CENTER FOR DEMOCRACY & TECHNOLOGY

Analysis of the proposed ePrivacy Regulation

May 2017

Introduction

The Center for Democracy and Technology (CDT) welcomes the European Commission's proposal for a Regulation on Privacy and Electronic Communications (COM(2017)10) of 10 January 2017 (the ePR) to replace the 2002 ePRivacy Directive (ePD).[1] The ePD "particularises and complements" the 1995 Data Protection Directive, and with the replacement of that Directive by the General Data Protection Regulation (GDPR)[2] in April 2016 arises the need to review and update the ePD.

In general, we support the Commission's initiative to update and rewrite the ePD. We agree with many of the motivations and intentions behind it. However, we offer a number of observations about the approach taken by the Commission that we suggest should be taken into account as the proposal is considered by the European Parliament and the Council of Ministers.

We agree with the need to update the ePD in light of the adoption of the GDPR and developments in communications technology and business models. In particular, we agree with the necessity to provide clear safeguards for protecting confidentiality of communications. At the same time, we are concerned that the extremely broad scope of the draft ePR could create a number of unintended consequences for technologies that do not involve interpersonal communications, as well as conflicts with the GDPR. Further, the ePR provisions on online tracking are well-intentioned, but very detailed and prescriptive, and focus overwhelmingly on traditional website use and tracking via browser-based cookies;[3] it is not clear that this approach will help enhance user control and transparency.[4] The ePR's exclusive reliance on consent in this context may be too restrictive given its broad coverage and may inhibit uses of data that have broad societal benefits. On this point, it is inconsistent with the GDPR, which not only reaffirms multiple legal bases for processing information but also acknowledges the privacy-protecting value of pseudonymisation in addition to anonymisation. The result is that the ePR may make some data uses completely unfeasible. Further, we fear that the draft ePR expands the ability of public sector agencies (not only law enforcement) to access a much wider set of electronic communications data than was the case under the ePD, and finally we argue that the ePR should recognize the ability of users and providers to use strong encryption technology to protect communications confidentiality.

---

[1] Proposal for ePrivacy Regulation, European Commission, *available at* https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation [hereinafter ePR].

[2] Regulation No. 2016/679 of the European Parliament and of the Council of April 27, 2016, on the Protection of Individuals 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) [hereinafter GDPR].

[3] For instance, Recital 22 notes the "ubiquitous use of tracking cookies and *other tracking technologies*" (emphasis added) but comments only that end users must provide consent for "such tracking cookies"; and Recitals 23 and 24 are devoted exclusively to addressing cookie controls.

[4] Ultimately, Article 10 of the ePR addresses privacy controls through the lens of browser-based cookie controls.

The Commission is right to put in place safeguards to protect electronic communications confidentiality, regardless of underlying technology.

In our contribution to the European Commission's consultation on the (then potential) ePRivacy instrument in 2016, we argued that a new instrument should primarily target the areas not covered by the General Data Protection Regulation (GDPR). In particular, it should provide for the protection of the right to confidentiality of communications.[5] This Article is not covered by GDPR, which implements Article 8 of the Charter of Fundamental Rights. It is essential that people can exchange views without fear of third parties monitoring, intercepting or interfering with private communications. It is also essential for various forms of professional privilege such as that required by attorneys with respect to their clients, physicians to their patients, and journalists to their sources.[6]

Communications confidentiality is also fundamentally important for companies (legal persons) of all descriptions that need to transmit sensitive and confidential data using electronic communications networks. Further, we agree with the European Commission that maintaining strictly separate confidentiality and data protection regimes for electronic communications networks as defined in the ePD is not sustainable given the widespread adoption of many new communications services that currently fall out of the scope of the ePD. It is sensible to adopt more technologically neutral rules. There should be legal protection against unwarranted intrusion into private communications by third parties, regardless of the underlying technology.

The ePR's broad scope creates complexity and possibly unintended consequences for scenarios that do not involve interpersonal communications or personal data.

