HERBERT SMITH FREEHILLS

E-PRIVACY REFRESH FOR TODAY'S ELECTRONIC COMMUNICATIONS SERVICES: GOOD INTENTIONS BUT DOES THE PROPOSED REGULATION STRIKE THE RIGHT BALANCE?

28 March 2017 | Europe
Legal Briefings

It is fair to say the European data protection and privacy framework is currently undergoing a full overhaul.

The European General Data Protection Regulation ("**GDPR**") and the current proposed reforms to the e-privacy regime have been firmly in the spotlight - with both initiatives supporting the European Commission's Digital Single Market Strategy for "reinforcing trust and security in digital services and in the handling of personal data".

The GDPR entered into force on 25 May 2016, with a two year implementation period before it applies from 25 May 2018. However, the scrutiny and debate is set to continue, with the Commission's long awaited first draft of the ePrivacy Regulation (the "**Draft Regulatio**n") published earlier this year. The Draft Regulation is expected to replace the existing Privacy and Electronic Communications Directive (the "**ePrivacy Directive**") – focusing on the processing of personal data and protection of privacy in **electronic communications** (compared with the more general application of the GDPR to the processing of personal data). Among other areas, it covers direct marketing, cookies and other forms of online tracking.

The proposal principally seeks to:

- bring e-privacy law up to date with the "evolution of technological and market reality", taking a technology neutral approach and extending its application beyond just traditional communications services, to new entrants such as internet-based services enabling interpersonal communications (e.g. voice over internet protocol ("**VoIP**"), messaging services and web-based email); and

- align the law with the incoming GDPR - aiming to complement it to the extent that electronic communications data qualifies as personal data.

In this article we take a look at some of the main features of the Draft Regulation at this early stage of the European legislative process and the potential impact on organisations in the technology, media and telecoms sectors – in particular whether the draft proposal addresses the balance between improving rights to privacy and being sufficiently practical and consumer and business friendly for today's digital age.

With a far broader scope than its predecessor, enhanced privacy measures, an increased risk exposure for non-compliance due to far higher monetary sanctions for certain breaches and an ambitious timetable to apply from 25 May 2018 to align with the GDPR, one thing is for sure - compliance, marketing and advertising teams across an equally broad spectrum of international service providers will be closely following the evolving e-privacy reform alongside their existing compliance programmes.

THE STORY SO FAR

A reform of the e-privacy and electronic communications regime has been long overdue. First established back in 2002 under the ePrivacy Directive and implemented in the UK through the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("**PECR**"), it was last reviewed in 2009 to provide clearer rules on customer's rights to privacy and new requirements regarding personal data breaches and cookies. As part of its Digital Single Market Strategy, the Commission launched a public consultation on the ePrivacy Directive in April 2016 (the "2016 Consultation"), attracting responses from 421 stakeholders from a cross-section of citizens, consumer and civil society associations, industry and public authorities. Whilst the results of the consultation highlighted that individuals consistently requested that their communications remain confidential with strong protection measures in place, there were more mixed views from industry and public authorities. In particular, industry responses requested rules that would not "stifle new opportunities related to use of data". The results of the 2016 Consultation fed into the Commission's review of the existing e-privacy regime and preparation of the Draft Regulation.

MAIN FEATURES OF THE DRAFT REGULATION

The proposal builds on the existing e-privacy framework, with some of the rules remaining broadly the same (e.g. in respect of direct marketing consents). Much of the proposal is in line with the Commission's approach to the GDPR, so it comes as no surprise. Some of the main features of the Draft Regulation are set out below.

1. Scope: There are a number of proposed changes that mean a whole plethora of organisations and services which were not otherwise caught by the ePrivacy Directive, will now need to comply with the regime. Organisations or services previously subject to the regime will also need to revisit their own compliance procedures in light of other broader applications of the rules:

- **Extra-territoriality**: As with the GDPR, the Draft Regulation will have extra-territorial effect – i.e. broadly speaking it will extend to apply to organisations located outside of the EU that process electronic communications data in connection with providing electronic communication services to end-users in the EU (or use of such services).

- **New players**: Provisions around confidentiality, processing of electronic communications data, storage and erasure of data now apply both to traditional voice, text and e-mail services as well as functionally equivalent online services, such as over-the-top providers of VoIP, messaging services and web-based e-mail services (e.g. Skype, WhatsApp, Viber, Facebook Messenger, Gmail). Given that end-users perceive these new entrants as comparable to their more traditional competitors, the Draft Regulation attempts to remove the lighter touch regulation for new entrants and put all such services on a level playing field - complying with one set of rules. We can expect divided comments from industry stakeholders on this scope change - based on industry responses to the 2016 Consultation, 42% did not want the scope to be broadened in this way, against 36% that did.

