ADVOCATEN
AVOCATS
ATTORNEYS

Jos Dumortier°
Geert Somers°
Edwin Jacobs°
Hans Graux°
Frederic Debusseré

Stefan Van Camp

Eleni Kosta°°
Davide Maria Parrilli
Ruben Roex
Yung Shin Van Der Sype
Bernd Fiten
Pieter Gryffroy
Zenzi De Graeve

° BVBA/SPRL
°° Bar of Heraklion

Legal memo with respect to the concept of metadata and its degree of sensitivity under future European e-privacy law

Executive summary

This legal memo examines the approach taken in the Proposal for an e-Privacy Regulation in relation to the lawful processing of metadata. The Proposal would currently only permit processing of non-anonymous metadata for a limited number of processing activities related to the proper functioning of electronic communications services (including transmission of the communication, billing, provision of mandatory quality of service, maintenance or re-establishment of network security), or where consent has been given by the end-user concerned.

This approach, which strongly emphasizes the importance of consent, appears to be driven by the consideration that metadata in electronic communications should be treated as a special category of personal data which is inherently sensitive. The European Court of Justice of the European Union (CJEU)'s Tele2 ruling has been referenced as a key driver behind this approach. As will be argued below, this assumption however is flawed for several reasons.

Firstly, the Tele2 ruling did not argue that metadata was sensitive by definition. Rather, the Court condemned the indiscriminate and universal collection of a very broad set of metadata, given that this data taken as a whole could establish a profile of the individuals concerned, in the context of potentially criminal activity. The nature, scope, purposes and (lack of) safeguards of the processing all contributed to the Court's decision. As will be examined below, the processing of metadata, even in the context of electronic communications, can also have very limited data protection implications. Context was critical in the Court's decision that the processing was considered as sensitive and unlawful; it did not rely solely on the nature of the data.

Secondly, the Proposal is not in line with the GDPR. The GDPR contains a list of special categories of personal data which are considered inherently sensitive; metadata is however not included in this list. Moreover, the GDPR follows a risk-based approach. This implies that data controllers, including providers of electronic communications services, must assess which risks are inherent to their processing activities, take appropriate and

documented measures to mitigate these risks, and comply with all other requirements of data protection law. By merely focusing on a consent obligation, the proposed e-Privacy Regulation deprioritises the risk-based approach. Other bases for lawful processing can be equally appropriate, if these are coupled with appropriate measures to mitigate potential risks.

Finally, the Proposal creates a discrimination, since the mandatory consent requirement would only apply to metadata which originates from electronic communications services. Metadata from other sources, such as GPS devices, online maps, cloud services or apps that do not qualify as electronic communications services, would fall under the general provisions of the GDPR (applying cumulatively with article 8 of the Proposal), meaning that e.g. such data could be further processed without consent even if all other elements of the service (risks, scope, context, purpose and safeguards) would be identical. This discrimination seems to have no justification.

In order to arrive to a consistent approach, the application of the risk-based approach of the GDPR to metadata appears to be a more effective safeguard against privacy challenges. The processing of any metadata – irrespective of its source technology or whether it originates from an electronic communications service – can create privacy challenges, and therefore may require a data protection impact assessment (DPIA), in line with the GDPR's risk-based approach and the accountability principle. This approach ensures that the nature, scope, context and purposes of the processing of the metadata are taken into consideration; that risks and impacts are identified; and that documented measures, safeguards and mechanisms for mitigating that risk are implemented, including a justification for which the controller can be held accountable.

Applying this same approach in the e-Privacy Regulation would appear to be a more appropriate and effective approach to managing and mitigating privacy challenges and would avoid creating undue discrimination.

Context

On 10 January 2017, a proposal for an EU level Regulation was adopted by the European Commission, concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (referred to as the 'Regulation on Privacy and Electronic Communications' or more commonly the e-Privacy Regulation)[1]. The proposed e-Privacy Regulation aims to particularise and complement the GDPR as regards electronic communications data that qualify as personal data. All matters concerning the processing of personal data not specifically addressed by the proposal are covered by the GDPR. The alignment with the GDPR resulted in the repeal of some provisions, such as the security obligations of Article 4 of the e-Privacy Directive. It however brings several other major revisions to existing law.

