Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique

Peter Swire & Yianni Lagos

Public Law and Legal Theory Working Paper Series
No. 204

May 31, 2013

MARYLAND LAW REVIEW

VOLUME 72 2013 NUMBER 2

Essay

WHY THE RIGHT TO DATA PORTABILITY LIKELY REDUCES CONSUMER WELFARE: ANTITRUST AND PRIVACY CRITIQUE

PETER SWIRE* & YIANNI LAGOS**

TABLE OF CONTENTS

* C. William O'Neill Professor of Law, at the Moritz College of Law of the Ohio State University. Brett Frischmann has provided insights at each stage of this paper. Thanks to comments from participants at the George Mason Conference on Competition, Search, and Social Media, the Intellectual Property Scholars Conference 2012, and a workshop at Cardozo Law School. Ingrid Mattson provided outstanding research support. Thanks for research funding from the Moritz College of Law. The authors also appreciate support from the Future of Privacy Forum, which receives financial support from a wide array of organizations, including software and online companies that would be affected by the right of data portability. The views expressed here are those of the authors, and were developed without specific funding or consultation with supporters of the FPF.

** Yianni Lagos received his J.D. and M.B.A. from the Ohio State University. He is currently a Legal and Policy Fellow with the Moritz College of Law of the Ohio State University and the Future of Privacy Forum.

INTRODUCTION

This Essay addresses a new economic and human right the European Union has included in a Draft Regulation[1] that would bind all its Member States: the right to data portability ("RDP").[2] The basic idea of the RDP is that an individual would be able to transfer his or her personal data and other material from one information service to another without hindrance.[3] A core example, referenced in the explanatory materials to the Draft Regulation, is for consumers to control the material they have posted to a social networking site such as Face-

1. *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and On the Free Movement of Such Data (General Data Protection Regulation)*, art. 18, at 53, COM (2012) 11 final (Jan. 25, 2012) [hereinafter "Draft Regulation"].

2. *Id.*

3. *Id.*

book.[4] In this example, the right would require it to be easy for users to transfer their photos, videos, and status updates to another social networking site.[5]

We emphasize at the outset that the idea of data portability is appealing.[6] As consumers, we like the convenience of easily moving all of "our" stuff to a new service if we so choose.[7] The RDP as defined in Article 18 of the Draft Regulation, however, is unprecedented and problematic. The new RDP provides the user (called the "data subject" under E.U. law)[8] the right to obtain data "in an electronic and structured format which is commonly used and allows for further use by the data subject."[9] Article 18, in many settings, also requires information in an automated processing system to be transferred "in an electronic format which is commonly used, without hindrance" from the entity operating the system directly to another entity.[10] We introduce the term "export-import module" ("EIM") to highlight the unprecedented nature of the RDP.[11] As drafted, Article 18 often requires an online service to write specialized code (the EIM) that will export the data from that service and import it into a second service.[12] The text of Article 18 is in no way limited to social networks; its lan-

4. *Id.* at 26.

5. *Id.* Even in the absence of legal requirements, Facebook has now provided a tool to enable consumers to download all of their data in a single computer file. Matthew Rogers, *Facebook to Allow Users to Download Their Data*, SWITCHED DOWNLOADSQUAD (Oct. 7, 2010, 4:40 AM), http://downloadsquad.switched.com/2010/10/07/facebook-to-allow-users-to-download-their-data/.

6. *See, e.g.*, *Vision & Mission*, DATAPORTABILITY PROJECT (Mar. 19, 2009), http://wiki.dataportability.org/pages/viewpage.action;jsessionid=2EDEAF2341B315BA17520E6301EDC4E9?pageId=3440714 (last visited Oct. 4, 2012) (explaining the convenience of data portability).

7. *Id.*

8. This Essay will use the terms "user," "consumer," and "data subject" interchangeably.

9. Draft Regulation, *supra* note 1, art. 18(1), at 53.

10. *Id.* art. 18(2), at 53.

11. *See* discussion *infra* Parts I.B.1, II–IV.

12. *See* Draft Regulation, *supra* note 1, art. 18(1), at 53 (giving data subjects the right to obtain their data in a commonly used format).

guage applies generally to cloud computing, web services, smartphone apps, and other automated data processing systems.[13]

More generally, data portability can address a "lock-in" or high switching costs problem—users start to use one service, such as Facebook, and then find it costly or technically difficult to shift to another service, even if they prefer the other service.[14] One rationale for a legal right to portability in such instances would be to reduce monopoly power and improve competition in the market, so that new services can innovate and attract customers away from the original service.[15] Within E.U. law, an important additional rationale for the RDP is to implement human rights related to privacy (generally called "data protection" in the E.U.).[16] The drafters of the RDP justify it as building on fundamental data protection rights included in earlier European legal instruments, such as the 1995 Data Protection Directive.[17] Proponents would include the new rights created by the Draft Regulation as fundamental rights under E.U. law.[18] In addition to competition law and fundamental rights, interoperability is an additional possible argument in favor of Article 18.

While we underscore our hope that major online services will provide data portability in many settings, we nonetheless write this Essay to express serious concerns about the RDP as drafted. A principal reason for our concern is that Article 18 is a bad fit with U.S. antitrust and E.U. competition law.[19] The concerns about lock-in and high switching costs have been extensively addressed in antitrust law.[20] One crucial requirement in competition law is that market domi-

13. *See* Gabriela Zanfir, *The Right to Data Portability in the Context of the EU Data Protection Reform*, 2 INT'L DATA PRIVACY L. 149, 149 (2012) (discussing Article 18's application to cloud computing).

14. *Id.* at 152.

15. *Id.*

16. Draft Regulation, *supra* note 1, at 1–2.

17. Council Directive 95/46/EC, art. 12, 1995 O.J. (L 281) 42 (EC) [hereinafter Council Directive 95/46/EC]; *see also* Draft Regulation, *supra* note 1 (noting the 1995 directive and recognizing that further initiatives might be necessary).

18. Zanfir, *supra* note 13, at 151.

19. *See infra* Part II.

