E-PRIVACY, TELCOS AND ONLINE PROVIDERS: ISSUES OF CONSENT

Legislative changes in Europe are highlighting apparent differences between rules applicable to telcos' and online providers' use of their customers' personal data. Can regulators create a level playing field?

By **ANN LAFRANCE**, **CATHAL FLYNN** and **MATTHEW BYFORD**

European telecoms providers are increasingly moving up the value chain to offer innovative value-added services whose appeal will rival the 'wow' factor of the myriad apps on offer from online and over-the-top providers (OTTPs). Many of these new services require the processing of subscriber traffic and location data. Such processing raises a number of issues under the existing EU data protection and e-privacy rules as well as proposed changes to the EU data protection rules.

The practical implementation of these rules is being dealt with in very different ways at the national level within Europe. The significant variations in approach may be the result of different social attitudes and cultural perspectives, as reflected in the balance set by national regulators between consumer protection and the legitimate business needs of this innovation-driven industry.

> **A central area of focus is the form of consent that is required when processing traffic and location data for marketing.**

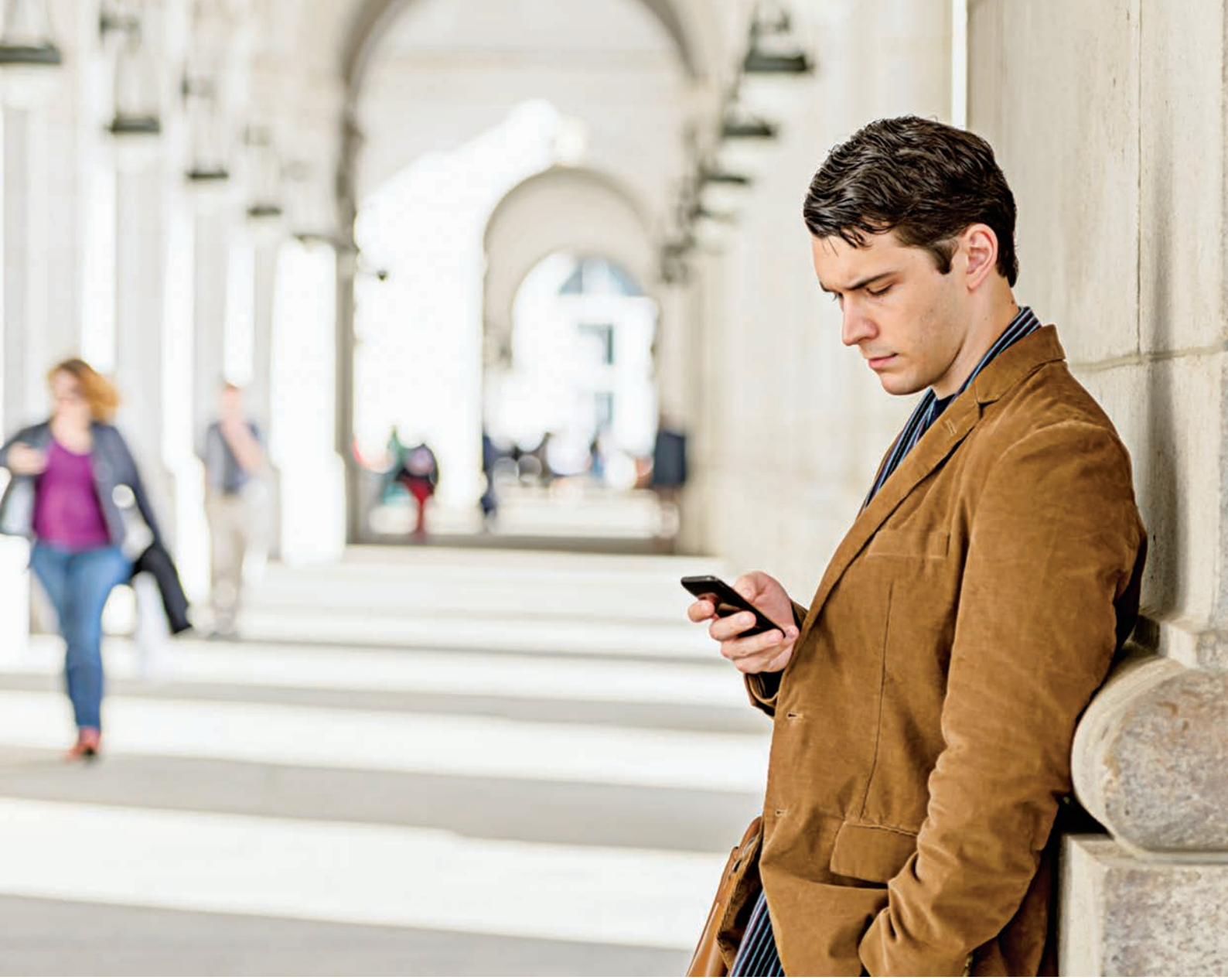
A central area of focus, which has also resulted in a diversity of approach, is the form of consent that is required when processing traffic and location data for purposes of marketing and providing value-added services.