As a key example of these changes, the proposed Regulation no longer uses the old concepts of 'traffic data' and 'location data' from the e-Privacy Directive. Instead, the concept of electronic communications data is split into two categories: communications content on the one hand, and metadata on the other hand. Electronic communications data content is defined in the proposal as "the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound"; whereas metadata is defined as "data processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content; including data used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication".

Building on Article 7 of the EU Charter of Fundamental Rights, the confidentiality and privacy of both content data and metadata are protected under the Proposal, although the level and methods of protection differ. Under Article 5 of the Proposal, any interference with electronic communications data (thus including both content and metadata) by persons other than the end-users is prohibited, except when permitted by the Regulation. The concept of interference is – compared to the current ePrivacy Directive - very broad, as it does not only include listening, tapping, storing, monitoring, scanning, surveillance or other kinds of interception, but also processing in general.

Content data is slightly more stringently protected. None the less, for metadata too the bar of protection is set at a very high level: Article 6.2 of the Proposal only permits providers of electronic communications services to process electronic communications metadata if:

[1] Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), see http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017PC0010

*"(a) it is **necessary** to meet **mandatory quality of service requirements** pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120 28 for the duration necessary for that purpose; or*

*(b) it is **necessary** for **billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services**; or*

*(c) the end-user concerned has given his or her **consent** to the processing of his or her communications metadata for one or more specified purposes, including for the provision of specific services to such end-users, **provided that the purpose or purposes concerned could not be fulfilled by processing information that is made anonymous**".* [emphasis added]

The first two paragraphs (a) and (b) refer to situations where the processing is inherently necessary to ensure a limited set of activities related to the proper functioning of electronic communications services. Beyond those cases of strict necessity, processing of non-anonymous metadata is only permitted when consent has been given, which, by virtue of the applicability[2] of the definitions of the General Data Protection Regulation (EU) 2016/679 (the GDPR)[3], has to satisfy the requirements of the GDPR. This implies that the consent must be a "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her", as stipulated in Article 4 (11) of the GDPR.

Thus, in practice, whenever the necessity of processing metadata cannot be demonstrated under Article 6.2 (a) or (b), consent becomes the only option for making processing of non-anonymous metadata lawful, irrespective of the nature, context or purposes of the processing operation in question.

This straightforward but strict approach in the Proposal is driven by the consideration that metadata is inherently sensitive, and therefore requires stringent protections. The Explanatory Memorandum to the Proposal[4] links this position explicitly to a ruling of the Court of Justice of the European Union

[2] As a result of Article 4.1(a) of the Proposal, which notes that the definitions in Regulation (EU) 2016/679 (i.e. the GDPR) shall apply to the Proposal.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); see http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

[4] Also available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017PC0010

(CJEU), the so-called Tele2 case[5], stating that "metadata derived from electronic communications, may also reveal very sensitive and personal information, as expressly recognised by the CJEU" (sic); this statement is repeated verbatim in recital (2) of the Proposal. While this statement is still conditional (metadata *may* reveal sensitive information), this nuance is missing in the text of the Proposal: Article 6.2 treats metadata as sensitive by definition, and always applies the necessity/consent test. The communication on the European Commission's website similarly takes a more absolute stance, noting that within the Proposal, "privacy is guaranteed for communications content and metadata, e.g. time of a call and location. Metadata have a high privacy component and is to be anonymised or deleted if users did not give their consent, unless the data is needed for billing". Again, an assessment of the nature, context or sensitivity of the metadata is missing.

The Tele2 case therefore seems to have been a key driver in the current approach to metadata in the e-Privacy proposal, and is interpreted as supporting the notion that metadata is by definition sensitive, and therefore may only be processed when necessary (as described under Article 6.2 of the Proposal) or when consent has been given. Alternative grounds permitted under the GDPR for processing personal data are thus implicitly not available for metadata.