20. ANDREJ FATUR, EU COMPETITION LAW AND THE INFORMATION AND COMMUNICATION TECHNOLOGY NETWORK INDUSTRIES: ECONOMIC VERSUS LEGAL CONCEPTS IN PURSUIT OF (CONSUMER) WELFARE 86–87 (2012).

nance must be shown, typically by demonstrating high market share.[21] The text of Article 18, however, applies to a start-up software company in a garage just as it does to a monopolist. In examining the best means to achieve the goal of consumer welfare, the U.S. and the E.U. have a nuanced application of the rule of reason, not the per se requirements of Article 18.[22] Competition law, not Article 18, would consider the many efficiencies that result from a service provider deciding what functions to include in its products, which undergo rapid innovation.[23]

Another concern is that Article 18 suffers from serious difficulties regarding privacy or data protection law.[24] No jurisdiction has experimented with anything resembling the proposed Article 18, casting serious doubt on its status as a new human right protecting privacy.[25] Among other difficulties, Article 18 poses serious risks to a long-established E.U. fundamental right of data protection: the right to security of a person's data.[26] Previous access requests by individuals were limited in scope and format.[27] By contrast, when an individual's lifetime of data must be exported "without hindrance," one moment of identity fraud can turn into a lifetime breach of personal data.[28]

A final concern with Article 18 is that the affirmative mandate to create an EIM goes far beyond previous law relating to interoperability, in both the U.S. and E.U., where the second service is permitted to write interoperable code, despite objections by the first service.[29]

---

21. *Id.* at 247.

22. *See, e.g.*, *id.* at 162; United States v. Microsoft Corp., 253 F.3d 34, 94 (D.C. Cir. 2001) (noting that the rule of reason is better suited to an appropriate balancing of benefits and costs than a per se rule).

23. *See infra* Part II.B.

24. *See infra* Part III.

25. *See infra* Part III.B.

26. *See infra* Part III.B.

27. *See infra* Part III.B.

28. *See infra* Part III.C.

29. *See* Lotus Dev. Corp. v. Borland Int'l, Inc., 49 F.3d 807, 815 (1st Cir. 1995), *aff'd*, 516 U.S. 233 (1996) (explaining that a method of operation, or the way a system is used, can be employed and explained by other users in their own words, and is thus "uncopyrightable"); Council Directive 91/250/EEC, art. 6, 1991 O.J. (L 122) 45 [hereinafter Council Directive 91/250/EEC] (stating that permission from the first service need not be sought when it is necessary to reproduce and translate code to achieve interoperability); Case C-406/10, SAS Inst. Inc. v. World Programming Ltd., 2011 E.C.R. I-13, ¶ 61 (finding

The new, mandated code must also perform at a high level of interoperability, transferring the data "without hindrance."[30] In practice, achieving interoperability is often a difficult task, requiring tailored code to interact with different recipients.[31] But the RDP puts a new obligation on the first service to write the EIM and meet that ambitious standard.[32]

Part I of the Article explains the RDP as contained in the Draft Data Protection Regulation issued by the European Commission in January, 2012. The RDP would apply both within the E.U. and to online services globally that sell in the E.U.[33] Part II analyzes the RDP under antitrust or competition law. A key finding is that the RDP, designed to help consumers, appears to reduce consumer welfare as understood in competition law. Competition law, in both the U.S. and E.U., recognizes important efficiencies that can occur from lock-in for some situations; notably, a certain level of switching costs can encourage investment in new products and services, creating efficiency over time.[34] In addition, the Draft Regulation as written can reduce interoperability by creating an incentive to use non-standard formats; only "standard and commonly used" formats trigger the RDP requirements.[35]

Part III analyzes the RDP as an expansion of human rights from a data protection and privacy perspective. With the absence of previous experimentation with data portability rules, and no consensus among experts about best practices, it is risky to lock in sweeping new requirements.[36] Part IV examines the RDP in light of other interoperability law, including *Lotus Development Corp. v. Borland International*[37]

---

that the "functionality of a computer program reproduced in another computer program" is not a copyright violation).

30. Draft Regulation, *supra* note 1, art. 18(2), at 53.

31. Rajiv Shah & Jay P. Kesan, *Lost in Translation: Interoperability Issues for Open Standards*, 8 I/S: J. L. & POL'Y 113, 113 (2012).

32. *See infra* Part IV.

33. Draft Regulation, *supra* note 1, art. 3(2), at 41.

34. *See* FATUR, *supra* note 20, at 176 ("[T]he core issue with regard to imposing a duty to deal is balancing short-run gains in efficiency with long-run incentives to invest and compete dynamically, which should be done on a case-by-case basis.").

35. *See infra* Part II.B.

36. *See infra* Part III.B.

37. 49 F.3d 807 (1st Cir. 1995).

and the E.U. Computer Programs Directive,[38] and shows that the proposed RDP goes considerably beyond previous interoperability requirements.[39] The general conclusion is that the RDP deserves careful attention from academics and policymakers, both within the E.U. and elsewhere, and that a sweeping or badly implemented version of the RDP could cause significant harm.

I. ARTICLE 18: THE RIGHT TO DATA PORTABILITY

This Part examines the text of Article 18, which defines the RDP. Three examples then illustrate the sorts of interpretive challenges facing the Commission and the many software and Internet service companies that would be required to comply with the RDP.

A. The Text of Article 18

The European Commission on January 25, 2012 proposed changes to the current regulatory framework protecting the personal data of individuals (the "Draft Regulation").[40] Among those protections is the RDP.[41] This Essay is concerned with Article 18's requirements on companies to transfer consumer data.[42] More specifically, the Commission's example of transfer of data between social networks illustrates the goal of the RDP. The Draft Regulation cites the example of a social network as a rationale for Article 18: "The data subject should . . . be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one."[43] For this core example, a Facebook user would have the right to export the data governed by Article 18 to the user or another social network.