- **Electronic communications services**: In an effort to future-proof the regime, the Draft Regulation achieves this breadth, in part, by using the wide definition of "electronic communications services" from the current draft European Electronic Communications Code (which itself forms part of the Commission's separate ambitious reform of the EU telecoms regulatory framework to meet the EU's growing connectivity needs). The majority of services with a communications element are likely to be caught by the definition, even if they are just an "ancillary" feature to another service – for example, a review site, e-commerce site or dating application.

- **Machine-to-machine**: Some rules will also now apply to machine-to-machine communications (i.e. so-called "internet of things" technology). The recitals acknowledge that machine-to-machine communications involve the conveyance of signals over a network and usually constitute an electronic communications services.

- **Marketing**: As is the case now, a number of the rules (e.g. those around direct marketing and cookies and similar technologies) also apply to marketers and websites,

whether or not they are regarded as "electronic communications services".

- **Software providers**: The Draft Regulation is likely to have a knock-on effect on software providers as well – as referred to in the "Cookies" section below.

2. Processing content and metadata:The proposal includes new rules relating to the confidentiality and processing of electronic communications data, as well as the storage and erasure of that data.

- It distinguishes between "communications metadata" which is generated from electronic communications (i.e. the timing, location and length of a call or a user browsing history – referred to as "traffic and location data" under the existing framework) and "communications content" (i.e. the content of the communication itself) - with more stringent rules applying to the latter. An electronic communications service provider is required to erase or anonymise both sets of electronic communications data if user consent is not given to its retention (unless certain exceptions apply e.g. use for billing purposes).

- The Commission believes the rules also provide greater business opportunities for traditional telecoms providers, allowing them to develop more bespoke and innovative services. Under the ePrivacy Directive, such providers are only currently permitted to process "traffic and location data" for value added services (such as suggesting similar products or services based on an end-user's usage). However, the new proposed rules allow processing of electronic communications data for other specified purposes as well – subject to end-user consent and certain privacy protections. The recitals to the proposal include practical examples such as the provision of heatmaps to geographically indicate the presence of individuals and help public authorities and transport companies when developing new infrastructure projects. Of course the way in which that consent is obtained in practice will need to be carefully addressed to ensure that these new opportunities are not inadvertently abused by electronic communications service providers and do not jeopardise the protection of rights to privacy.

3. Cookies: Cookies and other tracking technologies (e.g. fingerprinting and spyware) have been incredibly useful tools for service providers. Designed to recognise a user's device and track the user's navigation of, for example, a website, commercial uses have been wide-ranging, such as allowing websites to improve their services through data analytics and tailoring the user experience - without requiring the user to login on each visit to that website. The rules relating to those technologies have, however, been the cause of much criticism since their inception in 2009 - with many consumers and businesses alike claiming that the related consent requirements are excessive and to the detriment of the user experience. A Commission representative has even admitted "we have tried to overcome banner-fatigue" with the Draft Regulation. It is therefore unsurprising that the proposal seeks to simplify the existing provisions relating to cookies and, at least theoretically, make them more user-friendly.

- Consent is still required for websites to use cookies or other tracking technologies to access information stored on devices or track user behaviours online (unless certain limited conditions apply). However, consent is no longer required in situations that involve "no, or only very limited, intrusion of privacy" (an approach already adopted by the UK data protection regulator, the Information Commissioner's Office (the "**ICO**"), and more lenient than some of its European counterparts). Consent is therefore not required to use those technologies, for example, if necessary for: (i) web audience measuring for first party analytics (e.g. measuring visitors to a particular site - although websites using third party analytics, such as Google Analytics, will still need consent); (ii) providing an information society service requested by the end-user (e.g. recalling a shopping cart history); or (iii) the sole purpose of carrying out the transmission of an electronic communication.

- Whilst the Draft Regulation cross-refers to the definition of consent under the GDPR, the proposal allows consent to be expressed using "appropriate technical settings of a software application" – i.e. through browser settings. The software placed on the market permitting electronic communications is required to offer privacy settings that enable the blocking of third party cookies and, on installation, inform the end-user of a full range of privacy setting options (ranging from high and low privacy options, as well as information about the related risks of allowing third party cookies on a device). The end-user is then required to consent to a particular setting before being able to continue with the installation. By doing so, the Commission seeks to mirror the "privacy by design" principles set out in the GDPR. The recitals to the proposal also reiterate that any method used for providing information and obtaining consent should be as user-friendly as possible.