The draft Data Protection Regulation[1] (the 'Draft Regulation'), which is currently making slow progress through the EU's co-decision legislative process, aims to introduce a higher and more harmonised level of personal data protection in Europe by replacing the Data Protection Directive 95/46/EC (the 'General Directive'). If adopted, however, the Draft Regulation will not in fact harmonise the rules set out in the E-Privacy Directive[2] that govern the processing of traffic and location data by providers of 'public communications networks' and 'publicly available electronic communications services' (telcos). Moreover, the Draft Regulation will not address the apparent divergence in the regulatory treatment of telcos under the E-Privacy Directive, as compared with the treatment of OTTPs under the General Directive.

We outline some of the key areas of divergence below.

THE E-PRIVACY DIRECTIVE

Under the E-Privacy Directive, prior consent is required for the use by telcos of traffic data (including billing data) and location data both for marketing purposes[3] and for the provision of value-added services.[4] The E-Privacy Directive does not specify whether consent must be explicit or whether it may be implied. This is an important issue for telcos. If the requirements for gaining consent are cumbersome, tech-savvy customers are likely to be put off and will look for apps that are easier to access from other sources. To the extent that OTTPs are subject to less restrictive requirements under the General Directive (or because their activities fall outside the jurisdiction of EU regulators under the current framework)[5], their services may be viewed as more user friendly and so more attractive to consumers.



GETTY IMAGES

The E-Privacy Directive also provides that "[location] data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service".[6] By contrast, non-anonymised traffic data may be processed by OTTPs for marketing purposes on the basis of any of the conditions set out under Article 7 of the General Directive, for example if the "processing is necessary for the performance of a contract to which the data subject is party" or is "necessary for the purposes of the legitimate interests" of the provider as a data controller.

Finally, it would appear that the rules set out in the E-Privacy Directive relating to the use of unsolicited emails and SMS text messages[7] allow telcos to market their own 'similar' services to their customers on an opt-out basis, provided that consent has already been given for the processing of any traffic and location data needed for that purpose. So, to qualify for opt-out treatment when sending unsolicited marketing communications to their customers, telcos must make an assessment whether some or all of the value-added services they offer are sufficiently 'similar' to the basic telecommunications services covered by their customers' subscription agreements. This raises the central question, whether customers (and regulators) continue to view telecoms services as distinct from online services and applications.

These issues ought to be considered in the context of evolving customer expectations in relation to the use of their data to provide innovative apps and other value-added services by telcos and online providers alike. A harmonised approach across Europe would be a boon to both telcos and consumers in this area.

INTERPRETATION OF PRIOR CONSENT

So far, however, national data protection regulators in Europe have taken divergent approaches in interpreting and applying the E-Privacy Directive in this area, much as they have in relation to the controversial consent requirement for cookies.

For example, in terms of the processing of location data, France, Germany, Spain and Italy all require the explicit prior consent of the user. In France, Germany and Italy, the regulatory authorities also recommend that consent be obtained each time location services are provided. By contrast, this is not required by the Spanish authority. Unlike other European regulators, implied consent for the processing of location data (and traffic data) may be acceptable in the UK, provided that a number of cumulative conditions are met[8] (eg. taking a particular step such as

logging onto a particular application or website after being informed of the consequences of taking that step through a privacy policy or notice).

Likewise, the Spanish regulator allows for implied consent for the processing of traffic data for marketing purposes and the provision of value-added services. The telco must provide the customer with notice of the types of services being provided, the types of data to be processed, and the purpose and duration of the proposed processing. If the subscriber has not responded within one month of a request to use the subscriber's traffic data, consent to the processing will be implied.

However, the subscriber must be given an easy way to subsequently object to such processing, free of charge.