38. Council Directive 95/46/EC, *supra* note 17.

39. *See Lotus*, 49 F.3d at 815–16 (holding that a program's menu command hierarchy was not subject to copyright, even though programmers may have made some expressive choices in developing the menu functions); Council Directive 91/250/EEC, *supra* note 29 (stating that the original programmer's permission is not needed when reproducing or translating code is necessary for interoperability).

40. Draft Regulation, *supra* note 1, at 1.

41. *Id.* art. 18, at 53.

42. *Id.*

43. *Id.* at 26.

Article 18 is divided into three parts. Paragraph 1 gives consumers the right to download personal data,[44] which is defined broadly under E.U. law as "any information relating to a data subject."[45] The right applies to personal data "processed by electronic means and in a structured and commonly used format."[46] For this personal data, which we will refer to as "covered personal data," the organization that controls the data, such as the social network, must provide a copy of the covered data to the data subject.[47] The copy must be "in an electronic and structured format which is commonly used and allows for further use by the data subject."[48] In short, the user (called the "data subject" under E.U. law) has a right of data portability—a right to get a copy of the covered data in an easy-to-use format. For instance, a Facebook user would have a legal right to export his or her covered data in a form that is usable in another social network.[49]

Paragraph 2 gives consumers the right to transfer personal data and "other information" provided by the consumer in a commonly used format "without hindrance" from one processing system to another.[50] This paragraph differs in four important respects from Para-

---

44. *Id.* art. 18(1), at 53. Paragraph 1 states in full:

> The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.

Id.

45. *Id.* art. 4(2), at 41; *see also* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1873 (2011) ("[T]he European Union takes an expansionist approach to [personally identifiable information].").

46. Draft Regulation, *supra* note 1, art. 18(1), at 53.

47. *Id.*

48. *Id.*

49. *See supra* note 5.

50. Draft Regulation, *supra* note 1, art. 18(2), at 53. Paragraph 2 states in full:

> Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.

Id.

graph 1. First, it goes beyond the requirement to provide data to the data subject. It requires the first party, such as Facebook, to export the data directly to other websites, such as another social network.[51] Second, it requires data transfer to another processing system in a commonly used format "without hindrance."[52] Although the term "without hindrance" is not further defined in the Draft Regulation, the language suggests a strong obligation on the first party to have the export work smoothly. Third, Paragraph 2 extends not only to "personal data" but also to "other information" provided by the user.[53] Fourth, Paragraph 2 does not limit itself to data already stored in "a structured and commonly used format," as does Paragraph 1.[54] The right to export data applies to "any other information provided by the data subject."[55]

To further define the obligations of Article 18, Paragraph 3 vests considerable power in the Commission to determine the scope of Article 18.[56] We are not aware of any legislation in effect that implements anything like Article 18. Given that the Draft Regulation uses terms new to legislation, there is considerable uncertainty about the meaning of the RDP as defined in Article 18.

B. Defining Key Terms in Article 18

The novelty of Article 18, and the varying interpretations that can be given to its key terms, makes it difficult to gauge how broadly or narrowly the text will be interpreted. This Essay critically examines the possible rationales for and effects of Article 18. If Article 18 is interpreted broadly and enforced vigorously, then we believe there could be quite substantial effects on online software and services. Notably, as discussed in Part II, the current text of Article 18 can be in-

51. *Compare id.* art. 18(1), at 53, *with id.* art. 18(2), at 53.

52. *Id.* art. 18(2), at 53.

53. *Id.*

54. *Compare id.* art. 18(1), at 53, *with id.* art. 18(2), at 53.

55. *Id.* art. 18(2), at 53.

56. *Id.* art. 18(3), at 53. Paragraph 3 states in full:

> The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Id.

terpreted to be substantially at variance with how E.U. competition law assesses similar practices. By contrast, a narrow interpretation of Article 18, or decisions by data protection authorities not to enforce vigorously, would mean that the RDP creates few new issues—it would not be a major departure from the status quo.

We hope readers will understand this Essay as a useful attempt to analyze both the theoretical and practical implications of the innovative provisions of Article 18. The issues raised here may be helpful in considering whether to amend the current text of Article 18 before the Draft Regulation becomes final. The analysis may also be useful to the Commission and interested persons in subsequent proceedings under the authority delegated by Paragraph 3.[57] We now turn to the possible narrow and broad interpretations of three key terms: (1) "without hindrance"; (2) "other information"; and (3) "structured and commonly used format."[58]

1. Export "Without Hindrance" and the Requirement to Write an Export-Import Module

Under Paragraph 2, users have the right to transfer their data "without hindrance" to the data subject or another online service.[59] Interpretation of "without hindrance" will substantially determine the reach of Article 18. Quite possibly, under a broad reading that seems supported by the text, Article 18 requires an online service to write what we refer to as an "export-import module" ("EIM"). The EIM signifies the software code and services that will export the data from the first service and import it into a second service. The EIM software that works "without hindrance" would presumably meet the European e-Government initiative's definition of "interoperability," or "the ability of information and communication technology (ICT) systems . . . to exchange data and enable the sharing of information and knowledge."[60] A strong form of interoperability would enable consumers to transfer data seamlessly from one platform to another.[61]

57. Draft Regulation, *supra* note 1, art. 18(3), at 53.

58. *Id.* art. 18, at 53.

59. *Id.* art. 18(2), at 53.

60. *Interoperability*, IDABC EUROPEAN EGOVERNMENT SERVICES, http://ec.europa.eu/idabc/en/chapter/5883.html (last visited Nov. 12, 2012).

61. *See* JOHN PALFREY & URS GASSER, INTEROP: THE PROMISE AND PERILS OF HIGHLY INTERCONNECTED SYSTEMS 23–24 (2012) [hereinafter PALFREY & GASSER, INTEROP] (discussing the seamless transfer of information). Palfrey and Gasser emphasize downsides as

Such interoperability, however, is not free, and all consumer online services operating in the E.U. would apparently need to develop an EIM.

