Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

European Union Law Working Papers

No. 39

A Balancing Act: Assessing the Impact of the Proposed European ePrivacy Regulation on the Digital Single Market and European Privacy Rights

Emily Pehrsson

2019

European Union Law Working Papers

Editors: Siegfried Fina and Roland Vogl

About the European Union Law Working Papers

The European Union Law Working Paper Series presents research on the law and policy of the European Union. The objective of the European Union Law Working Paper Series is to share "works in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The working papers can be found at http://ttlf.stanford.edu.

The European Union Law Working Paper Series is a joint initiative of Stanford Law School and the University of Vienna School of Law's LLM Program in European and International Business Law.

If you should have any questions regarding the European Union Law Working Paper Series, please contact Professor Dr. Siegfried Fina, Jean Monnet Professor of European Union Law, or Dr. Roland Vogl, Executive Director of the Stanford Program in Law, Science and Technology, at:

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Emily Pehrsson is a J.D. candidate at Stanford Law School. During law school, Ms. Pehrsson studied European business law, including privacy law, for a quarter at the University of Vienna School of Law. Her main areas of interest include privacy, data protection, and cyber crime. She worked as a summer law clerk in the Criminal Division's Cyber Unit at the U.S. Attorney's Office and a summer associate at both Covington & Burling LLP and Harris, Wiltshire & Grannis LLP. She earned her bachelor's degree *summa cum laude* in International Relations at the College of William & Mary in 2013. Prior to law school, she worked as a Management Consultant with Deloitte's Federal Consulting practice, where she focused on implementing enterprise and innovation strategy for government clients.

General Note about the Content

Suggested Citation

This European Union Law Working Paper should be cited as:
Emily Pehrsson, A Balancing Act: Assessing the Impact of the Proposed European ePrivacy Regulation on the Digital Single Market and European Privacy Rights, Stanford-Vienna European Union Law Working Paper No. 39, http://ttlf.stanford.edu.

Copyright

Abstract

As part of the European Digital Market Strategy, the European Commission proposed an overhaul to the e-Privacy Directive (ePD), the EU's primary law regulating the privacy of electronic communications. The proposed e-Privacy Regulation (ePR) would update the outdated ePD, resolve conflicts between the ePD and newly-implemented GDPR, and expand the law's scope to include non-traditional communications providers.

This paper analyzes the anticipated impact of the ePR on digital economic growth and privacy protections in Europe. It identifies weaknesses in the current proposal and suggests a series of revisions. Specifically, the scope of the ePR should cover OTTs and ancillary service providers, but M2M service providers should be excluded. The ePR's data processing criteria should more closely align to the GDPR, so regulators should liberalize the current consent-based approach by permitting processing for a prevailing legitimate interest. The ePR grants Member States broad discretion in establishing their own enforcement mechanism, which will result in inconsistent implementation across the EU. This discretion should be limited to reduce variation in ePR enforcement. Finally, the penalty provisions adopted from the GDPR are too stringent, going beyond what is necessary for deterrence and risking economic growth in the digital sector. The range of possible penalties should be narrowed and the maximum penalties reduced. Overall, the ePR should be adopted to update the ePD in light of the GDPR and technological innovation, but it requires additional revision avoid imposing unnecessary administrative burdens on Europe's digital economy.

Table of Contents

1. Introduction

Facing unprecedented data breaches and a burgeoning digital economy, the European Union is again considering ambitious legislation to safeguard EU citizens' privacy online. CIOs, CEOs, and regulators worldwide are now familiar with the EU General Data Protection Regulation (GDPR), an omnibus law that prompted large-scale internal audits of data use policies and required many companies to spend millions on compliance. EU regulators have shifted their focus to a related, but distinct, area: electronic communications.

Following the implementation of GDPR in May 2018,[1] the European Union is expected to adopt a version of the proposed e-Privacy Regulation (ePR) in 2019.[2] The purpose of the ePR is to safeguard the privacy of electronic communications in the EU, including communications' content and associated metadata.[3] The ePR was first proposed in January 2017, but is still the subject of trialogue negotiations amongst the Commission, European Parliament, and Council.[4] The ePR is not the EU's first attempt to regulate the privacy of electronic communications—the

[1] European Commission, '2018 Reform of EU Data Protection Rules' <https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en#abouttheregulationanddataprotection> accessed 24 November 2018.
[2] *See* Cynthia O'Donoghue and John O'Brien, 'Proposed amendments to the ePrivacy Regulation' (*Technology Law Dispatch*, 16 August 2018) <https://www.technologylawdispatch.com/2018/08/regulatory/proposed-amendments-to-the-eprivacy-regulation/> accessed 24 November 2018.
[3] *See* Proposal for a Regulation of the European Parliament and of the Council 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) [19 October 2018] 2017/0003(COD), arts. 1, 2(1)(a) [hereinafter October 2018 ePR Draft].
[4] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/8/EC (Regulation on Privacy and Electronic Communications) [10 January 2017] 2017/0003(COD) [hereinafter January 2017 ePR Draft]; October 2018 ePR Draft.

EU enacted the e-Privacy Directive (ePD) in 2002 and updated it in 2009.[5] The proposed ePR, if approved, will replace the ePD.[6]

This paper examines the ePR's proposed changes, taking into account the interplay between the ePR and the GDPR. Specifically, it predicts the effect the ePR would have on the European digital economy.[7] It simultaneously assesses whether this approach fulfills the EU's privacy and data protection obligations under the Charter of Fundamental Rights of the European Union[8] and the European Convention on Human Rights (ECHR).[9] This paper analyzes the provisions relating to communications data processing—including related provisions on the scope of application, enforcement, and penalties.[10] It does not address, however, provisions pertaining to terminal equipment safeguards or "Rights to Control Electronic Communication"—for example, caller identification and blocking, directory information, and communications for direct marketing.[11]

Considering the EU's obligations to safeguard citizens' privacy under the Charter while promoting the free movement of data in a European digital single market, I propose a series of revisions to the current ePR draft. First, I advocate removing M2M technologies from the scope

---

[5] Directiive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37 [hereinafter 2002 ePD]; Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L337/11 [hereinafter 2009 ePD].

[6] 2002 ePD; 2009 ePD.

[7] *See* European Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe' (2015) COM(2015) 192 final [hereinafter DSM Strategy].

[8] Charter of Fundamental Rights of the European Union (Charter of Fundamental Rights) arts. 7-8.

[9] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) arts. 8-9.

[10] January 2017 ePR Draft, chs. 1-2, 4-5.