We have argued that, wherever possible, the ePrivacy instrument should defer to provisions in the GDPR to avoid overlap and conflicting obligations. The Commission's draft ePR takes a more expansive approach with a broader scope of application. This is the case both with regard to the categories of data considered to fall within the scope of the ePR, and the definition of electronic communications services providers covered. This entails a real possibility that over time, the ePR may become the primary legal instrument for data protection rather than the GDPR. Such broad coverage may lead to unintended consequences.

For instance, the ePR's definitions of "electronic communications content" and "electronic communications metadata" include more extensive categories of information than the "personal data" that is covered by the GDPR.[7] The GDPR is also concerned exclusively with the rights of natural persons

[5] Charter of Fundamental Rights of the European Union art. 7, 2010 O.J. C 83/02 [hereinafter CFR].
[6] *See, e.g.*, Case C-155/79, AM&S Eur. Ltd. v. Comm'n, 1982 E.C.R. 1575 (1982); Eur. Court of Human Rights, Protection of Journalistic Sources, April 2016, www.echr.coe.int/Documents/FS_Journalistic_sources_ENG.pdf; European Council of Medical Orders, Principles of European Medical Ethics (adopted 6 January 1987).
[7] Compare GDPR Art. 4(1), which explains that personal data is limited to "any information relating to an identified or identifiable natural person ("data subject")", with ePR Art. 4.3, which explains that electronic communications data includes both content and any data processed 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

while the ePR is focused on the "terminal equipment" of end users, both natural and legal persons, and not specific data subjects.

The potential difficulty with the Commission's approach is that, in time, the ePR may become the comprehensive rule rather than the exception. As more and more technologies are interconnected and communicate with each other and end users, it becomes difficult to envision a company or service that does not transmit or process data in electronic form using communications networks.[8] Logically, all such data would then be covered by the ePR. This would seem to be at odds with the intention behind the GDPR and could open up many possibilities of conflicts and inconsistencies with the GDPR. As the digital and physical worlds combine, it is unclear where the GDPR would actually take precedence.

The Commission's proposal has been expanded to include services offered by "over-the-top" providers, covering the confidentiality of both "current and future means of communication, including calls, internet access, instant messaging applications, email, internet phone calls and personal messaging provided through social media".[9]

It is sensible to attempt to future-proof the ePR, and the existence of a separate set of rules for communications services outside of the explicit scope of the ePD was one reason put forward by industry for largely repealing ePrivacy rules altogether.[10] Rules governing the confidentiality of communication remain necessary, but we note that language in the draft ePR captures a vast array of different business models and services. For instance, Article 4.2 explains that the ePR would apply even to apps and services which enable communications "merely as a minor ancillary feature that is intrinsically linked to another service". This brings into the scope of the ePR any website that has a chat function or online game that allows players to communicate, even if that functionality is not under the website's control.

Perhaps more challenging is the extension of the ePR's requirements to sensor data generated by the Internet of Things (IoT).[11] The proposed ePR makes clear that it applies to the collection of any information "emitted from/by terminal equipment" that may enable a device to connect online.[12] It is clear that the ePR is intended to cover machine-to-machine communications and to apply to data transmissions across traditional mobile devices but, increasingly, also cars, homes, wearables, and digestibles. However, many connectivity applications and device communications such as the industrial IoT environment do not entail the processing of personal data or pose privacy risks. The ePR's inclusion

---

the location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication".

[8] As the European Commission's Joint Research Centre acknowledges, information technologies ensure that EU citizens leave "an increasing trail of personal and individual data." European Commission, Citizens' Digital Footpring, https://ec.europa.eu/jrc/en/research-topic/citizens-digital-footprint (last accessed May 1, 2017).

[9] ePR Recital 11.

[10] ETNO, Study on the Revision of the ePrivacy Directive, August 2016, https://etno.eu/datas/publications/studies/DPTS_Study_DLA_04082016_ePrivacy_Final.pdf.

[11] ePR Recital 12.

[12] ePR Recital 20.

of such technologies, however, results in the ePR applying in a broad range of contexts that have little or nothing to do with interpersonal communications and do not involve personal data. It is difficult to predict how provisions of the ePR will impact the IoT environment, but the broader the ePR's scope, the more general its provisions will need to be in order to ensure the regulation is technology-neutral and future-proof and takes into account the vastly different contexts that are covered. The practical result of this broad application of the ePR is that it may actually provide less precision and clarity and hence less practical protection for the communications content that is the main focus of the regulation.