Under a narrower interpretation of "without hindrance," the RDP would not place an affirmative obligation on the controlling website to transfer data directly to data subjects and other websites including competitors. Instead, the RDP would primarily seek to prevent a first party from technically blocking the transfer of data to a second party. This interpretation would reduce the cost on the first party because it would not need to develop an EIM to transport data to competitors. The text of Article 18, however, may not be consistent with this narrow reading. The language appears to impose an affirmative obligation on the first party to provide software that accomplishes the goal of exporting the data easily for the data subject.

2. Defining "Structured and Commonly Used Formats"

The right to data portability in Paragraph 1 applies only to data "processed by electronic means and in a structured and commonly used format."[62] The Commission is specifically granted the authority to define what formats meet this definition.[63] "Structured" and "commonly used" are apparently two distinct formatting requirements and both must be satisfied before consumers can realize their right to data portability.

Structured data formats allow for increased functionality and easier data transfer.[64] Tim Berners-Lee is one advocate for greater use of

---

well as upsides of interoperability. We note that we received this book only after the ideas in this Essay were mostly developed and presented publicly, although we did read and benefit from the following article while developing this Essay: Urs Gasser & John Palfrey, *Breaking Down Digital Barriers: When and How ICT Interoperability Drives Innovation*, THE BERKMAN CTR. FOR INTERNET & SOC'Y (2007) [hereinafter Gasser & Palfrey, *Breaking Down*], *available at* http://cyber.law.harvard.edu/interop/pdfs/interop-breaking-barriers.pdf.

62. Draft Regulation, *supra* note 1, art. 18(1), at 53. Paragraph 3 specifically grants the Commission the power to define what counts as the "structured and commonly used formats" covered by Paragraph 1. *Id.* art. 18(3), at 53. The absence of a cross-reference to Paragraph 2 supports the view that Paragraph 2 applies and its reference to "other information" is not limited to "structured and commonly used formats." *Id.* art. 18, at 53.

63. *Id.* art. 18(3), at 53.

64. *See* Adam Cheyer & Joshua Levy, *A Collaborative Programming Environment for Web Interoperability*, SRI INT'L ARTIFICIAL INTELLIGENCE CTR., http://www.ai.sri.com/pubs/files

structured data formats. He supports the idea of a semantic web, or a "World Wide Web that enables people to share content beyond the boundaries of applications and websites."[65] To achieve the semantic web, websites would convert from using unstructured formats such as PDF, where words, data, and pictures all appear essentially as one image on a page; instead, websites would rely on structured formats such as RDL/XML, so that statistical and other information is exported to a new service in a way that allows automatic processing.[66] Currently, there is no easy tool for determining what formats count as structured. The standard-setting goals of the Internet Engineering Task Force, for instance, do not include a structured format.[67] The Commission will thus have to develop the expertise to determine over time which formats are sufficiently structured.

Once the Commission decides that a format is structured, it must still determine whether a format is commonly used.[68] A structured format is not necessarily commonly used—there are many standards that are not widely adopted.[69] The difficulty of finding the actual usage of a format will further complicate the Commission's task. It may be difficult enough for the Commission to assess the number of sales of a software package or downloads from a site. It is even more diffi-

/1272.pdf (describing the need to convert unstructured data formats into more structured formats to enhance interoperability).

65. *Main Page,* SEMANTICWEB.ORG, http://semanticweb.org/wiki/Main_Page (last visited Nov. 12, 2012) (emphasis omitted).

66. *See W3C Semantic Web Frequently Asked Questions,* SEMANTICWEB.ORG, http://www.w3.org/2001/sw/SW-FAQ#Manual (last visited Nov. 4, 2012) (explaining that a goal of the Semantic Web is to convert existing internet data into one common form, in this case RDF); *How Do PDF Files Work?*, NUANCE, http://www.nuance.com/imaging/resources/userGuides/pdfconverter/chapter5/ch5_6.pdf (last visited Nov. 4, 2012) ("PDF documents present their pages as images."); *see also Introduction to RDF*, W3SCHOOLS.COM, http://www.w3schools.com/rdf/rdf_intro.asp (last visited Nov. 12, 2012) (explaining that RDF/XML information can be easily exchanged between different computers running different operating systems and application languages).

67. *See The IETF Standards Process*, THE INTERNET ENG'G TASK FORCE, http://www.ietf.org/about/standards-process.html (last visited Nov. 12, 2012) ("The goals of the Internet Standards Process are: technical excellence; prior implementation and testing; clear, concise, and easily understood documentation; openness and fairness; and timeliness.").

68. Draft Regulation, *supra* note 1, art. 18(3), at 53.

69. For example, the IETF standard setting process does not include a widely adopted requirement. *See supra* note 67.

cult to measure the extent to which consumers actually use the format.[70]

3. The Amount of Data Covered by the RDP

Defining what data is covered by the RDP is vital for organizations that must comply with portability requests. An area of uncertainty in the Draft Regulation is the definition of "other information provided by the data subject" in Paragraph 2.[71]

Website controllers maintain numerous types of data on consumers. On the one end, consumers directly upload data to a web service. Examples include uploaded photos and information a user has typed into a site, such as status updates or profile information.[72] Direct uploads, where users supply the information, presumably fall within the definition of "other information."[73] On the other end, companies keep many kinds of metadata and analytics about usage of a website, some of which is aggregated to the point where there is no feasible link back to the individual user.[74] Data that is truly created by the site, for operational or analytic purposes, presumably does not fall within the definition of "other information provided by the data subject."[75]

Between the two ends lies a continuum with no natural line of demarcation. A large portion of the data on the Internet comes from a combination of the consumer and the controller's website. Face-

70. *See, e.g.*, Josh Catone, *Google Docs Use: Just a Blip*, SITEPOINT (Nov. 15, 2008), http://www.sitepoint.com/google-docs-use-just-a-blip/ (discussing how "58% of unique visitors to Google Docs and Spreadsheets in September 2008 never actually touched the applications themselves").

71. Draft Regulation, *supra* note 1, art. 18(2), at 53.

72. *See, e.g.*, *Downloading Your Information*, FACEBOOK, http://www.facebook.com/help/?page=116481065103985 (last visited Oct. 4, 2012) (discussing the different types of data consumers can already download from Facebook).