[11] *See, e.g.,* January 2017 ePR Draft, ch. 3.

of the ePR, while extending the law to OTTs and ancillary services. Second, I recommend more closely aligning the data processing criteria between the GDPR and ePR, moving the latter away from a consent-based approach to allow processing for prevailing legitimate interests. Third, I explain how the enforcement approach in the latest ePR draft echoes the weaknesses present in the ePD, arguing that GDPR enforcement authorities should oversee both the GDPR and ePR. Finally, I advocate for a narrower range of possible fines for violations of the ePR, which would reduce discrepancies across Member States that could inhibit the free movement of data.

2. General Overview of the E-Privacy Regulation

The ePR is a legislative proposal intended to protect the privacy of electronic communications in the EU.[12] In contrast to its predecessor, the ePR is a regulation. As such, it will be directly applicable, not requiring transposition into national law by the EU Member States.[13] By transitioning from a directive to a regulation, the Commission aimed to minimize discrepancies in Member States' interpretation and implementation that developed under the ePD.[14]

In general, the ePR regulates electronic communications' content and metadata.[15] Content is the message that is transmitted using electronic means, regardless of whether it is text, a picture, audio, or video.[16] Metadata is the rest of the information relating to a communication that is used to complete the communication—e.g., location, time, duration, or recipients.[17] Under the ePR, the communications provider must keep electronic communications confidential.[18] Not only

[12] *See* October 2018 Draft ePR, arts. 1, 2(1)(a).
[13] January 2017 ePR Draft, Explanatory Memorandum, sec. 2.4.
[14] *Ibid.*
[15] *See* January 2017 ePR Draft, arts. 2(1), 4(3)(a). *See also* October 2018 ePR Draft, art. 2(1)(a).
[16] January 2017 ePR Draft, art. 4(3)(b); October 2018 ePR Draft, art. 4(3)(b).
[17] January 2017 ePR Draft, art. 4(3)(c); October 2018 ePR Draft, art. 4(3)(c).
[18] January 2017 ePR Draft, art. 5; October 2018 ePR Draft, art. 5.

would more obvious actions, such as listening to or monitoring communications violate confidentiality—"processing of electronic communications data" is also prohibited under the confidentiality umbrella for anyone besides the end user of the communications service.[19] The ePR establishes a baseline prohibition of communications data processing; from that baseline, it outlines limited conditions under which communications service providers can collect or process content and metadata.[20] This paper analyzes these provisions, in particular.

Next, the ePR regulates the data that communications services providers are permitted to collect from or store on end users' devices.[21] These devices are called "terminal equipment," a term including smartphones, iPads, and laptops.[22] This provision governs what are commonly known as "cookies," in addition to other data collection technologies. A cookie is a data packet that is sent to a terminal device and stored there.[23] Cookies are used to track online activity, including website visits and navigation activity on a website.[24] Cookies enable consumers to store prospective purchases in a "shopping cart" or save login information for a subsequent visit.[25] The ePR would impose a general prohibition of these types of technologies, subject to limited exceptions.[26] An analysis of these provisions is not included in this paper and is a subject for further research.

The ePR's chapter 3 includes provisions enabling end users to control incoming or outgoing communications on their devices.[27] These provisions are not addressed in this paper, so they will

[19] *Ibid.*
[20] January 2017 ePR Draft, arts. 6-7; October 2018 ePR Draft, arts. 6-7.
[21] January 2017 ePR Draft, art. 8; October 2018 ePR Draft, art. 8.
[22] January 2017 ePR Draft, art. 4(1)(c); October 2018 ePR Draft, art. 4(1)(c); Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment [2008] OJ L162/20, art. 1(1).
[23] Norton, 'What Are Cookies?' <https://us.norton.com/internetsecurity-how-to-what-are-cookies.html> accessed 26 November 2018.
[24] *Ibid.*
[25] *Ibid.*
[26] January 2017 ePR Draft, art. 8; October 2018 ePR Draft, art. 8.
[27] January 2017 ePR Draft, ch. 3; October 2018 ePR Draft, ch. 3.

receive little attention here. The most important section of this chapter imposes restrictions on direct marketing using electronic communications.[28] Call-blocking of unwanted calls to end users,[29] information disclosures in public directories,[30] and caller identification rules[31] are also included in this chapter.

Lastly, the ePR establishes enforcement mechanisms, remedies, and penalties. The enforcement authority structure is still in flux during the ongoing trialogue negotiations. In the initial January 2017 ePR draft, the GDPR's supervisory authorities in each Member State were given the added responsibility of overseeing the ePR.[32] In the October 2018 draft, however, Article 18 was amended to exclude references to the GDPR's supervisory authority.[33] This change gives Member States discretion to set up the supervisory authority as they choose. Remedies and penalties, however, remain linked to the GDPR's penalty provisions.[34] Consequently, they apply the GDPR' stringent fines to the ePR. Violations of certain provisions of the ePR can result in maximum fines of 2% of the total worldwide annual turnover or €10 million.[35] Other provisions trigger the even more serious fine of 4% of the total worldwide annual turnover or €20 million.[36] Member States are given discretion to set penalties for provisions not specifically covered by Article 23, leaving room for divergent policies to develop across the EU.[37]

[28] January 2017 ePR Draft, art. 16; October 2018 ePR Draft, art. 16.
[29] January 2017 ePR Draft, art. 14; October 2018 ePR Draft, art. 14.
[30] January 2017 ePR Draft, art. 15; October 2018 ePR Draft, art. 15.
[31] January 2017 ePR Draft, art. 12-13; October 2018 ePR Draft, art. 12-13.
[32] January 2017 ePR Draft, art. 18.
[33] October 2018 ePR Draft, art. 18.
[34] January 2017 ePR Draft, art. 21(1), 23(2)-(5); October 2018 ePR Draft, art. 21(1), 23(2)-(5).
[35] January 2017 ePR Draft, art. 23(2); October 2018 ePR Draft, art. 23(2).
[36] January 2017 ePR Draft, art. 23(3), (5); October 2018 ePR Draft, art. 23(3), (5).
[37] January 2017 ePR Draft, art. 23(4); October 2018 ePR Draft, art. 23(4).

The ePR is related to the GDPR, but the two regulations govern different types of data. The ePR, like the ePD, is *lex specialis* in relation to the GDPR; while the latter regulates the processing of personal data, the ePR governs electronic communications, which can include personal or non-personal information.[38] Personal data not contained in a communication would fall under the purview of the GDPR, while personal or non-personal data in a communication would be subject to the ePR, the more specific piece of legislation.[39] Additionally, the GDPR pertains only to natural persons, whereas the ePR protects communications for both natural and legal persons.[40] The GDPR is grounded in Article 8 of the Charter, governing data protection, versus Article 7 for the ePR, governing privacy in one's personal life and communications.[41] It is precisely because these two regulations are closely related that an update to the ePD was prioritized this year, following the GDPR's implementation.[42] With the ePR update, EU regulators have the opportunity to clarify how the two laws should interact and eliminate contradictions between them. If done successfully, regulators can reduce legal uncertainty in the EU, increasing economic growth and preempting costly litigation.