Online tracking is and will remain a serious privacy concern. However, the draft ePR seems too prescriptive and unduly focused on user interaction with traditional websites, and may not be future-proof.

One of the most important priorities addressed by the ePR is online tracking. Tracking of people while they use communications services, websites, mobile applications, and a rapidly evolving and changing range of digital services and products, is a key privacy concern. Today, a significant portion of digital services and products are provided without fees charged to users, and funded by advertising. Under this business model, the use of websites and digital applications are tracked by first and third parties that measure usage and aim to deliver advertising that is targeted or otherwise tailored to users. Addressing the privacy implications of this model provided the impetus for the revision of the ePD in 2009 and subsequent introduction of the controversial cookie provisions.[13] It is clear that these rules are too specific and too inflexible to be fit for purpose, and should be updated.

The objective must be a digital environment in which users can trust the digital and communications services they use. It is essential that users understand how data about them is collected, used and shared when they engage with digital products and services. They must be able to make informed decisions about what services they wish to engage with and under what terms. The rules should enable transparency and control for end users and at the same time enable provision of a broad range of innovative communications and other digital services and products. It is not clear, however, that the ePR approach will succeed in achieving this result.

(1) Tracking Can Be Investigated and More Thoroughly Addressed via the European Data Protection Board

In our response to the Commission's ePrivacy consultation we did not specify whether rules for online tracking should be set out in the forthcoming ePrivacy instrument or regulated under the applicable GDPR provisions. The view taken on this question is separate from one's opinion on what those rules

[13] Council Directive 2000/136, rec. 66, 2009 O.J. (L337)11, 20 (EC). Recital 66 explains that it of "paramount importance that users be provided with clear and comprehensive information" about the use of cookies. However, the opt-in provisions of the ePD proved difficult to enforce, and by early 2013, citing the fact that "many more people are of cookies," the UK ICO moved to an implied consent framework for its own website: United Kingdom Information Commissioner's Office, Changes to Cookies on Our Website, 31 January 2013, https://ico.org.uk/about-the-ico/news-and-events/current-topics/changes-to-cookies-on-our-website/.

should be in substance. More flexibility is needed in the underlying legal text; this can be accomplished by further empowering data protection authorities (DPAs) to make decisions as and when market and technology developments require it.[14]

Specifically, the ePR could provide for a larger role for the European Data Protection Board (EDPB) established under the GDPR.[15] Under the GDPR, member states DPAs, via the EDPB, may issue guidance and opinions interpreting the Regulation on issues and questions as they arise with changing technologies and business models.[16] Tracking will remain a priority for DPAs for the foreseeable future. They will need to monitor market developments, business models, technologies, and user behaviours. A DPA-centric approach may allow flexibility in interpretation and can reflect the ongoing change in technology.[17]

(2) The Draft ePR Does Not Adequately Consider Context, Especially With Respect to Audience Measurement Technologies

The ePR also does not take into consideration the various contexts in which communications data may be collected and used. The privacy-invasiveness of a given activity can be highly context dependent. For instance, a browser-based Battery Status API that allowed websites to detect the status of an end user's battery level in order to save critical information would appear to be a generally beneficial technology, but the API was most frequently used by advertisers, who used it to track users across websites and forced the API's removal.[18] Similarly, how privacy-sensitive the placement of a cookie is depends on what function the cookie performs, and how the information it gathers is shared. It does not depend on whether it is placed by the website operator the user engages with, or by a third party. For example, a cookie may contain the value "lang=fr" to stipulate that the user prefers websites to be presented to them in French. The cookie is helpful in that the user does not have to manually select language each time they visit a page on the same website, but it is not useful for tracking as it does not identify a person or a device.