73. Draft Regulation, *supra* note 1, art. 18(2), at 53.

74. *See How to Prepare Your Organization for the Metadata Era*, VARONIS, www.varonis.com/pdfs/howtoprepare-metadata-era.pdf (last visited Nov. 12, 2012) (noting that organizations that store data often break that data in "containers" or "folders" that can contain data from dozens of users). Metadata is generally defined as data about data and is used by technology companies to manage data: "[W]e need metadata that will help us determine, for example, who it belongs to, [who] has access to it, who uses it, and what kind of content it contains." *Id.*

75. Draft Regulation, *supra* note 1, art. 18(2), at 53.

book's friend list provides an example of this middle area.[76] Users choose their Facebook friends, but Facebook may have a wide range of related data, such as current friends, close friends, acquaintances pending requests for friendship, declined friendship requests, and "defriended" friends.[77] An online game such as World of Warcraft provides another example.[78] Consumers develop individualized avatars that embark on unique quests, but such creations are done using World of Warcraft software.[79] If the avatars in the game meet the other requirements for the RDP, then it may be a complex task to determine what information was "provided by the data subject."[80] Somehow, the legal implementation of Article 18 will need to provide guidance on how to handle the nuanced issues regarding information that is provided at least in part by both the data subject and the controller, apparently for a huge number of different websites and apps.

Article 18 also fails to address how the RDP would apply in connection with intellectual property rights or claims by multiple individuals to have control over information. The RDP's requirement to export "other information" may conflict, for instance, with a license that limits the data subject from copying songs, photographs, or other content. Internet services themselves may have intellectual property and similar restrictions on what may be downloaded. Facebook, for example, restricts users from downloading any information "which is a trade secret or intellectual property of Facebook Ireland Limited or its licensors."[81] More generally, multiple individuals may have "other information" about them, such as when multiple people appear in a photograph. Allowing one user to transfer a second user's information may violate the privacy rights of the second user.[82] Controlling websites may thus find it difficult to determine what "other infor-

76. *See Lists for Friends*, FACEBOOK, http://www.facebook.com/help/friends/lists (last visited Nov. 12, 2012) (describing the way friends lists can be further subdivided by Facebook users).

77. *Id.*

78. WORLD OF WARCRAFT, http://us.battle.net/wow/en/ (last visited Oct. 22, 2012).

79. *What Is World of Warcraft?*, WORLD OF WARCRAFT, http://us.battle.net/wow/en/game/guide/ (last visited Nov. 12, 2012).

80. Draft Regulation, *supra* note 1, art. 18(2), at 53.

81. Emil Protalinsk, *Facebook: Releasing Your Personal Data Reveals Our Trade Secrets*, ZDNET (Oct. 12, 2011, 11:27 AM), http://www.zdnet.com/blog/facebook/facebook-releasing-your-personal-data-reveals-our-trade-secrets/4552.

82. Thanks to James Grimmelmann who expressed this idea to Tal Zarsky.

mation" may legally be transferred on behalf of a particular data subject.

The discussion here has presented three examples of as-yet undefined terms under Article 18: "without hindrance", "structured and commonly used format[s]", and "other information provided by the data subject."[83] Experience with Article 18 may reveal other textual challenges. As with any legal regime based on novel terms, there would appear to be a great deal of uncertainty about how the full range of software and Internet service providers are expected to comply with the RDP. Perhaps most importantly, controllers will need guidance on the scope of the new mandate for them to write the software for the Export-Import Module.[84] The Draft Regulation also contains enhanced penalties that can reach two percent of a company's global revenue.[85] The prospect of large penalties, combined with genuine uncertainty about the RDP's meaning, makes it important to scrutinize the proposed RDP carefully. The rest of this Essay will explore the problems that can arise from a broad interpretation of the RDP.

II. THE RDP AND COMPETITION LAW

A core argument for the RDP is the fear of lock-in, the idea that consumers will continue to use an inferior product because of high switching costs.[86] This Part of the Essay analyzes the RDP under E.U. competition law and U.S. antitrust law, which we refer to generally here as "competition law." The conclusion is striking: The RDP as proposed is far broader than competition law would support. The chief goal of competition law is to increase consumer welfare.[87] At least as understood in competition law, the proposed RDP is consid-

83. Draft Regulation, *supra* note 1, art. 18(1)–(2), at 53.

84. *See supra* Part I.B.1.

85. Draft Regulation, *supra* note 1, art. 79, at 92–94.

86. *See* James F. Ponsoldt & Christopher D. David, *A Comparison Between U.S. and E.U. Antitrust Treatment of Tying Claims Against Microsoft: When Should the Bundling of Computer Software Be Permitted?*, 27 NW. J. INT'L L. & BUS. 421, 448 (2007) (discussing lock-in and its effects on the software industry).

87. *See* FATUR, *supra* note 20, at 137 ("[EU competition policy] acknowledges the importance of consumer welfare."); Brooke Group Ltd. v. Brown & Williamson Tobacco Corp., 509 U.S. 209, 221 (1993) (recognizing "the antitrust laws' traditional concern for consumer welfare and price competition").

erably over-broad and appears to reduce consumer welfare.[88] Although there may be other justifications for the RDP, Article 18 as drafted is contrary to the teachings of competition law.

In competition law, a successful case would need to establish three elements: dominant market power, an exclusionary practice, and no efficiencies to offset the harms of the exclusionary practice.[89] Compared with these basic requirements of an antitrust claim, the RDP is over-broad. It applies even in the absence of market power. It does not take into consideration the substantial efficiency arguments that apply in many settings. Additionally, under European law for exclusionary practices, it would often be quite difficult to show the main types of exclusionary practices, such as a refusal to supply, denial of access to an essential facility, or a tying violation.[90]

Put another way, the RDP essentially creates a per se rule for the cases covered by the RDP—for these cases, the Draft Regulation prohibits software unless it has an EIM.[91] Current E.U. and U.S. competition law, however, applies the rule of reason to exclusionary conduct rather than a per se rule. For those not familiar with competition law, that means that enforcement is case by case, and depends on the efficiencies of the action as well as the possible harm to competition.[92] This departure from E.U. and U.S. competition law does not in itself mean that the RDP is flawed. It does mean, however, that lock-in effects and high switching costs do not justify the proposed RDP. When tested against modern understandings of competition law, the RDP as drafted goes far beyond the rules that competition law would apply to lock-in and switching costs, in ways that reduce consumer welfare.