- The Commission believes that this centralised consent process will remove the need for a significant proportion of businesses to use clunky cookie banners and pop-up notices, leading to potentially significant cost savings and simplifications. However it may also make it more difficult for online third party targeted advertisers to obtain consent (e.g. if a large proportion of end-users opt for "reject third party cookies" settings) and

commentators have suggested this approach has the potential to deprive content providers of important advertising revenues and disrupt many existing digital advertising business models. Whilst it does not preclude website operators from making individual requests for such consent from end-users instead, this may mean that in reality, targeted advertisers / websites continue to use the very same banners and pop-up notices the Commission sought to reduce.

- No doubt software providers will need to configure browsers or similar software to take account of this anticipated functionality as well. The Draft Regulation further requires software that has already been installed when the regulation is due to come into effect to comply with the privacy setting requirements by no later than 25 August 2018.

4. Direct marketing: Direct marketing can be an effective tool to market and advertise to identifiable end-users. The regime (and consent requirements) remains materially the same as under the ePrivacy Directive with some additional requirements:

- User consent is still required to send unsolicited direct marketing communications to end-users using electronic communications services. The breadth of the "electronic communications services" definition and that of "direct marketing communications" mean that the circumstances in which this applies remain wide - regardless of the communication method used (with automated calling and communication systems, instant messaging applications, emails, SMS and MMS and Bluetooth called out by way of example).

- Given that the definition of "consent" aligns with that of the GDPR, organisations ought to adhere to the GDPR standards when obtaining such consent. The most recent ICO guidance on the GDPR suggests that consent should involve a positive indication of the wishes of the data subject (e.g. via an unticked opt-in box) with separate consents for different processing activities, purposes and methods - at the very least, this will require organisations to invite end-users to give consent by separately opting-in to each type of electronic marketing e.g. emails, texts, automated calls etc. (as is currently the ICO's best practice approach to direct marketing consent), but there is also the possibility that consents will need to be unbundled even further.

- The existing ePrivacy Directive "soft opt-in" remains for marketing via email – i.e. consent will not be required where a marketer has obtained an end-user's email contact details from the "sale of a product or service" and subsequently wishes to offer its own similar products or services – this is provided the right to opt out is given at the time of collection and each time a subsequent message is sent. Users should still be able to withdraw their consent at any time, free of charge and in an easy manner.

- As well as individuals, the new rules also expressly protect corporate entities from unsolicited communications – leaving it to Member States to legislate to ensure the

legitimate interests of those entities are sufficiently protected.

- The Draft Regulation also includes slightly new transparency requirements for direct marketing calls, including using a particular pre-fix to identify a marketing call or the existing option of presenting the end-user with the number from which it is calling (i.e. prohibiting methods to block caller ID which is in line with the current ICO guidance).

- Member States are left to decide whether live direct marketing calls require "opt-out" consent (i.e. soft opt-in) as is currently the case in the UK – a move that may well be debated further following divided stakeholder responses to the 2016 Consultation on this point (close to 90% of citizens, civil society and public authorities favouring an opt-in regime against 73% of industry favouring an opt-out approach).

5. Sanctions and enforcement: The existing enforcement action by the ICO for breach of PECR includes criminal prosecution, non-criminal enforcement and audit - these powers are not mutually exclusive. The ICO can also impose a monetary penalty notice of up to £500,000 which pales in significance to the regime envisaged under the Draft Regulation - a tiered approach to fines aligned with that of the GDPR.

- Breach of certain provisions (including in relation to notice and consent, unsolicited communications and privacy settings of software enabling electronic communications) could lead to fines of up to Euro 10,000,000 or 2 per cent of total worldwide annual turnover, whichever is the higher.

- Even larger fines of up to Euro 20,000,000 or 4 per cent of total worldwide annual turnover (whichever is the higher) are introduced for breach of other provisions (including in relation to confidentiality of communications, processing of electronic communications data and limitations on data erasure periods).

- End-users of electronic communications services will have certain remedies against data controllers and data processors as well as the right to receive compensation if they have "suffered material or non-material damage" resulting from breach of the Draft Regulation.

- To ensure full consistency with the GDPR, the proposal anticipates enforcement by the same national data protection authorities, as well as the same cooperation and consistency procedures applying for enforcement across the EU.

A WORD ON BREXIT

As with the GDPR, the reform takes the form of a regulation (rather than a directive) in an effort to harmonise the new electronic communications privacy framework - it will be directly applicable in all EU Member States. This also seeks to address other policy issues with the existing framework around fragmentation at the national level and inconsistent enforcement. It could also simplify and lower the costs of compliance for international businesses with a cross-border EU footprint – complying with one set of e-privacy rules.