[38] January 2017 ePR Draft, Explanatory Memorandum, sec. 1.2.
[39] *Ibid.*
[40] *See* 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) [hereinafter GDPR], art. (1-2); January 2017 ePR Draft, art. 1(102); October 2018 ePR Draft, art. 1(1-2).
[41] Neil Dyer, 'GDPR versus ePrivacy Regulation: What's the Difference?' The Marketing Eye Blog (30 August 2018) <https://www.themarketingeye.com/blog/marketing-tips/post/the-difference-gdpr-eprivacy-regulation.html> accessed 23 November 2018.
[42] European Commission, 'Proposal for an ePrivacy Regulation' <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation> accessed 15 October 2018.

3. Foundational Principles

3.1 The Charter of Fundamental Rights, ECHR, and TFEU

The EU protects the privacy of its citizens through several provisions in the Charter of Fundamental Rights and the ECHR. The latest ePR draft directly links its protection of electronic communications privacy with Article 7 of the Charter, [43] which states: "Everyone has the right to respect for his or her private and family life, home, and communications."[44] There is a close relationship between a person's electronic communications—which can include instant messages, texts, emails, etc.[45]—and the privacy she is entitled to in her private life. These communications can serve as a map of someone's s hobbies, relationships, ideological leanings, and daily patterns. The ePR attempts to fulfill a portion of Article 7's broad mandate.

Article 8 of the Charter was foundational to the GDPR's stringent protection of personal data.[46] Despite its closer tie to the GDPR, Recital 4 of the ePR references the Charter's Article 8(1), which states: "Everyone has the right to the protection of personal data concerning him or her."[47] Personal data can be conveyed through electronic communications, and thus compromised if the confidentiality of a communication is violated.

The European Convention on Human Rights similarly protects family life and communications. When it proposed the legislation, the Commission used Article 8 of the ECHR to justify application of the ePR to legal—in addition to natural—persons.[48] According to Article 8,

[43] October 2018 ePR Draft, rec. 19, Annex 1.
[44] Charter of Fundamental Rights, art. 7.
[45] October 2018 ePR Draft, art. 4(3)(b): "'Electronic communications content' means the content exchanged by means of electronic Communications services, such as text, voice, videos, images, and sound."
[46] GDPR, rec. 1.
[47] *Ibid.*, art. 8.
[48] January 2017 ePR Draft, Explanatory Memorandum, sec. 2.1.

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

Echoing Article 7 of the Charter, the ECHR lends additional weight to Europe's defense of its citizens' privacy in their personal lives, particularly regarding their communications.

While the ePR does not reference Article 9 of the ECHR, safeguarding communications privacy is critical to securing "freedom of thought, conscience, and religion."[49] Communications' content and metadata can shed light on sensitive information in a person's life.[50] These freedoms can be threatened if communications are not appropriately safeguarded.

Finally, Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) states that "Everyone has the right to the protection of personal data concerning them."[51] Articles 16 and 114 are the legal basis of the ePR.[52]

3.2 Free Movement of Data

In tension with citizens' rights to privacy, the EU has an obligation to prevent obstructions to the free movement of data within the Union. The ePR's Article 1(2) states:

[49] ECHR, art. 9; *see also* January 2017 ePR Draft, Explanatory Memorandum, sec. 3.9.
[50] October 2018 ePR Draft, rec. 2.
[51] Treaty on the Functioning of the European Union (TFEU), art. 16(1). *See also* October 2018 ePR Draft, rec. 4.
[52] January 2017 ePR Draft, Explanatory Memorandum, sec. 2.1.

> "The free movement of electronic communications data and electronic communications services within the Union shall be neither restricted nor prohibited for reasons related to the respect for the private life and communications of natural persons and the protection of natural persons with regard to the processing of personal data, and for protection of communications of legal persons."[53]

Free movement of data is a necessary component of the European internal market, especially as the digital sector becomes a larger component of the overall economy.[54] EU companies must rely on data-driven analytics to remain competitive, necessitating access to data across national boundaries.[55] Recently, some EU leaders have referred to the free movement of data as the EU's "fifth freedom," complementing the free movement of goods, labor, capital, and services.[56] Several EU laws will affect the free movement of data in the Union, including the GDPR, the proposed ePR, and the newly-approved regulation on the free flow of non-personal data.[57] In effect, the ePR may curtail or expand the free movement of data in the EU, depending on how it balances the free movement of data with citizens' rights to privacy in their communications.

---

[53] October 2018 ePR Draft, art. 1(2). Safeguards against restrictions to free movement here have been narrowed since the initial January 2017 draft. In that draft, Article 1(2) did not allow restrictions of free movement of data to protect the "private life and communications of natural and legal persons." January 2017 ePR Draft, art. 1(2).
[54] In 2015, the data economy made up 1.94% of the EU's GDP. In 2016, its share rose to 1.99%. By 2020, it could reach 4%. European Commission, 'Building a European Data Economy' <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy> accessed 16 October 2018.
[55] European Commission, 'A framework for the Free Flow of Non-Personal Data in the EU' (Press Release) (21 June 2018, updated 4 Oct 2018) <http://europa.eu/rapid/press-release_MEMO-18-4249_en.htm>.
[56] Samuel Stolton, 'A 'Fifth Freedom' of the EU: MEPs Back an End to Data Localization (*Euravtiv*, 4 October 2018) <https://www.euractiv.com/section/data-protection/news/a-fifth-freedom-of-the-eu-meps-back-end-of-data-localisation/>; European Parliament, 'Free Flow of Non-personal Data: Parliament Approves EU's Fifth Freedom' (Press Release) (4 October 2018) <http://www.europarl.europa.eu/news/en/press-room/20180926IPR14403/free-flow-of-non-personal-data-parliament-approves-eu-s-fifth-freedom>.
[57] *See* Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union [2017] 2017/0228 (COD).