However, this is not reflected in the draft text, and may have especially negative consequences for basic user measurement and analysis. Article 10 obliges software permitting electronic communications to offer the option of preventing third-party cookies. The article, read in conjunction with Article 8.1(d), is a presumption against the use of third-party cookies, and it prohibits web

[14] An example is found in the U.S. Federal Trade Commission's January 2017 'Report on Cross-Device Tracking' available at: https://www.ftc.gov/news-events/press-releases/2017/01/ftc-releases-new-report-cross-device-tracking.
[15] The European Data Protection Supervisor, in an Opinion on the ePR, recommended that further guidance from the EDPB might be explicitly referenced in the ePR. *See, e.g.*, EDPS Opinion 6/2017, 24 April 2017, https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf.
[16] GDPR Art. 68.
[17] *See* F. Roesner et al., 'ShareMeNot - Balancing Privacy And Functionality Of Third-Party Social Widgets', https://www.usenix.org/system/files/login/articles/roesner.pdf.
[18] Battery Status API being Removed from Firefox due to Privacy Concerns, 2 November 2016, https://www.bleepingcomputer.com/news/software/battery-status-api-being-removed-from-firefox-due-to-privacy-concerns/.

audience measuring unless carried out by the service provider itself.

Basic measurement, analysis and reporting of how end users interact with websites and online services is essential for website operators to understand and evaluate how their services are operating, and both the Article 29 Working Party[19] and the SMART 2013/0017 study[20] acknowledge that cookies (and presumably other mechanisms) used exclusively for usage statistics should not require consent. (Recital 21 further recognizes that cookies are "a legitimate and useful tool, for example, in measuring web traffic to a website".) While the ePR provides an exception for "web audience measurement," Article 8(1)(d) only excludes this type of analytics when done *directly* by a service provider requested by the end user. It is unclear how this language applies to the existing analytics ecosystem, which is often carried out by third-party providers on behalf of website and service providers, since website owners may not have the knowledge or capabilities to provide their own effective first-party analytics.

The Commission's approach is understandable, given how opaque third-party tracking can be in today's ad-based internet offerings.[21] The question is whether this approach is going to be effective in providing the user control and transparency the Commission intends.

(3) The Draft ePR Remains Overly Prescriptive and Over Emphasizes the Role of Web Browsers

Though the draft ePR recognizes that device fingerprinting and other inferential and probabilistic tracking technologies raise serious privacy issues,[22] the proposal continues to view and address cookies as a matter of particular concern, and we note that, with respect to its provisions on consent, the proposal also focuses disproportionately on user interaction with traditional websites. This is evident from Recitals 22-24, wherein browsers are referred to extensively as mediators of access to digital services. It is doubtful that traditional use of websites will continue to be as important as it is today. Detailed legislative mandates on browsers could be rendered irrelevant, even in the medium term. For several years there has been a significant shift towards mobile devices, notably smartphones and the apps that run on them.[23] New forms of applications, including wearables, are going to become ever more widely used, and a continued focus on the role of web browsers and cookies does not address how to properly obtain consent or to offer controls for other tracking and tagging capabilities.

---

[19] Article 29 Working Party, Opinion 4/2012 Cookie Consent Exemption, 7 July 2012, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pd.

[20] European Commisison, ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, 2015, available at http://www.bvdw.org/fileadmin/downloads/cookie-richtlinien/Studie_der_EU-Kommission_zur_ePrivacy-Richtlinie_v._31.01.2015.pdf.

[21] *See* The Murky World of Third Party Web Tracking, MIT Tech. Rev., 12 September 2014, https://www.technologyreview.com/s/530741/the-murky-world-of-third-party-web-tracking/.

[22] ePR Recital 20.

[23] Almost 8 out of 10 internet users in the EU surfed via a mobile or smart phone in 2016, Eurostat, 20 December 2016, http://ec.europa.eu/eurostat/documents/2995521/7771139/9-20122016-BP-EN.pdf/f023d81a-dce2-4959-93e3-8cc7082b6edd; *see also* Charles Arther, Apps more popular than the mobile web, data shows, The Guardian, 2 April 2014, https://www.theguardian.com/technology/appsblog/2014/apr/02/apps-more-popular-than-the-mobile-web-data-shows.