This is remarkable for several reasons. Firstly, the proposed e-Privacy Regulation thus implicitly seems to introduce a new type of processing of special categories of personal data (regulated under Article 9 of the GDPR), for which the generic processing justifications of Article 6 of the GDPR are deemed inappropriate, inadequate or prohibited. Secondly, the approach of the e-Privacy Regulation does not consider the new risk-based approach of the GDPR, which grants data controllers a margin of appreciation of the risks and mitigation measures for the processing of personal data, coupled with a greater responsibility and accountability duty. No appreciation of the nature, context or sensitivity of metadata is permitted in the Proposal: only necessity or consent are acceptable.

This memo aims to examine firstly whether this approach is indeed dictated by the requirements of the Tele2 case – i.e. whether the Tele2 decision indeed found that metadata was sensitive by definition and therefore requires consent by default and/or additional safeguards – and secondly whether this approach is in line with the GDPR's risk-based approach. The ultimate goal is to determine whether the approach taken by the Proposal is required and appropriate, given the need to ensure a consistently high level of personal data and privacy protection across the EU, including with respect to electronic communications, and given the need to ensure that innovation and progress in the Digital Single Market are not stifled.

[5] Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB and Secretary of State for the Home Department, ECLI:EU:C:2016:970; see http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=101544

The Tele2 case

As noted above, the Tele2 case seems to have been a significant driver behind the Proposal's approach to metadata, as witnessed by the references to it in the Explanatory Memorandum of the Proposal. It is therefore useful to examine briefly what the context, decision and implications of the Tele2 case were.

The Tele2 case as such didn't revolve around the concept of metadata in general. It originated from multiple requests for a preliminary ruling, both dating from 2015, from the Administrative Court of Appeal in Stockholm, Sweden on the one hand, and the Court of Appeal of England & Wales - Civil Division in the United Kingdom) on the other hand. Both requests for a preliminary ruling noted that the e-Privacy Directive contains specific provisions aiming to protect the confidentiality of electronic communications, including traffic data and location data; and that national data retention laws in Sweden, England and Wales contained a specific derogation from this principle.

Notably, the Data Retention Directive 2006/24/EC[6] required Member States to "*adopt measures to ensure that the data specified in Article 5 of this Directive [i.e. specific types of traffic data and locations data] are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned*". As a result, Swedish and English/Welsh national law had introduced a generic obligation to retain such data for the purpose of the investigation, detection and prosecution of serious crime, which arguably ran contrary to the confidentiality principles of the e-Privacy Directive. Doubts about the validity of such laws had increased significantly after the prior CJEU ruling in Digital Rights Ireland[7], in which the Court struck down the Data Retention Directive.

The requests for a preliminary ruling aimed to determine whether these national data retention obligations were compatible with the provisions of the e-Privacy Directive, given (as the Court described it in section 97 of the Judgment) that "it must be observed that that legislation provides for a general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication, and that it imposes on providers of electronic communications services an obligation to retain that data systematically and continuously, with no exceptions".

---

[6] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54); see http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32006L0024

[7] Joined Cases C-293/12 and C-594/12, Judgment of the Court (Grand Chamber), 8 April 2014.Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others. Requests for a preliminary ruling from the High Court (Ireland) and the Verfassungsgerichtshof. See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293

The context of the Tele2 case was therefore crystal clear: the Court assessed a case where *all* traffic and location data of *all* subscribers for *all* means of electronic communication was retained, *systematically and continuously, with no exceptions*, with the explicit intent to make this data accessible *for the purpose of the investigation, detection and prosecution of serious crime.* Given these boundaries, or rather the complete lack thereof, the sensitivity of traffic and location data under such a blanket and indiscriminate absolute obligation was a point that could hardly be argued.

Indeed, the Court ruled that the protections of the e-Privacy Directive, including in relation to traffic and location data, precluded any national legislation that would introduce such an obligation; and that they precluded more particularly any "*national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union*".

The issue of sensitivity of metadata – or rather, of traffic and location data, which is the terminology used by the e-Privacy Directive – was of course also addressed by the Court. It noted in section 99 of the Judgment that "***That data, taken as a whole**, is liable to **allow very precise conclusions** to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them (see, by analogy, in relation to Directive 2006/24, the Digital Rights judgment, paragraph 27). In particular, that data provides the means, as observed by the Advocate General in points 253, 254 and 257 to 259 of his Opinion, of **establishing a profile of the individuals concerned, information that is no less sensitive**, having regard to the right to privacy, **than the actual content of communications***".