3.3 DIGITAL SINGLE MARKET STRATEGY

An impetus for the recent wave of legislation surrounding privacy, free movement of data, and data protection has been the EU's Digital Single Market Strategy (DSM Strategy).[58] Adopted in May 2015, the DSM Strategy aims to develop Europe's digital economy by eliminating national barriers to online activities in the Union.[59] In the current system, small- and medium-sized enterprises in the EU are often failing to leverage online capabilities, with a mere 7% selling across national borders.[60] Complying with other country's online regulations poses a substantial obstacle to the development of cross-border business.[61] Siloing data within Member States prevents companies from using large-scale data analytics to drive innovation.[62] In an attempt to establish favorable regulatory conditions for the development of the digital economy, the EU adopted three initiatives under the DSM.[63] First, the EU will facilitate access to online commerce across Member States.[64] Second, it will put in place the infrastructure and regulations necessary for an innovative and fair digital market.[65] Third, the EU will make strategic investments in digital capabilities intended to drive digital economic growth.[66]

The second initiative highlighted the necessity of increasing consumer confidence in digital service providers to promote growth in the digital economy.[67] Specifically, in an era of

---

[58] European Commission, 'Roadmap for Completing the Digital Single Market /// Initiatives' <https://ec.europa.eu/commission/sites/beta-political/files/roadmap_en.pdf> [hereinafter DSM Roadmap].
[59] DSM Strategy, at 3.
[60] European Commission, 'Why We Need A Digital Single Market' <https://ec.europa.eu/commission/sites/beta-political/files/dsm-factsheet_en.pdf>, at 2.
[61] *See ibid*. at 2: "Small online businesses wishing to trade in another EU country face around €9,000 extra costs for having to adapt to national laws. If the same rules for e-commerce were applied in all EU Member States, 57% of companies would either start or increase their online sales to other EU countries."
[62] DSM Strategy, at 14.
[63] *Ibid.* at 3-4.
[64] *Ibid.* at 3.
[65] *Ibid.* at 3-4.
[66] *Ibid.* at 4.
[67] *Ibid.* at 12.

frequent cyber breaches and data misuse, the EU planned to enact measures protecting personal data of consumers online. One such measure was reviewing the ePD in light of the GDPR.[68]

4. Directive to Regulation

The Commission introduced the ePR as a regulation to integrate the digital single market across Europe.[69] The Commission asserted that allowing Member States to regulate electronic communications independently would create an inconsistent regulatory landscape, disrupting the cohesion of the EU's internal market.[70] Incongruent national legislation would risk siloing data within national borders, potentially inhibiting innovation and economic growth.[71] Variations in the way communications are regulated in the EU makes it more difficult for businesses to work across borders.[72] Defending its choice of instrument in the January 2017 ePR draft, the Commission explained that "A Regulation can ensure an equal level of protection throughout the Union for users and lower compliance costs for businesses operating across borders."[73] Furthermore, the GDPR and ePR regulate closely-related subject matter—since the GDPR is a regulation, the ePR should also be for the sake of legal clarity.[74]

Public opinion in the EU indicates that the ePD was less effective as a directive than it would have been as a regulation because it required transposition into national law yielding disparate interpretations the ePD's provisions. In 2016, the Commission completed a public consultation on the ePD. It found that 76% of citizen and civil society organization respondents believed that

[68] *Ibid.* at 13; DSM Roadmap.
[69] January 2017 ePR Draft, Explanatory Memorandum, sec. 2.2.
[70] *Ibid.*
[71] *Ibid.*
[72] *Ibid.* at 3.1.
[73] *Ibid.* at 2.4.
[74] *Ibid.* at 2.2.

the ePD did not fully accomplish its privacy objectives.[75] One reason that respondents were dissatisfied with the ePD was that Member States implemented the law differently, so end users received varying levels of protection across the EU.[76] Though informative, this statistic should be taken with a grain of salt—it does not reflect industry responses and fails to indicate what proportion of the 76% cited the ePD's transposition specifically as the cause of its shortfalls.

The Commission determined that there was substantial differentiation in the measures enacted by Member States to implement the ePD.[77] In addition to five Member States failing to meet the implementation deadline,[78] the Commission noted that seven Member States granted broader protection than the ePD mandated.[79] As a result, the providers and types of services covered by the ePD varied based on the applicable Member State law. Under the ePD, Member States were tasked with transposing communications confidentiality provisions into national law.[80] Some Member States opted to protect the confidentiality of only in-transit communications, while others extended the protections to messages before they were sent or after they were received.[81] Member States also diverged in the regulation of metadata, or "traffic data." While most Member States drafted one law addressing both content and metadata, others chose to differentiate metadata from content and regulate it in a separate law.[82] Divergence in the

[75] European Commission, 'Summary Report on the Public Consultation on the Evaluation and Review of the ePrivacy Directive' (4 August 2016) <https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive>.
[76] *Ibid.*
[77] European Commission, 'Ex-Post REFIT evaluation of the ePrivacy Directive 2002/58/EC' (Commission Staff Working Document) (10 January 2017), sec. 5.1 [hereinafter REFIT Evaluation].
[78] *Ibid.*
[79] *Ibid.*
[80] European Commission, 'ePrivacy Directive: Assessment of Transposition, Effectiveness and Compatibility with Proposed Data Protection Regulation' (Report) SMART 2017/0071, at 42.
[81] *Ibid.*
[82] *Ibid.*

implementation of fundamental tenets of the ePD created an excessive administrative burden, hindering the free movement of data and economic growth.

As an important caveat, some of the ePD's implementation challenges were caused by vague provisions, rather than from the legal instrument itself. For example, the ePD required Member States to establish a "competent national authority" to enforce the law.[83] The Commission explained the issues that stemmed from this provision: "Each of these authorities has different responsibilities, structures, and inherent specificities not conducive to reaching the same views on the interpretation and enforcement of the ePD, so that the same processing is treated divergently across Member States and thus impacts cross-border processing activities."[84] Undoubtedly, Member States implemented the ePD's enforcement provision in different ways—but it was the provision's text, not the instrument, that caused the legal uncertainty. In the October 2018 ePR draft, the parallel provision states: "Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation ('supervisory authorities')."[85] Despite changing the instrument from a directive to a regulation, writing in broad discretion for Member States on the enforcement mechanism will nevertheless transfer this provision's weakness from the ePD to the ePR.

Considering the various perspectives in the choice of instrument debate, a regulation is more likely than a directive to enable free movement of data in the European Union, while safeguarding citizens' privacy rights more equally across the EU. The lower administrative burden from a regulation will likely promote economic growth in Europe's digital economy. Some of the obstacles to legal clarity and consistent implementation under the ePD, however,

[83] 2009 ePD, art. 15(a)(2).
[84] REFIT Evaluation, sec. 6.1.3.
[85] Oct. 2018 ePR Draft, art. 18(0).

will persist under the latest ePR draft. For example, the draft allocates broad authority to Member States to override the rights and obligations the ePR establishes.[86] As mentioned above, it fails to proscribe a specific structure for enforcement authorities, instead leaving enforcement primarily to the Member States' discretion. The Commission made the appropriate decision in choice of instrument to meet the obligations of the Charter and ECHR, as well as its goals under the DSM. It failed in another regard, however, by allotting too much discretion to Member States in some provisions. For those provisions, the drafting negates the benefits gained from changing the instrument from a directive to a regulation. Consequently, free movement of data and economic growth would not be maximized under the current ePR draft.