In the future, meaningful privacy controls will be the shared responsibility of browsers, mobile operating systems, and other dedicated IoT platforms. End users will engage with devices that communicate with not just apps but also their homes, vehicles, and bodies. The ePR mandates software-based controls without a full appreciation of the complexity of the current online ecosystem or how internet services operate. We caution that the obligations required of software developers in Article 10 may be excessively specific and prescriptive.

Absent centralized controls, the Commission insists that entities will be able to obtain user consent by means of individual requests to end users,[24] but this only encourages industry to engage in the sorts of practices and pop-up banners that generated consent fatigue with the existing ePD.[25] To the extent the ePR is designed to address tracking concerns with respect to advertising business models, it is also worth emphasizing that the GDPR arguably already provides detailed obligations and safeguards for processing of data for advertising and/or profiling purposes. Recitals 70-72 and Article 21 of the GDPR specify that data subjects have the right to object to such data processing at any time. In that sense it seems unnecessarily prescriptive, perhaps superfluous, to specify a requirement in Article 9(3) of the ePR for providers to remind users of the right to withdraw consent every six months.

Consent is the only grounds for processing data under the ePR, and it may be too restrictive.

Like the GDPR, the ePR establishes a strong consent-based framework for processing data. Yet the ePR goes beyond the GDPR. Article 9(1) of ePR refers appropriately to the corresponding GDPR provisions[26] that consent be freely given, specific, informed, and unambiguous and requires an affirmative action on the part of an end user. However, Articles 9(2) and 9(3), which impose further technical and procedural mechanisms on top of consent, seem to be more or less redundant. As use of digital technology evolves, there will most likely be additional models for expressing consent and to set user privacy preferences. We recommend that that the ePR simply refer to the GDPR's consent obligation as it does in the first provision of Article 9.

Further, it is not obvious why the general legal framework for data processing established in the GDPR should not also apply in the context of electronic communications. The GDPR also provides a strong consent-based framework, but a key difference is that it is also includes a provision for processing based on an entity's "legitimate interest". The legitimate interest is set out in GDPR Article 6(1)(f) and allows processing of data without consent if this interest is not found to override the fundamental right to privacy and data protection. The GDPR specifies that determining whether a legitimate interest exists requires careful assessment, and excludes cases where the data subject cannot reasonably expect such processing. It is for DPAs to determine the balance between legitimate interest and consent. Some fear that the legitimate interest exception will be too broad and will risk 'swallowing the

[24] ePR Explanatory Memorandum § 3.4.
[25] LucidPrivacy, New ePrivacy Rules will Transform Consent — But How?, 10 May 2017, https://lucidprivacy.io/new-eprivacy-rules-will-transform-consent-but-how-1536f159c4d5.
[26] GDPR Art. 4(11).

rule'.[27] If true, this would be a serious privacy concern. On the other hand, DPAs have the authority to make determinations about the rights of the data subject and the legitimate interest of the processor under the GDPR. It would seem consistent with GDPR to take a similar approach under the ePR.

A prioritisation of consent over context in the ePR also leads to counter-intuitive consequences. For example, location data and metadata may generally only be processed with consent under the more restrictive ePR regime while explicitly personal data governed by the GDPR may be processed subject to the full range of acceptable legal bases. Regardless of whatever one's preferred degree of privacy protection should be, this is an incongruous and unequal result. The ePR attempts to address this in certain limited situations where the proposal's consent-based frameworks has clear negative consequences for uses of communications data that are a high value to society -- importantly, these are exceptions that the Commission could presently identify.

For example, Recital 17 discusses use of location information to generate 'heatmaps' or to enable public authorities and public transport operators to understand transport infrastructure. Because the ePR does not include any sort of carve out for legitimate interests like the GDPR, the Article 8(2)(b) of the ePR creates a carve-out of sorts where "clear and prominent notice" can be displayed informing individuals about the modalities of collection, its purpose, and the entity responsible for such collection. Whether this approach will prove workable is impossible to know.