The Court therefore indeed ruled the use of traffic and location data to be no less sensitive than communications contents in this specific data retention context: it made its decision in relation to the data "taken as a whole", i.e. considering the fact that the national data retention laws under examination required an extensive subset of metadata to be collected for all subscribers for all means of electronic communication, systematically and continuously, with no exceptions. Considering the breadth of this particular obligation, which fundamentally created a universal collection of all of the targeted metadata in the Member States under consideration, the sensitivity in this specific context was beyond any reasonable doubt. The Court condemned the indiscriminate and universal collection and potential use of metadata as being contrary to the e-Privacy Directive, given the sensitivity and potential use of this data "taken as a whole" for profiling purposes in the context of criminal activity.

In contrast, it did not rule that any processing or use of location data or traffic data would be sensitive by definition. The Court explicitly considered the context of the Tele2 ruling, and referenced this as the driver behind its decision. It underlined its concern that the data provided the means of "establishing a profile of the individuals concerned" as the element that lead it to conclude that this specific metadata in this specific context was no less sensitive than telecommunications content. If, *a contrario,*

the Court would have felt that traffic data and location data would inherently be sensitive, it could have simply made this statement and have rendered its judgment on this ground. The fact that it did not, supports the observation that the context of the Tele2 case was critical in the decision.

The importance of context was further emphasized by the Court in paragraph 122 of its ruling, noting that the provisions of the e-Privacy Directive in relation to security and protection of data "*require those providers to take appropriate technical and organisational measures to ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data. Given the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. In particular, the national legislation must make provision for the data to be retained within the European Union and for the irreversible destruction of the data at the end of the data retention period*".

Again, the context of data retention obligations was the only element under consideration in this section of the judgment, hence the reference to "*the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it."* The Court did not rule metadata to be sensitive by definition, and in fact emphatically endorses a risk-based approach: rather than imposing necessity and consent as fundamental requirements to safeguard confidentiality, the Court references the need for "a high level of protection and security by means of appropriate technical and organisational measures".

In summary, the Tele2 judgment must be read in its full context, which was the introduction at the national level of a general and indiscriminate retention of extensive traffic and location data of everyone relating to all means of electronic communications, without any prior checks on proportionality or effectiveness, without information to the subscribers, accessible to law enforcement for the purposes of fighting serious crime, which implies that the traffic and location data could potentially inculpate or exculpate a person. This is clearly a scenario in which the use of traffic and location data should be considered sensitive. The Court's ruling in Tele2 therefore considered this processing activity to be sensitive, given the scoping, context, and purposes of the national data retention measures. It does not logically follow that the Court therefore would find traffic and location data (or metadata in general) to be sensitive by definition.

The impact of the GDPR on metadata and its sensitivity

The Proposal for an e-Privacy Regulation must of course be seen and interpreted in the broader context of data protection reform in the EU, including particularly the adoption of the GDPR. As was already the case in the relationship between the prior Data Protection Directive 95/46/EC and the e-Privacy Directive, the GDPR does not address the context of electronic communications (or traffic data, location data or metadata) directly or explicitly. Rather, it notes in Article 95 that the GDPR "*shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC*." In other words, the e-Privacy Directive retains its position as *lex specialis* compared to the *lex generalis* of the GDPR: the GDPR establishes the general framework which will also apply to the electronic communications sector, except insofar that more specific obligations with the same objective are set out in the e-Privacy Directive. This situation will not change by an entry into force of the Proposal for an e-Privacy Regulation.

The GDPR does not address metadata, traffic data, or location data in the context of electronic communications. However, recital (49) of the GDPR does reference network and information security, noting that "*The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security […] and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned"*. Since these types of processing, which are necessary to ensure the security of networks, will also typically involve the processing of metadata in a telecommunications context, it is clear that the GDPR does implicitly acknowledge metadata, and labels it as a type of information that can be processed under the legitimate interest grounds of Article 6.1.(f) of the GDPR.

