 'may also concern individuals who are neither subscribers nor actual users of the IoT. For instance, wearable devices like smart glasses are likely to collect data about other data subjects than the owner of the device. It is important to stress that this factor does not preclude EU law from applying to such situations.'[12]

Technologies that could be in scope

Below we provide a non-comprehensive list of M2M/IoT use cases to illustrate our points above:

- Connectivity for factories can be provided by mobile operators, third-party providers, directly by the factory owners themselves or through a combination thereof based on a variety of business models, many of which have not emerged yet. One factory may decide to deploy and operate its own connected equipment in a local private network using dedicated licensed, sublicensed or unlicensed radio spectrum; another may purchase from telecoms operators tailored communications services implemented in 5G network slices; another may use a VPN service delivered over the internet access service it provisions from telecoms operators. The ePR may apply to all or some of these business models.
- Smart metering infrastructure can (partly) make use of public networks to transfer meter data to utilities that collect such data for the management of their grid, as part of their legal obligations. Smart meters or related devices such as smart meter gateways are, however, installed and operated by the utility in what is technically a closed network, where end-users cannot install and connect meters by themselves and information is encrypted, authenticated

[9] 'Such an expansion [brings] all publicly available networks and services (wired or wireless, public or privately owned or managed) within the scope of the confidentiality requirements.' See p. 8, Article 29 Working Party Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC).

[10] Art. 2(14), Directive (EU) 2018/1972.

[11] P. 14, Article 29 Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things. See also Recital 19b, doc. 6771/19: 'Providers of electronic communications services may, for example, obtain the consent of the end-user for the processing of electronic communications data, at the time of the conclusion of the contract, and any moment in time thereafter. In some cases, the legal entity having subscribed to the electronic communications service may allow a natural person, such as an employee, to make use of the service. In such case, consent needs to be obtained from the individual concerned.'

[12] P. 13, Article 29 Working Party Opinion 8/2014 on the on Recent Developments on the Internet of Things.

and not accessible by third parties. The current ePR version does not explicitly exclude this information exchange.

- Energy transition, grid stability and security of supply. Managing and controlling the energy grid is already partly automated. In the future, the volume of data will increase considerably, driven by the need for smart grids. The collection and increasingly automated evaluation of metering data are indispensable for digitised and automated control of energy grids, including for the integration of decentralised generation from renewable energies, intelligent load control and demand-side management. The European specifications for smart meters lay the foundations for the introduction of smart metering systems. They form the basis for energy efficiency measures and the participation of consumers in the energy market, driven forward by the European Commission, including as 'prosumers.' Requiring consent for the use of intelligent metering systems would mean that end-users could endanger the security of the system and supply by refusing the required electronic communication which is needed for running smart grids, particularly when an extremely large number of decentralised generation plants and consumption sites need to be controlled and managed automatically.

- A patient is monitored in a hospital or at home by a connected heart monitor, provided as a service to the hospital by a medical device manufacturer. The device manufacturer has no customer relationship with the patient. The individual qualifying as end-user would need to give consent for the processing of his/her heart readings each time he or she is connected to the monitor.

- A patient is picked up by an ambulance equipped with connected medical devices and transported to the hospital. Similar to the example above, the service is delivered by the medical device manufacturer to the hospital and the device manufacturer has no customer relationship with the patient. The individual qualifying as end-user would need to give consent for the processing of his/her device readings, which in this case might be impossible because the individual may be incapable of doing so.

- Cooperative Intelligent Transport Systems (C-ITS) are deployed on road networks, allowing road users (cars, etc.) and traffic managers (road infrastructure) to share information and use it to coordinate their actions. Although it doesn't necessarily rely on telecoms networks, C-ITS is ancillary to the transport network and is available to anyone who drives cars with compatible radio functionality and could hence be considered a publicly available ECS.

- Digital signage can provide traffic signal prioritisation (for emergency or public vehicles) or optimisation (for traffic management). Unlike C-ITS, it is based purely on local processing of data from sensors or cameras that recognise an incident and can inform users purely via digital displays. But similarly to C-ITS, digital signage can be considered as publicly available – the roadway is a public space, the service is ancillary to the transport network and is being offered to an unspecified group of end-users. The end-user may comprise the transport authority (depending on whether they operate the service themselves) but also the persons in the cars involved in the incident whose data is being processed and possibly those who are provided information from the digital signage. Finally, the processing is happening during transmission in the fog node. The data in question – whether from a video source, sensor or combination – can be considered as content data.