In general, methods for offering users notice and obtaining their consent in the digital environment are, and should be, a major focus for research and development. The situation today is generally seen to be unsatisfactory. Privacy notices are often long and incomprehensible disclaimers, aimed at legal compliance and minimizing risk of litigation. In general, users click through their consent without reading these notices, and they have not proven effective tools for the user to make well-informed decisions.[28] The draft ePR seems to rely completely on this traditional form of notice and consent mechanism, but it is not clear that user control and transparency would improve. There is a great need for continuing technical and process innovation in this area, and it is important that the legal language on notice and consent is flexible enough to accommodate new and improved solutions[29]. This will especially be the case in IoT environments, where browser-type interfaces are not in operation and where the prescriptive and technology-specific language in the draft ePR will not apply in a meaningful

[27] EDRi, for example, cautions that the concept of "legitimate interests" is "notoriously slippery". European Digital Rights, Key Aspects of the Proposed GDPR Explained, https://edri.org/files/GDPR-key-issues-explained.pdf. *See also* Klint Finley, EU Cracks Down on Data Privacy, but Loopsholes May Remain, Wired, 15 April 2016, https://www.wired.com/2016/04/eu-cracks-data-privacy-loopholes-may-remain/ (highlighting concerns raised by Access Now).

[28] A 2014 study of U.S.-based internet users discovered that 52% surveyed did not know what a privacy policy was. Pew Research Center, December 2014, http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/ . This has been a common and recurring problem with respect to online notices. *E.g.*, Cameron Scott, Fewer Than Half of Facebook and Google Users Understood the Sites' Privacy Policies, 4 May 2012, http://www.pcworld.com/article/255076/fewer_than_half_of_facebook_and_google_users_understood_the_sites_privacy_policies.html.

[29] See for example: http://sagebase.org/governance/participant-centered-consent-toolkit/

way. The question is whether the ePR approach will be conducive to the sorts of innovative solutions that will be needed going forward.

The ePR does not include the concept of pseudonymous data, an inconsistency with the GDPR that may have unintended consequences.

Articles 7(1) and 7(2) require electronic communications service providers to either erase or make anonymous content and metadata, when no longer needed for the purpose of transmitting the communication. Under the GDPR, data that has been rendered anonymous such that "the data subject is no longer identifiable" is not covered by the Regulation, but anonymisation is a high standard, if not impossible[30]. Ensuring data is rendered in such a way that no individual can ever be identified either directly or indirectly by any means or by any person is challenging, and perfect anonymisation, if resulting in usable data, is a technically complex task.[31]

The GDPR also recognizes more intermediate steps/classifications of data beyond personal data and anonymised data. For example, for purposes of processing data by means other than legitimate consent, the GDPR recognizes that data controllers can take into account "the existence of appropriate safeguards, which may include encryption or pseudonymisation".[32] Pseudonymisation is recognized as a sort of middle road and is defined as "processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information." To pseudonymise a data set, the "additional information" must be "kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable person".[33] It might be worth considering ensuring that the ePR opens up the possibility to process pseudonymous data under the safeguards set out by GDPR.

The draft ePR could enable access to electronic communications data by public authorities that is significantly broader than the ePrivacy Directive. Strong safeguards for privacy are necessary.

In the 2002 ePD, Article 15 allows Member States to adopt legislation that limits the ePD's protections for certain purposes. These purposes are: "defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system".[34] The ePD makes reference to these purposes, set out in the corresponding Article 13(1) of Directive 95/46/EC.

The draft ePR provisions in Article 11 broadens the scope for Member States to adopt such legislation. Member States may suspend ePR protections if justified by the any of the objectives set out in GDPR Article 23(1)(a)-(e). This list includes the purposes in DPD Article 13(1), and adds: "other important

[30] See article by Professor Ross Anderson, Cambridge University: https://www.edge.org/response-detail/27195.
[31] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques, 10 April 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pd.
[32] GDPR Art. 6(5)(d).
[33] GDPR Art. 4(5).
[34] ePD Art. 15.

objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security".[35]

This could permit a significant expansion of public authorities' ability to compel providers of electronic communications services to hand over users' personal data, including location and metadata. Where the ePD provision was narrowly focused on law enforcement, criminal investigations and public security, the ePR allows public authorities access to data for any "other important objectives of general public interest". This could enable public sector agencies to access a far broader range of personal data than permitted under the ePD.