Several other observations can be made that show that the GDPR is not without an impact on the status of metadata, traffic data or location data. Firstly, it is highly relevant to note that the GDPR (like the Data Protection Directive before it) contains an explicit listing of "special categories of personal data" in Article 9. This article applies to processing of "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation". Article 10 furthermore contains explicit rules for an additional type of sensitive processing, namely for personal data relating to criminal convictions and offences.

Metadata (e.g., traffic data and location data) have not been included by the European legislator in this list. It would be incorrect to attribute this to a conservative desire to retain the pre-existing list of special categories of processing from the Data Protection Directive, as the GDPR already added genetic data and biometric data. Nor is the omission the result of an oversight; indeed, location data is

explicitly listed as an example in the definition of personal data in Article 4 (1) GDPR[8]. It would therefore have been feasible to add it (or other types of metadata) in the scope of Article 9 if the legislator considered it to be inherently sensitive. Rather, the lack of inclusion of any metadata within Article 9 of the GDPR can be seen as a recognition that this type of information is not sensitive per se – as is the case with the types of data in Articles 9 and 10 – but that its sensitivity depends on the context and thus needs to be assessed on a case-by-case scenario for each individual processing. Furthermore, the e-Privacy Regulation proposal does not make any explicit reference to Article 9 of the GDPR, stipulating that metadata should be added – per reference – as another special category of personal data to the provision.

Moreover, the GDPR also foresees other mechanisms than consent for addressing potential risks of data processing activities. The main approach of the GDPR is to require data controllers to apply a risk-based approach to their processing activities. This implies that data controllers, including providers of electronic communications services, must assess which risks are inherent to their processing activities, and take appropriate measures to mitigate these risks, document these, and comply with all other requirements of data protection law.

The risk-based approach is captured most explicitly by the accountability principle (Article 5.2 of the GDPR), which is one of the GDPR's most significant innovations compared to the Data Protection Directive. It requires that data controllers are not only responsible for complying with the principles of data protection law as formulated in Article 5.1 of the GDPR, but moreover that they must be able to demonstrate compliance with these principles. The accountability principle thereby captures a key element of the risk-based approach: the obligation to assess potential risks for individuals, comply with data protection principles, and assume responsibility for the justification of any decisions made on that basis.

Recitals (74) and (75) to the GDPR emphasise the importance of a risk-based approach, and explicitly state its application to location data:

> *(74) The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.*

[8] The definition of personal data of article 4 (1) notes that "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, **location data**, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". (emphasis added)

*(75) The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, **location or movements**, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.* (emphasis added)

The risk-based approach is visible in many aspects of the GDPR, including notably:

- In the compatibility rule of Article 6.4 of the GDPR, which specifies the conditions under which processing is permitted for purposes other than that for which the personal data have been originally collected. When a further processing for a new purpose is not based on the data subject's consent or on certain Union or Member State law, the controller must assess compatibility on the basis of, inter alia:
    - (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
    - (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
    - (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
    - (d) the possible consequences of the intended further processing for data subjects;
    - (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

  Thus, the compatibility mechanism of the GDPR requires a careful consideration of context, measures and potential impacts on the data subjects.

- The legal framework in relation to automated individual decision-making, including profiling (Article 22), which prohibits decisions based solely on automated processing which produce

legal effects concerning the data subject or similarly significantly affects him or her. The GDPR contains exceptions to this prohibition, some of which however only apply if the data controller implements "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision". Thus, automated decision making (including profiling) requires a context specific assessment of whether the effect is "significant", and which measures are "suitable" to protect the data subject, which is a clear example of a risk-based approach.

- The new obligations of privacy by design and by default (Article 25), which require data controllers to consider "the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing" in the design of their processing infrastructure and services; the obligation is thus based on consideration of potential risks and justification of the decisions made.

- The obligation to conduct data protection impact assessments (Article 35) when "a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons"; the decision to conduct a DPIA requires careful consideration and justification in its own right, and of course the DPIA itself revolves entirely around risk identification, mitigation and justification of the outcomes.