5. Extending ePR Scope to Include Over-the-Top (OTT) Providers, Ancillary Services, and M2M Services

The ePR proposes extending communication privacy rules from traditional telecommunications providers to include over-the-top (OTT) providers, ancillary services, and machine-to-machine services.[87] OTT providers are electronic communications services that are functionally equivalent to traditional communication services, and so can be used as substitutes by consumers.[88] Examples of OTTs are "Voice over IP [VoIP], instant messaging and web-based e-mail services."[89] Under the 2002 and 2009 ePD, consumers using Skype video-calling, Gmail, Facebook messenger, or Whatsapp were not covered by the Directive's privacy protections.[90]

[86] October 2018 ePR Draft, art. 11(1): "Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate, and proportionate measure in a democratic society to safeguard one or more of the general public interests . . . or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests."
[87] *See e.g.*, January 2017 ePR Draft, arts. 2(1), 3(1), 4(1)(b), 6-7.
[88] REFIT Evaluation, sec. 6.3.2.
[89] January 2017 ePR Draft, Explanatory Memorandum, sec. 1.1.
[90] REFIT Evaluation, sec. 6.3.2.

Furthermore, in addition to OTT providers, the ePR draft extends the law's scope to include communication services that are ancillary to another service.[91] Chat functions within dating or gaming applications are examples of ancillary services.[92] The October 2018 ePR draft limits this provision to communications between a sender and a finite group of recipients that the sender chooses.[93]

The ePR draft also broadens the regulatory scope to include machine-to-machine (M2M) services.[94] These services—typically referred to as the Internet of Things (IoT) [95]—encompass "automated transfer[s] of data and information between devices or software-based applications with limited or no human interaction."[96] In one example, sensors installed on parking spaces can communicate with cars in the area, notifying them when the space is open.[97] In another, a thermostat can be programmed to sense the changing temperature of a house and adjust the heater accordingly.[98] The ePR would cover not only communications between people online, but these automated communications between machines and devices as well.

If these new service categories are included in the final version of the ePR, under the current ePR text, they would be bound by the ePR's data processing limitations.[99] Electronic communications providers would be obligated to keep end-users' communications data confidential—preventing companies from, for example, processing or storing the data—unless

[91] October 2018 ePR Draft, rec. 11a. *See also* January 2017 ePR Draft, rec. 11 (including ancillary services within the scope of the law, but without the "finite recipient" requirement that is present in the October 2018 draft.)
[92] Dan Dwyer and Elaine Morrissey, 'More Data Rules for May 2018: ePrivacy Regulation' (McDowell Purcell, 3 April 2017) <https://www.mcdowellpurcell.ie/data-rules-may-2018-eprivacy-regulation/>.
[93] October 2018 ePR Draft, rec. 11a.
[94] October 2018 ePR Draft, rec. 12; January 2017 ePR Draft, rec. 12.
[95] *See, e.g.,* January 2017 ePR Draft, rec. 12.
[96] October 2018 ePR Draft, rec. 12.
[97] *Ibid.*
[98] *Ibid.*
[99] January 2017 ePR Draft, art. 6; October 2018 ePR Draft, art. 6.

their activities fell within a series of exceptions enumerated in the ePR.[100] The exceptions have varied in the recent drafts, but typically include end-user consent,[101] processing required to complete the communication,[102] and processing necessary for the maintenance of the communications network,[103] among other reasons. Service providers would also incur data erasure obligations[104] and limitations on their interactions with end-users' terminal equipment.[105]

The primary justification for extending ePR obligations to OTT, ancillary, and M2M providers is safeguarding consumers' communication privacy across the board, not just for select communication services.[106] Use of OTT services rose rapidly in the last decade; in 2010, OTT services constituted a small minority of overall messages sent, but three years later, they were the majority.[107] This trend is expected to continue, making OTTs even more predominant.[108] Both technology and consumer preferences have changed in the communications sector, opening up new avenues for communication and shifting consumers away from traditional communication services. The Article 29 Data Protection Working Party supports expanding the scope of the ePR, arguing that because OTTs are functionally equivalent to traditional providers, they "have a similar potential to impact on [sic] the privacy and right to secrecy of communications of people in the EU."[109]

[100] January 2017 ePR Draft, art. 5-6; October 2018 ePR Draft, art. 5-6.
[101] October 2018 ePR Draft, art. 6(2)(c).
[102] *Ibid.*, art. 6(1)(a).
[103] *Ibid.*, art. 6(1)(b).
[104] *Ibid.*, art. 7.
[105] *Ibid.*, art. 8.
[106] REFIT Evaluation, sec. 6.3.2.
[107] REFIT Evaluation, sec. 6.3.2 (citing DG for Internal Policies, 'Over-the-Top players (OTTs), Study for the IMCO Committee' (2015), at 31).
[108] *Ibid.*
[109] Article 29 Data Protection Working Party, 'Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)' (4 April 2017) <https://iapp.org/media/pdf/resource_center/wp247enpdf.pdf>, at 3.

The Commission also argued that the current regulatory landscape disadvantages traditional providers, who are competing under the burden of the ePD, while OTTs are not.[110] OTTs may be able to exploit this regulatory inequality to gain market share from traditional telecommunications providers. If OTT providers offer services that are functionally equivalent, and consequently substitutable, to traditional communication services, they should be held to the same regulatory standard.

Public opinion is, predictably, split between consumers, government officials, and civil society on one side, and the plurality of industry organizations on the other side: "76% of citizens, consumer and civil society organisations and 93% of public authorities believe the rules should (in part) be broadened to cover over-the-top service providers. On the contrary, industry is more divided as 42% do not want the scope to be broadened while 36% do."[111] Some industry representatives have argued that OTT providers, ancillary providers, and M2M services should all be excluded from the ePR due to the inherent differences between them and traditional telecommunications providers.[112] Unlike traditional providers, using and collecting end users' data is a key component of nontraditional communications services.[113] Consequently, strict regulations on the use of data, particularly if primarily consent-based, can severely undermine this flourishing industry.[114] Alternatively, industry representatives argued that including M2M services in addition to OTT providers is a dramatic overreach unjustified by the Commission's