This Part explores the differences between the RDP and current competition law. First, the RDP does not require a showing of market power and applies equally to monopolies and to small and medium

88. *See Commission Communication on Guidance on the Commission's Enforcement Priorities in Applying Article 82 of the EC Treaty to Abusive Exclusionary Conduct by Dominant Undertakings,* 2009/C 45/02, ¶¶ 86–88 [hereinafter Guidance] (recognizing that consumers may be harmed when service providers are prevented from innovating or are excluded from the market due to price constraints).

89. *Id.* ¶¶ 9–31.

90. *See id.* ¶¶ 47–62, 75–90 (discussing various anticompetitive actions and how they would be dealt with under the Draft Regulation).

91. Draft Regulation, *supra* note 1, art. 18, at 53; *see also supra* Part I.B.1.

92. *See, e.g.*, United States v. Microsoft Corp., 253 F.3d at 34, 34, 94 (D.C. Cir. 2001); FATUR, *supra* note 20, at 162.

enterprises.[93] Second, the RDP uses a per se approach that does not compare the precompetitive efficiencies against the harms to competition.[94] Third, failure to write EIM software does not fit under the traditional categories of exclusionary conduct prohibited by current competition law.[95]

A. Market Power and Effects on Small and Medium Enterprises

Competition law leads to enforcement only when market power exists: "A finding of dominance in general, and a high market share in particular, serves as an initial screen to identify market conduct which may potentially be harmful."[96] Where there is no market power, consumers and the market are not harmed by the actions of one company—the company by definition cannot exercise monopoly power.[97] In the E.U., the Commission strongly presumes that companies with less than a forty percent market share do not dominate a market, and so are exempted from competition enforcement.[98] The required showing of market power, to trigger possible enforcement, is generally even higher in the U.S.[99] In addition to high market share, substantial barriers to entry must exist for a company to possess market power.[100]

The Draft Regulation applies the RDP even in the absence of market power. Any company that meets the other criteria of standard format and electronic processing, for example, comes within the requirements of the RDP.[101] This simple fact is a major departure from competition law. Applying the RDP in the absence of market power signals that the monopoly power problems of lock-in alone do not jus-

93. *See infra* Part II.A.

94. *See infra* Part II.B.

95. *See infra* Part II.C.

96. FATUR, *supra* note 20, at 246.

97. *See id.* (discussing the effects-based approach).

98. Guidance, *supra* note 88, ¶ 14.

99. E.I. du Pont de Nemours & Co. v. Kolon Indus., Inc., 637 F.3d 435, 450-51 (4th Cir. 2011) ("Supreme Court cases, as well as cases from this court, suggest that absent special circumstances, a defendant must have a market share of at least 50 percent before he can be guilty of monopolization.").

100. United States v. Microsoft Corp., 253 F.3d 34, 54-55 (D.C. Cir. 2001).

101. Draft Regulation, *supra* note 1, art. 18, at 53.

tify the proposal as drafted.[102] By not requiring market power, the RDP imposes obligations on numerous companies without a corresponding consumer benefit.

Competition law requires market power before enforcing against even very large companies.[103] Competition agencies are even less likely to bring enforcement actions against small and medium-sized enterprises ("SMEs").[104] Yet the RDP as drafted applies to SMEs the same as it does to large software companies.[105] Mandating the RDP for SMEs, in the name of preventing lock-ins, has at least three major disadvantages. First, SMEs rarely, if ever, have market power. Second, the compliance burdens on SMEs are likely to be substantial relative to the benefits. Under the RDP as drafted, a start-up in a garage would appear to have the same responsibility to create an EIM as a large company.[106] A large company may have enough software writers and compliance lawyers on staff to build and test the EIM to meet the Article 18 requirements. SMEs are far less likely to have the resources to learn their compliance obligations and write software to meet them. The third disadvantage follows from the first two: Innovation by small software companies will be discouraged if they must write an EIM from the start and comply with the RDP.[107] The concern is that the RDP, rather than promoting consumer welfare, would deprive

102. Put another way, competition law would not find an enforceable harm in the absence of market power. *See supra* note 96 and accompanying text. A proponent of the RDP as drafted would thus need to have factual views about markets that are quite different from the views of the competition enforcement agencies. Presumably, a heavy burden should be on proponents to make the case that markets affected by the RDP are so far at variance with the competition agencies' understanding of markets. To date, proponents have not made any such case.

103. The test in both the U.S. and E.U. is market share and not market size. *Microsoft Corp.*, 253 F.3d at 54; *E.I. du Pont de Nemours*, 637 F.3d at 450-51.

104. *Cf. supra* note 98 and accompanying text (explaining that the E.U. will not presume market competition violations where a company has less than a forty percent market share).

105. Draft Regulation, *supra* note 1, at 19.

106. *See id.* (applying the Draft Regulation to "micro, small and medium-sized enterprises").