- Monitoring crime in a smart city environment – for instance intrusion detection, licence plate recognition and behavioural analysis – can similarly be based on video or sensor data identifying a suspect or their vehicle or monitoring or acting on their behaviour. The monitoring, identification or action based on intrusion prevention takes place in a public or semi-private space. The end-user could include the suspected criminal and incidental individuals who are monitored. Processing takes place during transmission in the fog node. The

data in question – whether from a video source, sensor or combination – can be considered as content data.

- Home security systems, detecting suspected intruders or taking deterrent action in response to their presence, can be considered a publicly available service that runs on a public network offered by a telecoms provider. The end-user could include the suspected criminal. Processing takes place during transmission in the fog node. The data in question – whether from a video source, sensor or combination – can be considered as content data.

Terminal equipment provisions

Even when it states that the ePR's Art. 6 is not applicable to an M2M/IoT service, because the ECS definition doesn't apply to it, the Commission's non-paper highlights that by contrast the terminal equipment provisions (Art. 8) *will* apply. This is crucial, because any M2M/IoT service will be entirely based on data received from terminal equipment. The impact of Art. 8 is therefore very broad and needs to be considered carefully.

a) Scope of Art. 8

Contrary to the Commission's non-paper, it is important to understand how the ePR's material scope in fact differs from the current ePrivacy Directive.[13] While the current Directive has already been interpreted expansively, it only applies to the process of storing information or accessing information *already stored* in terminal equipment.

By contrast, the ePR will apply more broadly not only to the use of devices' processing functions (which itself can be interpreted very broadly, as computing devices process information by their very nature)[14] but also to the collection of information *about* terminal equipment, including software and hardware.

It is also worth noting that, like Art. 5(3) in the current ePrivacy Directive and unlike Art. 6, Art. 8 applies irrespective of the nature of the entity and makes no distinction between a data controller, data processor or a third party. In addition, it makes no difference between personal and non-personal data.[15]

b) Relationship with Art. 6 and the GDPR legal bases for processing M2M/IoT data

One aspect that merits more attention is the relationship between the ePR's Art. 8 and processing allowed on the basis of the GDPR. The crucial question is whether the *lex specialis* nature of the ePR means that Art. 8 supplants the legal bases available under the GDPR when it comes to processing terminal equipment information.

In relation to the current ePrivacy Directive, DPAs have stressed the distinction between ePrivacy consent, which applies to storage in, and access to, terminal equipment – and in the new ePR will apply

[13] Directive 2002/58/EC, as revised by Directive 2009/136/EC.

[14] DPAs have explicitly argued that the new terminal equipment provisions should also apply where data is not stored on the device 'but can also be processed (including collected and stored) elsewhere and made available through the device.' See p. 11, Article 29 Working Party Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC).

[15] See p. 7, Article 29 Working Party Opinion 02/2013 on apps on smart devices.

more broadly, as described in the section above – and GDPR consent, which applies to 'the processing of *different* types of personal data.'[16]

We stress that processing under the GDPR is here limited to *different* types of personal data, meaning that when the types of personal data covered by the ePrivacy provisions are concerned, it is the ePrivacy legal bases alone that will apply. This is clear in the example of smartphone apps, where DPAs explain that legal grounds other than ePrivacy consent can subsequently be invoked only 'for *other* types of data processing,'[17] i.e. for types of data other than those covered by ePrivacy.

The European Parliament's report has specified the relationship more explicitly by providing that 'any other processing on the basis of Article 6 of [the GDPR] should be considered as prohibited, including processing for another purpose on the basis of Article 6 paragraph 4 of that Regulation.'[18]

To sum up, even if an M2M/IoT service isn't covered by the ePR's Art. 6 as the ECS definition doesn't apply to it, the related terminal equipment data can only be processed for the specific purposes established under the ePR and not for the purposes established by the GDPR's other legal bases. Some practical implications of this are that:

a. Once terminal equipment data is acquired in compliance with the ePR's Art. 8, it cannot be used for other purposes under the GDPR's legitimate interest legal basis, which would be particularly applicable to M2M/IoT use cases involving anonymous, anonymised or pseudonymised data, as these won't, or are less likely to, impinge on user's privacy; and

b. Similarly, further processing for compatible purposes as established under the GDPR will not be possible.

For instance, terminal equipment data originally collected for providing a service requested by the end-user cannot be used for a company's internal AI-based R&D with respect to new products and services even if it has been anonymised or pseudonymised so as to provide appropriate safeguards.

[16] Ibid., p. 14 (emphasis added).

[17] Ibid, p. 16 (emphasis added).

[18] Amendment 14, A8-0324/2017.