- The designation of data protection officers (Article 37), which is mandatory for public authories or bodies other than courts, or in cases where the core activities of the controller or processor "consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or of processing on a large scale of special categories of data[…]". The application of this rule thus requires an assessment of the context of the nature and characteristics of processing activities.

In each of these examples of the risk-based approach, the approach of the GDPR is unambiguously based on an obligation to make responsible, case-based and context-sensitive decisions, rather than relying on standardised responses that do not consider the specific characteristics and context of the processing activities.

It is worth repeating that the GDPR explicitly references location of the data subject as an example of personal data (and not as a special category of personal data under Article 9), but also as the potential

object of profiling activities[9]. This implies – and is indeed explicitly stated in recitals (71) and (75) of the GDPR – that a risk-based approach must be applied in which automated decision-making and profiling on the basis of location data can be permissible, subject to the implementation of appropriate safeguards.

Thus, the European legislator has made the conscious choice not to include metadata (including location data) in its list of personal data that is considered sensitive by definition. Moreover, it has referenced location data as an explicit example of a type of personal data that requires a risk-based approach, at least when location data is used for the purposes of automated decision making, including profiling.

Even if this had not been the case and metadata (including location data) should be considered as sensitive by definition, the choice of consent as a justification mechanism should not be seen as a panacea that is most capable of addressing data protection risks and challenges. The GDPR makes this clear by not establishing a hierarchy among the six legal bases which are available under article 6 of the GDPR to ensure the lawfulness of processing. This topic has also been addressed by the Article 29 Working Party on several occasions, including most explicitly in its opinion on the definition of consent[10], which noted that "There is a need to emphasise that consent is not always the primary or the most desirable means of legitimising the processing of personal data. Consent is sometimes a weak basis for justifying the processing of personal data and it loses its value when it is stretched or curtailed to make it fit to situations that it was never intended to be used in. The use of consent "in the right context" is crucial. If it is used in circumstances where it is not appropriate, because the elements that constitute valid consent are unlikely to be present, this would lead to great vulnerability and, in practice, this would weaken the position of data subjects in practice".

Consent is indeed inviable in many contexts where a (real or perceived) element of coercion may exist, such as an employment relationship, medical situations, student-teacher relationship, parent-child contexts, and in many interactions between a public administration and an individual citizen. In summary, if personal data is considered to be sensitive, requiring consent is not necessarily an appropriate or viable way to address this concern. Excessive and systemic reliance on the consent mechanism can lead to consent fatigue, leading ultimately to worse decision-making and a lack of effective data protection. A high level of data protection can be ensured via other bases for lawful processing, if these are coupled with appropriate measures to mitigate potential challenges, as required by the risk-based approach.

[9] Specifically in the definition of profiling of article 4 (4), which notes that "'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, **location or movements**". (emphasis added)

[10] Opinion 15/2011 on the definition of consent (WP187) of 13 July 2011, see http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

Some types of processing of metadata can have a very limited impact on the rights and interests data subjects, depending on the scope, nature, explicit purposes, and implemented safeguards, among other elements. By way of examples:

- Metadata can be processed by telecommunications operators to determine whether there are black spots in their coverage, or more generally where there might be a shortage of capacity (e.g. insufficient antenna coverage) that could create insufficient quality of service.

- In case of a sudden spike of customer complaints in a sudden region, an operator could also conduct a quick analysis of metadata to determine what the cause might be in order to quickly address it. Similarly, an operator could also proactively analyse metadata in order to be able to identify or even predict service interruptions or weaknesses before customers notice them. It is not always possible to identify causes, nature or scope of incidents on the basis of anonymous statistical information; sometimes only metadata of specific users can provide sufficient insights to allow a problem to be addressed.

- Operators can analyse metadata – such as call duration or mobile data use – to proactively inform the customer of more appropriate tariff plans, or to create excessive use warnings to avoid bill shock (e.g. when using mobile data outside of the European Union).

- Metadata is also useful for service providers to enable customer segmentation, not with the objective of enabling profiling in the context of automated decision-making, but rather to observe common behaviours and thereby improve service quality. The goal is not to influence a customer's behaviour or choices, but rather to ensure that service is improved in a manner that benefits customers.