107. *Cf.* Guidance, *supra* note 88, ¶ 87 (recognizing that proposed rules and regulations may prevent companies from innovating or bringing their services to the market).

consumers of innovative products with no corresponding benefit to competition generally.[108]

B. The RDP Fails to Weigh Pro-Competitive Efficiencies Against Anti-Competitive Harms

At a common-sense level, there are significant efficiencies to letting software writers decide what functions to include in their software. The leading decision in the D.C. Circuit Court of Appeals, *United States v. Microsoft Corp.*,[109] captured this intuition that there are many valid reasons a programmer might include or exclude particular features and functions, including that "integration of new functionality into platform software is a common practice,"[110] and integration "is common among firms without market power."[111] That a practice is common among firms without market power is strong evidence that the practice has efficiencies, rather than generally being an attempt to lock-in or otherwise exercise market power.[112]

The RDP, as drafted, creates a per se rule against software that lacks an EIM.[113] The provider cannot defend itself by saying that its practices improve competition and are more efficient than they would be if it followed the RDP requirements. Competition law, by contrast, uses a rule of reason rather than a per se rule, which allows deviations where significant efficiencies exist.[114] E.U. competition law frowns on the use of a per se rule in the area of exclusionary practices, such as

108. As with other regulatory requirements, an additional concern is that established companies that become experts in the regulations will use them to their own competitive advantage. For instance, the RDP might enable a major company to complain when a smaller company is not complying with the RDP. In this way, the large player can impose regulatory burdens on smaller competitors, and also in this case perhaps require the smaller competitor to shift data to the large company. Such mandated shifts in data from smaller to larger companies can actually reinforce problems of competition in the market.

109. 253 F.3d 34 (2001).

110. *Id.* at 95.

111. *Id.* at 93.

112. *See id.* at 86–87 (reasoning that firms without market power tend to buy "bundled" goods and services, as opposed to buying those services separately, because it is more efficient, not because the bundled goods are the only option available).

113. *See supra* Part I.B.1.

114. FATUR, *supra* note 20, at 162.

an alleged lock-in.[115] Additionally, as the D.C. Circuit explained in its *Microsoft* decision, "[i]t is only after considerable experience with certain business relationships that courts classify them as per se violations."[116] Adopting a per se rule for what software is included in a product "creates undue risks of error and of deterring welfare-enhancing innovation."[117]

As discussed in this Section, a per se rule would likely create significant inefficiencies for current software providers by requiring them to create an EIM for software covered by the RDP. Creating an EIM could be costly for both SMEs and larger providers. Writing interoperable software is more challenging than it may seem.[118] A per se rule would also harm dynamic efficiency—the efficiency of the market over time.[119] The ability to attract users to a software service, and keep them there in at least some instances, is an important incentive for innovation and new entrants.[120] Additionally, and ironically, the RDP as drafted may create incentives for software providers to actually reduce their use of commonly accepted standards.

1. Static Efficiency and the Cost and Difficulty of Achieving Interoperability

The RDP mandates that covered software include an EIM by requiring that the data subject be able to get covered data "without hindrance" from the first party.[121] As many readers have likely experienced in their own lives, it is often difficult to get two software

115. *See, e.g.*, C-468/06 to C-478/06, Sot. Lelos Kai Sia EE v. GlaxoSmithKline AEVE Farmakeftikon Proionton, 2008 E.C.R. I-07139, ¶ 62 ("For both legal and economic reasons, Article 82 EC [the provision governing exclusionary practices] is not appropriate to govern conduct branded as abusive per se.").

116. *Microsoft Corp.*, 253 F.3d at 84 (alteration in original) (quoting Broad. Music, Inc. v. Columbia Broad. Sys., Inc., 441 U.S. 1, 9 (1979)).

117. *Id.* at 89–90. Tying law in the E.U., similar to U.S. law, recognizes that "serious errors can be made if such [tying] practices are condemned as anti-competitive without a thorough analysis and balancing of legitimate production purposes and anti-competitive effects." FATUR, *supra* note 20, at 162. In fact, "the Commission explicitly confirmed its intention to apply the rule of reason type of analysis to tying and bundling cases." *Id.* at 162.

118. Shah & Kesan, *supra* note 31, at 143.

119. *See infra* Part II.B.2.

120. *See infra* Part II.B.2.

121. Draft Regulation, *supra* note 1, art. 18, at 53.

programs to interoperate smoothly.[122] Interoperability is a problem for even the most sophisticated of organizations. "Even the internationally respected Mayo Clinic, which treats more than a million patients a year, has serious unresolved problems after working for years to get its three major electronic records systems to talk to one another."[123] In assessing the efficiency of the RDP, the costs of creating the EIM should be weighed against the benefits of the RDP.

The cost and difficulty of achieving interoperability is highlighted in a recent study by Professors Rajiv Shah and Jay Kesan that assessed the effects of open standard document formats on interoperability.[124] The authors examined interoperability for the OpenDocument Format ("ODF") and other alternatives to Microsoft's proprietary DOC format.[125] Their study showed "very significant issues with interoperability" between existing document formats.[126] More specifically, "[t]he best implementations may result in formatting problems, while the worst implementations actually lose information contained in pictures, footnotes, comments, tracking changes, and tables."[127]

This finding of the difficulty of interoperability suggests important lessons for interoperability and the RDP. First, the study considered an internationally recognized and widely supported open standard, ODF.[128] This sort of open standard for word processing would presumably meet Article 18's definition of an "electronic and structured format which is commonly used."[129] Thus, Shah and

122. *See* PALFREY & GASSER, INTEROP, *supra* note 61, at 21-22 (discussing a common interoperability problem between a Mac and a projector).

123. Milt Freudenheim, *The Ups and Downs of Electronic Medical Records*, N.Y. TIMES, Oct. 9, 2012, at D4.

124. *See* Shah & Kesan, *supra* note 31, at 121 (discussing how OpenDocument Format and OpenOffice.org combine to create a program that is not limited to one software vendor).

125. *Id.* at 119.

126. *Id.*

127. *Id.*

128. *See* OPENDOCUMENT FORMAT, http://opendocumentformat.org/ (last visited Nov. 12, 2012) ("OpenDocument Format (or ODF for short) is the worlds [sic] leading document standard as maintained by the Organization for the Advancement of Structured Information Standards (OASIS), and was first adopted as an international standard in 2005.").