It is also interesting to note that in France, somewhat uniquely, OTTPs may be subject to many of the same rules as telcos under the relevant legislation on the use of traffic data and location data, owing to the fact that the rules expressly cover any person whose main activity or ancillary business is to supply online communications by way of access to a network.[9]

THE STANDARD OF CONSENT

Under the General Directive, consent is just one of the potential bases for the processing of personal data.[10] The Article 29 Working Party has opined that where consent is the basis for processing, there is a basic consensus that, in order to be valid, consent should be "freely given, specific, informed and unambiguous".[11]

The distinguishing feature of consent under the General Directive in comparison to the requirements under the E-Privacy Directive is that the latter specifically requires 'prior' consent. However, the E-Privacy Directive does not stipulate whether prior consent must be *explicit* (eg. provided by checking a box) or *implied* (eg. ordering a service that obviously requires the processing of the personal data in question). Where consent is relied on as a legal basis, and depending on the applicable laws and local practice, prior consent, or deemed consent subject to withdrawal, may be acceptable.

The Draft Regulation aims to set a EU-wide standard for consent and includes a requirement that such consent must be 'explicit'.[12] Indeed, the working party recently issued an advice paper[13] underlining the importance of explicit consent as a legal basis for data processing for the purposes of profiling[14] within the context of the Draft Regulation. Interestingly, the processing of traffic data for marketing purposes under the E-Privacy Directive would appear to be covered by the actual definition of profiling. If this is true, it may mean that OTTPs covered by the future Draft Regulation will be in a similar but potentially less flexible position as telcos currently are under the E-Privacy Directive in respect of the processing of traffic or location data.

However, the imposition of an explicit consent requirement is seen by many as an inflexible and impractical one-size-fits-all approach that may well work to the detriment of industry. The German government has recently said the Draft Regulation should be revised to make clear that consent may be obtained through a variety of tools and need not always be explicit.[15] Several other member states have expressed similar concerns about the proposed change to the consent requirement.

CHALLENGES AHEAD

Where does this leave the industry? It is perhaps good news for lawyers, but not necessarily for consumers, that the rules relating to consent in this fast moving area are so complex. The proposed Draft Regulation and the debates surrounding it are a clear indication that a flexible but consistent approach in this area may not be on the cards anytime soon.

> **A converged and more user-friendly approach to data protection regulation would make life much easier for consumers.**

In an industry where speed, brevity and convenience are features that are highly prized by consumers, the applicable data protection and e-privacy rules should be interpreted by regulators in a proportionate way. This 'proportionality principle' is an important feature of the EU data protection and e-privacy framework, but it is one that appears to be often overlooked by regulators.

In a world where telcos and OTTPs are competing to provide the same types of innovative apps and other value-added offerings to consumers, a converged and more user-friendly approach to data protection regulation would make life much easier for the supposed beneficiaries of regulation – consumers – and establish a level playing field for competition among telcos and OTTPs in this rapidly developing area.

***ANN LAFRANCE**, **CATHAL FLYNN** and **MATTHEW BYFORD** are at Squire Sanders (UK) LLP in London.*

REFERENCES

1 On the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) 2012/0011 (COD). **2** EU Directive on Privacy and Electronic Communications 2002/58/EC. **3** Although oddly the E-Privacy Directive does not envisage the possibility of using location data for marketing purposes. **4** Articles 6 and 9 of the E-Privacy Directive. **5** This jurisdictional issue may be resolved by Article 3(2) of the Draft Regulation, which imposes all of the obligations of the Draft Regulation on data controllers (including OTTPs) outside the EU which offer goods or services to data subjects in the EU or even merely track the online behaviour of data subjects within the EU. **6** Article 9(1) of the E-Privacy Directive. **7** Article 13 of the E-Privacy Directive. **8** By analogy with the Information Commissioner's guidance on the use of cookies. **9** See Article L34-1 of the Code of Postal Services and Electronic Communications. **10** Article 7 of the General Directive. **11** Opinion 15/2011 on the definition of consent, adopted on 13 July 2011. **12** Article 4(8) of the Draft Regulation. **13** Advice Paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, adopted on 13 May 2013. **14** Defined in the Advice Paper as "any form of automated processing of personal data, intended to analyse or predict the personality or certain personal aspects relating to a natural person, in particular the analysis and prediction of the person's health, economic situation, performance at work, personal preferences or interests, reliability or behaviour, location or movement." **15** Rainer Stentzel, a data protection official at Germany's Home Affairs Ministry, speaking at 'Consumer policy in the digital world: what role should the EU play?' Brussels, May 15, 2013.