[110] *Ibid.*
[111] European Commission, 'ePrivacy: Consultations Show Confidentiality of Communications and the Challenge of New Technologies are Key Questions' (Public Consultation) (19 December 2016) <https://ec.europa.eu/digital-single-market/en/news/eprivacy-consultations-show-confidentiality-communications-and-challenge-new-technologies-are>.
[112] Centre for Information Policy Leadership, 'Comments on the Proposal for an ePrivacy Regulation' (11 September 2017) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_the_proposal_for_an_eprivacy_regulation_final_draft_11_september_2017.pdf>, at 5-6 [hereinafter CIPL Report].
[113] *Ibid.*
[114] *Ibid.*

explanations.[115] Due to the growing IoT sector, M2M services generate an increasingly large portion of the data being processed in today's economy.[116] Currently, personal data in the EU is regulated by the GDPR's Article 6. If the ePR applies to M2M data processing, it would carve out a substantial portion of the data already regulated by the GDPR's Article 6. This situation would create confusion and undermine the GDPR's balance between data use and privacy.[117] Furthermore, M2M services enhance the efficiency, safety, and usability of machines and devices consumers use in their daily lives and work. Subjecting these transmissions to confidentiality requirements beyond the GDPR's protections could create unnecessary burdens for consumers and businesses.[118]

In evaluating the scope of the ePR, one consideration must be consumers' ability to understand the general tenets of the law, in order to adjust their conduct accordingly. It seems unreasonable to expect an average consumer without legal or technical training to make a distinction between traditional electronic communication providers and OTT / ancillary providers. If the law maintained the same definition employed by the ePD, consumers would need to make this distinction when deciding which communications service to use and what they are willing to disclose on that service. Not only is it unlikely that consumers will be able to make this distinction, it also would be inefficient to expect consumers to educate themselves on the nuances of privacy law to make mundane decisions about which communication service to use. If the ePR covered only traditional communications providers, the most likely outcome is a continuation of the current situation—consumers assume that communications services with

[115] *Ibid.* at 4.
[116] *Ibid.*
[117] *Ibid.*; GDPR, art. 6.
[118] The American Chamber of Commerce in the European Union, 'E-Privacy Proposal: A Roadblock to Innovation' <http://www.amchameu.eu/sites/default/files/infographic-amchameu-eprivacy.pdf> accessed 23 November 2018.

similar functionalities are treated the same under the law. Making this erroneous assumption, consumers' privacy can be more easily compromised by unregulated OTT providers capitalizing on this lack of awareness. The Charter does not qualify European citizens' right to privacy based on the type of provider; failing to cover OTTs and ancillary services, therefore, would be a decision to limit the broad maxim of Article 7.

Protecting OTTs from further regulation, however, might be justified if the benefits of innovation and economic growth outweigh the added privacy protections. EU regulation in this sphere cannot be considered in a vacuum. EU companies must compete with services based outside of the EU, particularly in the United States and possibly China, in the future. Some stakeholders assert that it is precisely the data-driven nature of OTTs, ancillary services, and M2M technologies that make them valuable to customers.[119] Regulators cite consumers' transition to non-traditional services as grounds for the extension of the ePR's scope—but perhaps it was precisely this lack of regulation that made these services appealing in the first place. These non-traditional services are often highly-tailored and responsive to consumer preferences—consequences of using consumer data creatively and effectively.[120] Presumably, substantially restricting companies' ability to use the data that formed the core of their competitive advantage would risk stagnating this critical growth industry in the EU. Reflecting on the impact of the GDPR, however, the EU may be able to use the ePR to force major companies worldwide to accept EU privacy standards as the new baseline. Companies that choose not to fragment their services between markets may opt to adhere to the most stringent standard—which, arguably, would lessen the risk that European companies would fall behind international competitors. Even if Europe's relative growth is not at risk, however, restricting

[119] CIPL Report.
[120] *Ibid.*

companies' data use under the ePR still risks causing a general slow-down in digital economic growth. Such a slow-down could risk jobs and hinder innovation benefitting consumers.

In this same vein, regulators have acknowledged that imposing new privacy regulations on businesses will increase their costs.[121] As compliance expenses rise, companies must divert their capital from R&D, market entry, and other growth-oriented investments to address added legal constraints.[122] As a result, economic growth can slow as businesses face a higher barrier to entry, new products are stalled or slower to roll out, and innovation decreases.[123] If EU regulations become too onerous, companies will avoid launching new technologies in the EU until they have reached maturity, denying EU citizens the latest innovations on the market.[124] The Commission addressed these concerns by noting that compliance costs would only rise for those service providers that do not already operate on a consent model—but the Commission failed to otherwise quantify the projected costs to innovation.[125]

The extent of the ePR's administrative burden can be adjusted in two basic ways. First, the scope of services can be limited by excluding OTT providers, ancillary providers, M2M services, or all three from regulation. Second, the ePR's scope can remain broad, but the substantive provisions can be reworked to limit the impact of the law. Weighing the arguments made by civil society organizations, regulators, and industry representatives, the ePR's scope should be partially limited, excluding M2M services. Despite the data-driven nature of OTT and ancillary service providers' businesses, EU regulators makes a compelling argument that they are functionally equivalent to traditional communications services, with nearly identical information

[121] *See* January 2017 ePR Draft, Explanatory Memorandum, sec. 3.4.
[122] Richard Steinnon, 'Unintended Consequences of the European Union's GDPR' (*Forbes* 27 November 2017) <https://www.forbes.com/sites/richardstiennon/2017/11/27/unintended-consequences-of-the-european-unions-gdpr/#78957954243c>.
[123] *Ibid.*
[124] *Ibid.*
[125] *See* January 2017 ePR Draft, Explanatory Memorandum, sec. 3.4.

being conveyed on traditional, OTT, and ancillary services. Subjecting a subsection of providers to regulation while excluding another group with a similar function and impact would be inequitable and substantially undermine the protections outlined in the Charter. M2M services, however, should be excluded from the ePR. For automatic transmissions between devices and machines, requiring consent from an end-user would have a greater negative than positive impact. Personal data collected in this way is protected by the GDPR already. M2M services do not communicate human-generated messages, so the risk to EU citizens' privacy is lower. The cost of demanding consent for an IoT service would unnecessarily slow down innovation and economic growth. Consequently, the regulatory scope should be extended to OTT and ancillary providers, but exclude M2M providers.