In addition, under the ePD the data made accessible to law enforcement authorities consisted mainly of traffic and location data held by providers of traditional telecommunications services. But, as mentioned above, the ePR definition of electronic communications data captures a vastly expanded amount of data and categorises a much broader range of companies as electronic communications providers. This opens up the possibility of broader access to this data by a wide array of public authorities. This is a cause for concern. At a minimum, it will be essential to include strong safeguards in line with the recent ruling by the Court of Justice of the European Union in *Tele2/Watson* cases from 21 December 2016.[36]

Furthermore, the issue of law enforcement access to e-evidence is becoming increasingly complex. There are significant ambiguities and jurisdictional conflicts in determining when and under what conditions providers of electronic communications services (under the EPR definition) are obliged or permitted to provide user data (whether content, location/transmission data or subscriber information) to law enforcement authorities of which countries. The European Commission, led by DG Migration and Home Affairs, is working on policy recommendations in this area.[37]

It is crucial that these issues are dealt with in a manner that do not undermine protection of communications data, while at the same time enabling law enforcement to access data necessary for criminal investigations, and give legal certainty to service providers. It is important that the debate on the ePR is coordinated with this policy process.

---

[35] GDPR Art. 23(1)(e).

[36] Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen & C-698/15 Secretary of State for the Home Department v Tom Watson and Others, *available at* http://curia.europa.eu/juris/liste.jsf?num=C-203/15 (the CJEU suggested that EU law precludes "general and indiscriminate retention of traffic data and location data" and that legislation was permissible for targeted retention of data solely for the purpose of fighting serious crime or preventing serious risk to public security).

[37] European Commission, DG Migration and Home Affairs, e-evidence, https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/e-evidence_en (last visited 10 May 2017).

The draft ePR should affirm the right of providers and users to use encryption technology to protect the confidentiality of communications.

Encryption technology is an essential tool to enable secure transactions, communications and storage of data. Without these technologies, Europe's digital economy and society would not be able to function. The importance of secure communications has been recognised by EUROPOL and ENISA in a joint statement in May 2016.[38] At the same time, there is an ongoing policy debate in the EU and elsewhere about cases in which law enforcement agencies have difficulty intercepting, decrypting and accessing communications or electronic data that they deem useful for criminal investigations and counter-terrorism operations. This has led to calls from high-level policy makers for encryption 'backdoors' and even bans on the provision of communications services equipped with end-to-end encryption. The European Commission's DG Migration and Home Affairs is working on analysing the technical and legal issues involved in this discussion and aims to provide policy recommendations to JHA Ministers by the end of 2017.[39]

The draft ePR sidesteps this debate entirely, although the EDPS has emphasised that new ePrivacy rules "should clearly allow users to use end-to-end encryption (without 'backdoors')" and "decryption, reverse engineering or monitoring of communications protected by encryption" should be explicitly prohibited.[40] Instead, the only reference in the draft ePR is made in Recital 37 (replicating Recital 20 of the ePD), which suggests that electronic communications providers should inform customers of steps they can take to protect the confidentiality of their communications.

It is unfortunate that the importance of technical measures to protect the confidentiality of communications is not reflected in the draft ePR. It would be desirable to include an article that affirms the right for both service providers and users to use the best available technologies, such as end-to-end encryption, to protect electronic communications confidentiality. This provision should also set out strong safeguards and clear limits on the ability of law enforcement authorities to interfere with or break such technical measures. The ePR should also include a general prohibition on providers from decrypting, reverse engineering, or monitoring communications protected by encryption. It should specify that service providers are not permitted to degrade the security of systems.

[38] Joint Statement, ENISA & EUROPOL on Lawful Criminal Investigation, 23 May 2016, https://www.enisa.europa.eu/news/enisa-news/enisa-europol-issue-joint-statement.
[39] European Commission, DG Migration and Home Affairs, Encryption, https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/encryption_en 2(last visited 10 May 2017).
[40] Opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC) at 3, 22 July 2016, https://edps.europa.eu/sites/edp/files/publication/16-07-22_opinion_eprivacy_en.pdf.