- Automated emergency notification services in modern vehicles permit emergency services to be contacted in case of a car crash, including location data. The sensitivity is relatively low due to the implemented safeguards: while location data is retained in the vehicle continuously, it is only communicated to a third party in the event of a crash, and even then only to emergency services.

- In case of terrorist attacks or anticipated emergency weather (hurricanes etc.), public authorities may decide to send cautionary messages to all participants in a more or less defined area. This implies the collection and use of location data, typically on the basis of a legally defined duty upon telecommunications operators to issue the warning. The processing of the location data in this case is however not particularly sensitive to the extent that the communication is used one-time only for the purposes of sending a cautionary message, and that no monitoring takes place. Consent would not be possible or appropriate

in this case, since cautions would then not be sent to persons who were unaware of the existence of such services. Neither would anonymised data be sufficient, as the identifier allowing to send the alerts to the users currently residing in the affected area would be missing.

- In smart city contexts, it can be useful to use location data of smartphones or other communications devices to detect how crowded a particular area is at any given point in time. This can be useful for urban planning, mobility, emergency services, environmental measures, or even for identifying commercially appealing areas for a business (i.e. determining where most customers would pass by). This can be implemented in a privacy-friendly manner: while the provider of electronic communications services would collect and process personal data (metadata including location data), this data could be effectively pseudonymised, and third parties would only be given access to knowledge at the aggregate and statistical level, with appropriate safeguards against the risk of re-identification. In this manner, significant societal gains could be realised, while eliminating any significant data protection threat, without necessitating prior consent from each potentially affected data subject.

The examples are illustrative on the importance of context, scope and mitigation measures. In all cases mentioned above, the collection and use of metadata would be limited to a scale which is tailored to a specific use case (as opposed to the "general and indiscriminate retention" of the Tele2 case), respecting the principles of purpose limitation and data minimisation established by the GDPR, and no profiling would occur that would result in negative repercussions for end users (as opposed to the use for "detection and prosecution of serious crime" in the Tele2 case).

Moreover, the Proposal creates a significant risk of discrimination: recital (17) to the Proposal emphasizes that "*Location data that is generated other than in the context of providing electronic communications services should not be considered as metadata. Examples of commercial usages of electronic communications metadata by providers of electronic communications services may include the provision of heatmaps; a graphical representation of data using colors to indicate the presence of individuals. To display the traffic movements in certain directions during a certain period of time, an identifier is necessary to link the positions of individuals at certain time intervals. This identifier would be missing if anonymous data were to be used and such movement could not be displayed. Such usage of electronic communications metadata could, for example, benefit public authorities and public transport operators to define where to develop new infrastructure, based on the usage of and pressure on the existing structure*".

This recital suggests that, where location data (or other metadata) originates from electronic communications services (which would now include at least some apps), it should be automatically considered as sensitive, and any service that uses the data without strict necessity requires consent, independent of any consideration of the scope, nature, or purposes of the service, and implemented safeguards.

Inversely, location data or other metadata that originates from other sources, such as GPS devices, online maps, cloud services or apps that do not qualify as electronic communications services, would fall under the generic provisions of the GDPR. Even if the granularity of the location data or metadata would be identical, and the service using it would have an identical scope, nature, and purposes, with identical safeguards, the e-Privacy Regulation would not consider the data to be sensitive by definition. By way of example, a service such as Google Maps Timeline[11], which automatically logs an end user's location data for years, would be considered as automatically processing sensitive data if it relied on mobile phone triangulated location data, but not if it relied on GPS data from map apps, even if the latter would be more accurate and granular, and all other elements of the service (scope, context, purpose and safeguards) would be identical.

This distinction seems to have no rational justification, and appears to be based solely on a misinterpretation of the Tele2 case as requiring all metadata from electronic communications services to be considered as sensitive and requiring the prior consent of the end-user. As was discussed above, the lesson from the Tele2 case would rather appear to be that the nature, scope, context and purposes of the processing operation is decisive. The Court did not suggest that all metadata should be considered as sensitive by definition.