6. Provisions Protecting the Confidentiality of Communications

The ePR's provisions protecting communications are more restrictive than the GDPR's personal data protections. While the ePR uses primarily a consent-based approach,[126] the GDPR permits processing for a wider range of justifications,[127] including "legitimate interest."[128] The substance of the communications privacy provisions is based in a general declaration that "electronic communications data shall be confidential."[129] This provision prohibits "any interference with electronic communications data," save when a specific exception applies.[130] Interference includes almost any use of data, including "storing," "monitoring," and "processing."[131]

[126] October 2018 ePR Draft, art. 6.
[127] GDPR, art. 6.
[128] GDPR, art. 6(1)(f).
[129] October 2018 ePR Draft, art. 5.
[130] *Ibid.*
[131] *Ibid.*

Communications data in this context includes both the content of a communication and its metadata.[132] Electronic communications providers can process both content and metadata to complete the communication or maintain and defend the network, e.g., from security risks.[133] Metadata may be processed under a variety of exceptions, including end-user consent, limited scientific research, network maintenance and optimization, billing for services, and protecting end users' vital interests.[134] Even if the metadata falls within a specific exception, providers must adhere to certain safeguards, such as pseudonymization.[135] Such metadata can only be shared with third parties if it is made anonymous.[136] Content can only be processed for two reasons in the latest draft. First, it can be used to provide a service to an end user that has *explicitly* asked for it, provided that the processing would not "adversely affect fundamental rights and interests of another person concerned" and is limited to the duration necessary to provide the service.[137] Second, providers may process data if the end user consents, it is not possible to anonymize the data, and the provider conducts an impact assessment and consults with the supervisory authority prior to processing.[138] Finally, the October 2018 draft adds a new provision not contained in the January 2017 draft—it permits third parties to process data meeting the conditions of Article 6 so long as they also fulfill the conditions of the GDPR's Article 28.[139]

Unsurprisingly, industry representatives generally oppose the ePR's consent-driven model. One major concern is that it diverges from the GDPR's model, which permits processing for legitimate interests, a broader, if somewhat vague, category.[140] The GDPR and ePR deal with

[132] October 2018 ePR Draft, art. 4(3)(a).
[133] *Ibid.*, art. 6(1).
[134] *Ibid.*, art. 6(2).
[135] *Ibid.*, art. 6(2a)(e).
[136] *Ibid.*, art. 6(2aa)(b).
[137] *Ibid.*, art. 6(3)(aa).
[138] *Ibid.*, art. 6(3)(b).
[139] *Ibid.*, art. 6(4).
[140] CIPL Report, at 2.

categories of data that overlap—personal data within communications. By implementing more stringent consent provisions to the data falling under the ePR's purview, the EU risks undermining the model established in the GDPR.[141] This situation will also risk increasing administrative costs, as organizations must navigate different standards in at least two major laws.

Industry representatives have also pushed back against the consent-based model by arguing that it is burdensome for consumers.[142] Some research has shown that consent requests become less valuable to end-users as their number increase.[143] Indeed, the 2009 ePD generated substantially more consent requests for online cookies, which regulators recognized were burdensome, negatively impacted the web-browsing experience, and were not as effective as they should be.[144] Frequently, consumers accepted cookies without understanding what they were agreeing to.[145]

Lobbyists have argued that the ePR's consent requirements and restrictions on third-party transfers will undermine the free press, allowing only larger players to publish online.[146] Data-driven advertising, for example, would be severely restricted by the ePR, inhibiting publications' ability to generate revenue and thus, stay in business.[147] Regulators have pushed back, arguing alternatively that privacy is a fundamental right and thus outweighs such concerns. They have

---

[141] *Ibid.*
[142] Harting, 'Study on the Impact of the Proposed ePrivacy Regulation' (19 October 2017) <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/epr_-_gutachten-final-4.0_3_.pdf>.
[143] *Ibid.*, at 11 (citing Bart W. Schermer, Bart Custers and Simone van der Hof, 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014) Vol. 16 Issue 2 Ethics and Information Technology, 171-182.).
[144] January 2017 ePR Draft, Explanatory Memorandum, sec. 3.1.
[145] *Ibid.*
[146] Jennifer Baker, 'Behavioral Advertising Industry Slams ePrivacy Plans' (*IAPP* 7 September 2017), <https://iapp.org/news/a/behavioral-advertising-industry-slams-eprivacy-plans/>.
[147] *Ibid.*

also maintained that the ePR is only updating the existing ePD, not implementing revolutionary changes to this sector.[148]

While it is true that privacy is a fundamental right, free movement of data and freedom of expression are also important rights in the EU—the balance between them is not proscribed, but it seems reasonable that none of them should displace the others. Regarding regulators' second counter-argument, it is true that Article 5 of the ePD made communications confidential, subject to a consent exception.[149] The scope of the ePD, however, was limited to traditional communications providers—so while this is an update to the status quo for some companies, it is an entirely new regulatory regime for others.

In presenting the first draft of the ePR, regulators noted that "78% [of EU citizens] say it is very important that personal information on their computer, smartphone, or tablet can only be accessed with their permission."[150] Additionally, the European Data Protection Supervisor (EDPS) argued that traditional telecommunications services are already subject to consent provisions—they cannot use end-users' metadata, for example, to offer value-add services without the consent of the end user.[151] By contrast, OTT providers in particular have taken advantage of their lack of regulation to design and offer new data-driven services using consumer data.[152] This, the EDPS argues, creates an unequal playing field between types of service providers and undermines EU citizens' rights to privacy.[153]

---

[148] *Ibid.*
[149] 2002 ePD, art. 5(1).
[150] January 2017 ePR Draft, Explanatory Memorandum, sec. 3.2 (citing European Commission, Flash Eurobarometer 443 Report e-Privacy (2016)).
[151] Giocanni Buttarelli, 'The Urgent Case for a New ePrivacy Law' (European Data Protection Supervisor 19 October 2018) <https://edps.europa.eu/press-publications/press-news/blog/urgent-case-new-eprivacy-law_en>.
[152] *Ibid.*
[153] *Ibid.*

Industry representatives have advanced some alternatives to the proposed ePR approach. Some industry representatives called for self-regulation, but this outcome is highly unlikely. The more reasonable alternative was aligning the ePR's standards more closely to the GDPR, which permits processing based on a prevailing legitimate interest.[154] The GDPR requires heightened consent standards for processing of "special categories" of personal data.[155]

Considering the arguments on both sides, regulators should more closely align the GDPR's processing provisions with the ePR. Legitimate interest processing is a term that must necessarily be clarified further in case law, and has already created legal uncertainty. However, it will counteract "consent fatigue" issues that will likely arise from the consent-driven model presented in the current ePR draft. It will also reduce the legal uncertainty that would arise when companies try to navigate different standards for data processing under the GDPR and ePR. The legitimate interest processing standard was deemed adequate to protect EU citizens' privacy interest under the Charter when regulators adopted the GDPR; while it would relax the privacy protections under the ePR, it would still afford protection while permitting data markets more freedom to grow and innovate. Legitimate interest processing strikes a more appropriate balance between digital economic growth and privacy protections than a consent-based model, which could threaten the competitiveness of a key European growth sector.