However, if the timeframe for the new e-privacy regulation coming into force remains as currently expected (i.e. before the UK leaves the EU), the existing PECR are likely to be repealed, at least in part, in anticipation of the new regime. This means that a UK exit from the EU post May 2018 will leave the UK having to take steps to adopt new e-privacy legislation when the new e-privacy regulation falls away on exit.

That aside, the extra-territorial scope of the Draft Regulation and the commercial practicality of compliance across an EU footprint, mean that in reality organisations are likely to have to comply with the new e-privacy regulation regardless of whether located in the EU or not and the UK is unlikely to want to stray far from the principles set out in any such legislation. Brexit may, however, impact the ICO's enforcement role but this will depend in part on the UK's future relationship with the EU.

THE BALANCING ACT

Given the breadth of stakeholders with an interest in the e-privacy reform and the divided opinion flowing from the 2016 Consultation, the Commission clearly had a difficult task juggling, and seeking to satisfy, those interests, alongside its targeted initiative under the Digital Single Market Strategy.

As to whether the Draft Regulation strikes that balance; there are certainly a number of good intentions – for example: traditional telecoms providers in particular will welcome the expansion of opportunities to use electronic communications data in developing new products and services; e-commerce businesses and consumers alike will, no doubt, support the simplified, more streamlined approach to cookies and other tracking technologies; as well as supporting the consistency of an aligned approach to the new GDPR regime.

However, it remains to be seen whether those good intentions will materialise in practice or disadvantage other areas of the ecosystem as well – as highlighted by, for example, the potentially detrimental effect on online third party target advertisers of the proposed centralised consent regime based on browser settings (see "Cookies" above) - as well as the ability of that consent regime to neutralise the effect of improving the end-user journey in those circumstances.

As with most things, the devil is likely to be in the detail – for example whether the Draft Regulation truly aligns with the GDPR or whether it leads to confusion and sets up a "double regulatory regime" instead, as recently suggested by representatives of the telecommunications industry. From a UK perspective, it is also not yet clear how the Draft Regulation will interact with existing national initiatives on e-privacy, for example, the ePrivacy Direct Marketing Code forming part of the draft Digital Economy Bill and due to receive Royal Assent in spring 2017. In addition, some civil rights organisations have already commented that the proposal still requires more significant improvement to truly promote trust, privacy and innovation.

The Article 29 Working Party (made up of representatives from the data protection authority of each EU Member State, the European Data Protection Supervisor (the "**EDPS**") and the Commission) is expected to provide its opinion on the proposal during the course of 2017, with the EDPS listing the review as one of its strategic priorities for the year. The opinion will be reviewed with much interest across the board.

Only time will tell whether the Commission has also adequately been able to future-proof this new e-privacy regime, particularly as the reform of the telecoms regulatory framework (and related concepts under that regime) unfold in parallel.

WHAT SHOULD ORGANISATIONS BE DOING NOW?

At this early stage, the Draft Regulation is just that, a draft proposal. However, it is worth re-iterating that the proposal provides for the regulation to apply from 25 May 2018, along with the GDPR. Given the many European legislative obstacles in place before it is approved (by the European Parliament and the Council of the EU) and the likely potential for criticism from a full spectrum of European institutions and stakeholders - not least given the far wider remit of the new rules - arguably a considered debate may be difficult in the challenging time frame proposed.

It is therefore too early to fully assess the impact of the proposal on organisations at this stage. However, given the proposed timing and high monetary sanctions deterring non-compliance, compliance teams ought to consider whether the broader scope of the proposed new privacy rules could apply to their business and closely follow the evolving e-privacy reform alongside their existing compliance programmes - particularly for organisations or electronic communications services that were not previously caught by the ePrivacy Directive (such as over-the-top service providers). Affected organisations should also build e-privacy concerns into any GDPR readiness programme they are currently undertaking, given the interplay between the two pieces of legislation.

Whatever the trajectory of the current Draft Regulation, if the timing remains as currently anticipated, the run up to May 2018 is set to be a very busy period for many organisations, with preparations for the full trio of e-privacy, data protection and potentially cyber security regime compliance - the Network and Information Security Directive is also due to apply to certain "operators of essential services" and certain "digital service providers" from May 2018.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

AARON WHITE
PARTNER, LONDON

+44 20 7466 2188
aaron.white@hsf.com

HAYLEY BRADY
PARTNER, HEAD OF MEDIA AND DIGITAL, UK, LONDON
+44 20 7466 2079
Hayley.Brady@hsf.com

CLAIRE WISEMAN
PROFESSIONAL SUPPORT LAWYER, LONDON
+44 20 7466 2267
Claire.Wiseman@hsf.com

LEGAL NOTICE