Furthermore, the Proposal for an e-Privacy Regulation does not provide for the application of the compatibility test in the context of electronic communications. However, it is in this context that innovative uses of metadata that are both privacy-friendly and allow for flexibility are crucial. Testing compatibility of a new purpose using the safeguards contained in GDPR, such as pseudonymisation which de-links a dataset from the individual end-user, should therefore be allowed in order to reflect the philosophy of GDPR that allows for further processing with a new purpose.

Conclusion

The application of the risk-based approach of the GDPR appears to be a more effective safeguard against data protection challenges in relation to metadata. In fact, several parts of the Proposal hint at the fact that this should be possible. As noted above, the Explanatory Memorandum to the Proposal and recital (2) both note that "metadata derived from electronic communications *may* also reveal very sensitive and personal information"; the sensitivity is recognised as a potential risk, not as a certainty. Furthermore, recital (17) to the Proposal notes, in relation to location data from other sources than electronic communications services, that "*Where a type of processing of electronic communications metadata, in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, a data protection impact assessment and, as the case may be, a consultation of the supervisory*

[11] See https://www.google.com/maps/timeline?pb

authority should take place prior to the processing, in accordance with Articles 35 and 36 of Regulation (EU) 2016/679."

This indeed seems like a reasonable position: the processing of *any* location data – irrespective of its source technology or whether it originates from an electronic communications service – can create significant data protection challenges, and therefore should be subject to a data protection impact assessment, in line with the GDPR's risk-based approach and the accountability principle. If the data protection impact assessment indicates that, after the application of mitigation measures, a high residual risk to the data subject remains, a prior consultation with the competent data protection authority should take place, as required by Article 36 of the GDPR. This approach ensures that the nature, scope, context and purposes of the processing of the location data are taken into consideration; that risks and impacts are identified; and that documented measures, safeguards and mechanisms for mitigating that risk are implemented, including a justification for which the controller can be held accountable.

Applying this same approach to the e-Privacy Regulation, rather than qualifying only metadata from communications services as automatically sensitive, would appear to be a more future-proof, rational and effective approach to managing and mitigating data protection challenges without creating undue discrimination between functionally equivalent services that create equal data protection concerns. This would imply a recognition in the e-Privacy Regulation – as has already been done in its recitals – that the processing of metadata including location data *may* be sensitive, depending on the nature, scope, context, purposes and safeguards, and therefore that a data protection impact assessment would be required before processing such data when the processing is not strictly necessary to ensure the proper functioning of electronic communications services, including the organisation of billing, payments and fraud controls, as already described in Article 6.2 (a) and (b) of the Proposal.

In other words, the current permissibility wording of Article 6.2 of the Proposal would then no longer be linked solely to the lawfulness of processing, but also to the obligation to conduct a DPIA: if the processing is necessary to ensure the proper functioning of electronic communications services as currently described in Article 6.2 (a) and (b), the processing is considered lawful and no DPIA would be required. In any other case, the Proposal could permit lawful processing based on any of the grounds described in Article 6 of the GDPR – including but not limited to consent - but always subject to the prior completion of a DPIA.

This approach would be more conducive to innovation, would avoid discriminations, would guarantee that the rules are future-proof and is more in line with the risk-based approach of the GDPR. In contrast, the current Proposal would establish a discrimination in which sensitivity is judged on the basis of the origin of the data rather than on a full and equal consideration of nature, scope, context, purposes and safeguards. It furthermore assumes that high-risk processing of metadata can only be addressed by obtaining prior consent of the end-user. This may be an optimistic assessment of the ability of end-users to assess the full impacts of their choices, and may not be feasible in all cases given the requirement that consent must be freely given, specific, informed and unambiguous in order to be valid. Therefore, a re-orientation of the approach of the e-Privacy Regulation that more strongly

emphasises a contextual appreciation of the nature, scope, context, purposes and safeguards of the processing of metadata (including location data), that eliminates or at least softens the mandatory consent requirement, and that ensures an equal approach for functionally identical services with identical data protection risks, seems preferable.

Hans Graux

29 January 2018