The prior consultation requirement in Article 6(3)(b) should be removed from the law. Requiring companies to suspend processing in order to consult a supervisory authority that may or may not have adequate resources to handle such an influx of requests risks not only European businesses' efficiency and innovation, but imposes unreasonable costs on the government as well. The GDPR avoided prior consultation provisions except in extreme cases—a controller is

[154] CIPL Report, at 2. *See* GDPR, art. 6(f).
[155] GDPR, art. 9.

only mandated to consult with the supervisory authority if a data protection impact assessment "indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk."[156] The proposed ePR provision requires an impact assessment and prior consultation with the supervisory authority even after end users have consented to the processing. The risks of backlog and unnecessary administrative burden here outweigh the benefits, given that consent is already a requirement of the provision.

7. Enforcement

The oversight approach in the ePR varies little from the ePD, despite the administrative burden the ePD created.[157] The ePD was enforced by a "competent national authority," the structure of which was left to the discretion of the Member States.[158] Similarly, the October ePR draft provides that each Member State will designate a "supervisory authority" responsible for overseeing the application of the ePR, including authorizing penalties and other remedies.[159] This provision modifies the January 2017 draft, which assigned ePR oversight to the GDPR supervisory authority.[160] According to the Commission's assessment of the ePD:

> "Each of these authorities has different responsibilities, structures, and inherent specificities not conducive to reaching the same views on the interpretation and enforcement of the ePD, so that the same processing is treated divergently across Member States and thus impacts cross-border processing activities."[161]

[156] GDPR, art. 36.
[157] *See* ePD, art. 15a.
[158] *Ibid.*
[159] October 2018 ePR Draft, art. 18.
[160] January 2017 ePR Draft, art. 18; GDPR, art. 51.
[161] REFIT Evaluation, sec. 6.1.3.

The same report found that most stakeholders, including both industry and consumers, believed that this enforcement structure undermined the effectiveness of the ePD.[162] Consequently, the January 2017 ePR draft explicitly called for an "alignment of the supervisory authorities with the authorities competent to enforce the GDPR" to decrease the ePR's administrative burden.[163] The approach presented in the October 2018 draft risks exacerbating the ePD's enforcement failures even further. In addition to the confusion that can result from a different enforcement authority in each Member State, now regulated organizations may have to coordinate with both a GDPR and ePR supervisory authority. This enforcement approach would be costlier for businesses, slowing economic growth. It also would not afford greater privacy protection to end users and will likely result in different levels of protection for end users across the EU.

Given the enforcement approach adopted in the GDPR, it is highly unlikely that the EU would adopt a central enforcement approach for the ePR—although for the sake of legal clarity, it should be considered in the future. The lack of specificity in the October 2018 draft, however, can at least be remedied. Centralizing enforcement of the related ePR and GDPR legislation will decrease the administrative burdens and enhance cohesion between the two laws. The January 2017 approach, extending the authority of the GDPR supervisory authority to the ePR, should be reinstated. Consequently, inconsistency in enforcement across Member States can be minimized, if not eliminated—reducing potential barriers to the free movement of data without substantially affecting Charter privacy rights.

[162] *Ibid.*
[163] January 2017 ePR Draft, Explanatory Memorandum, sec. 3.5.

8. Remedies, Liabilities, and Penalties

The remedies, liability, and penalties in the ePR closely mirror the GDPR's stringent provisions. End-users that have been harmed by an infringement to the ePR's provisions were given a right to sue for damages to compensate the loss.[164] Depending on the violation, an entity can be fined the higher of "EUR 10 000 000 or . . . up to 2% of the total worldwide annual turnover of the preceding year,"[165] or "EUR 20 000 000 or . . . up to 4% of the total worldwide annual turnover of the preceding financial year."[166] For violations not addressed by either of these provisions, Member States may determine the penalty.[167]

These penalties, which were subject to frequent debate following the GDPR's adoption, are controversial in the context of the ePR as well. The implementation of the heightened penalties is a divergence from the ePD's penalty approach.[168] A key goal of such high penalties is deterrence.[169] While the GDPR's recitals call for a consideration of the context of the violation in determining the fine level, the threat of a maximum fine persists.[170] Companies must consider the risk of incurring the maximum fine when determining their courses of action.

The threat of such high penalties, as seen from the GDPR compliance push, has encouraged companies to take the law seriously. Consequently, consumer privacy likely benefits, helping to fulfill the Charter's privacy rights. These provisions could, however, create a backlash—fearing massive fines, some companies may choose to avoid the EU market altogether, or at least until they have reached a maturity level that can support the compliance and legal costs that

---

[164] October 2018 ePR Draft, art. 22. *See also* GDPR, art. 79.
[165] October 2018 ePR Draft, art. 23(2). *See also* GDPR art. 83(4).
[166] October 2018 ePR Draft, art. 23(3). *See also* GDPR, art. 83(5).
[167] October 2018 ePR Draft, art. 24.
[168] Alex van der Wolk and Sotirios Petrovas, 'First Wave of Ripple Effects off the General Data Protection Regulation' (2017) 34 No. 18 Westlaw Journal Computer and Internet 1, 5. *See* ePD 2002, rec. 47.
[169] General Data Protection Regulation (GDPR), 'Key Issues' <https://gdpr-info.eu/issues/fines-penalties/> accessed 3 December 2018.
[170] GDPR, rec. 148.

necessarily result from the legislation. EU citizens' privacy will be more adequately safeguarded, but consumers may lose out on new technologies that may be rolled out in the United States, China, or other markets prior to entering the EU. Furthermore, the penalty provisions only establish a maximum level and lay out vague guidelines for supervisory authorities to consider as they determine the fine for a particular case. As a result, there could be substantial divergence across Member States in the average fines doled out, which could over the long run create uncertainty in the market, inhibit the free movement of data, and slow digital economic growht.

Such a large range of potential fines goes beyond what is necessary to protect EU citizens' privacy. Lower fines could still have a deterrent effect, but would decrease the chance that Member States would adopt dramatically different fine levels. They would also encourage reasonable expenditures on compliance by businesses, without imposing a crippling financial burden. Such a scenario would more effectively balance rights to the free movement of data and Charter privacy protections.

If regulators maintain these high penalties, they should build in a long lead time following adoption of the final law, allowing organizations the necessary time to evaluate their systems and practices and update, as needed.

9. Conclusion

Revising the ePD with an updated ePR regulation is a needed step to promote the European digital single market, safeguard Europeans' privacy under the Charter, and enable free movement of data. Considering arguments made by industry, EU citizens, regulators, and civil society organizations, I propose revisions to the scope, data processing model, enforcement structure, and penalties range. With revisions, the ePR can increase European consumers' privacy

protections while avoiding unreasonable administrative costs that would substantially slow the growth of Europe's digital economy.