129. Draft Regulation, *supra* note 1, art. 18(1), at 53.

Kesan's experience with ODF is relevant to the likely experience with other open standards going forward. Second, the study applied to major software products with large numbers of users.[130] Google Docs, for instance, had around four million users at the time of the study,[131] but the study found significant interoperability lapses by Google Docs.[132] Third, the study applied to software producers that had strong commercial incentives to achieve interoperability. Google Docs, for example, is a major strategic investment by a leading company trying to gain market share in the large market for word processing software.[133]

This study, in short, supports the idea that interoperability may well be costly and difficult to achieve.[134] The requirement of interoperability could impose high costs on small companies relative to the size of their market. Even for major software programs, supported by large companies with strong commercial incentives, the study found significant issues of interoperability.[135] Especially if the first party has a responsibility to make sure that interoperability works with a range of second parties, then there may be serious feasibility concerns about the extent to which the RDP can be achieved in practice. This sort of mandate goes well beyond what is required by competition law.[136] At a minimum, regulators should not assume that interoperability is easy and inexpensive to achieve.

130. Shah & Kesan, *supra* note 31, at 119 (explaining that their study of ODF interoperability included popular software programs such as Microsoft Office, Wordperfect, and Google Docs).

131. Catone, *supra* note 70.

132. Shah & Kesan, *supra* note 31, at 133–34 (finding that Google Docs had "significant problems correctly reading the test documents" in the interoperability study).

133. *See* Catone, *supra* note 70 (noting that Google Docs is trying to compete with Microsoft Word for customers).

134. *See* Shah & Kesan, *supra* note 31, at 136, 143 (failing to find 100 percent interoperability between the commonly used document formats and noting that achieving interoperability might involve costly updates and testing).

135. *Id.* at 136.

136. *See, e.g.*, Steven C. Salop, *Refusals to Deal and Price Squeezes by an Unregulated, Vertically Integrated Monopolist*, 76 ANTITRUST L.J. 709, 735 (2010) ("If the firm lacks the technical ability to supply an entrant, then the refusal to supply clearly would be permitted.").

2. *Dynamic Efficiency and a Reduced Incentive to Use Standards and to Innovate*

Along with current costs of creating an EIM, the RDP can have significant effects on dynamic efficiency and consumer welfare over time. First, the RDP creates one especially perverse incentive. The Paragraph 1 requirements about providing a copy of personal data apply only to companies that process data "in an electronic and structured format which is commonly used."[137] Based on the language of the Draft Regulation, companies can avoid the need to write an EIM if they decide *not* to use electronic and structured formats. Ironically, this measure designed to increase interoperability thus could lead companies to reduce their use of the standard formats that foster interoperability.[138] With an increase in the use of non-structured formats, the RDP may exacerbate current data lock-in problems—precisely the opposite of the intended effect.

Second, and more broadly, a major consideration in achieving consumer welfare is how to create incentives for innovation.[139] Consumers flock to new services, such as social networks, and new devices, such as smartphones. A principal task of antitrust law for the information and communications technology ("ICT") sector is how to foster continued innovation.[140]

Proponents of the RDP and of interoperability generally make the case that greater interoperability will lead to more innovation.[141] The idea is that there will be less lock-in, and the second players will be able to offer new products and services once portability increases and switching costs are reduced: "One of the reasons why we tend to like interoperability is that we believe it leads to innovation, as well as other positive things like consumer choice, ease of use, and competition."[142]

This sort of increased innovation by second players can certainly occur. Mandated interoperability, however, can also reduce innova-

137. Draft Regulation, *supra* note 1, art. 18(1), at 53.

138. Thanks to Howard Beales for suggesting this point.

139. *See* FATUR, *supra* note 20, at 178 ("[T]he core issue with regard to imposing a duty to deal is balancing short-run gains in efficiency with long-run incentives to invest and compete dynamically, which should be done on a case-by-case basis.").

140. *Id.*

141. *See, e.g.*, PALFREY & GASSER, INTEROP, *supra* note 61, at 11–12.

142. Gasser & Palfrey, *Breaking Down*, *supra* note 61, at ii.

tion.[143] In addition to the cost of writing an EIM, there will be lower expected returns to a new entrant whose business plan is based at least in part on not fully sharing the data provided by the consumer.[144] This sort of potential first player will have lower expected profits if there is lower consumer stickiness to their platform.

Resolving this tradeoff between innovation by first players and second players is a complex task.[145] Our main point here is that this complexity supports a rule of reason approach, based on the characteristics of a particular market, rather than the per se approach of the RDP. Although market structures vary considerably, important aspects of ICT industries suggest that a rule that mandates interoperability will often reduce innovation.[146] In general, a major theme of innovation theory is the Schumpeterian idea of creative destruction.[147] Dynamic competition in the technology space has resulted in "successive waves of creative destruction."[148] For example, MySpace replaced Friendster as the dominant social network, only for Facebook to later usurp MySpace's position as the market leader.[149]

143. *See* FATUR, *supra* note 20, at 81 ("The right to exclude ensures that successful innovators can recover their sunk costs and receive a return that compensates them for the risk.").

144. *Id.*

145. The debate about interoperability is structurally similar to longstanding debates in the intellectual property area. Owners of patents and copyrights argue that they need strong intellectual property rights in order to create incentives for the first players, who are the owners of such rights. Yochai Benkler, Brett Frischmann, and other scholars emphasize the importance of the second players, who make fair use of copyrights or otherwise innovate based on narrower property rights. *See generally* YOCHAI BENKLER, THE WEALTH OF NETWORKS (2006); BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES (2012). We do not take sides in this general debate about the scope of intellectual property rights; instead, the point here is that there are complex, situation-dependent considerations about what is likely to create optimal overall innovation, considering effects on both first players and second players. Copyright and other intellectual property law is very complex—we should not expect a simple rule of mandated interoperability to best cover the full range of market structures.

146. FATUR, *supra* note 20, at 81.

147. *Id.* at 72; *see also* Spencer Weber Waller, *Antitrust and Social Networking*, 90 N.C. L. REV. 1771, 1800 (2012) (explaining that Schumpeterian competition consists of "one dominant firm being replaced by another, and then yet another dominant firm").

148. Waller, *supra* note 147, at 1801.

149. *Id.*

Many technology markets have the basic feature that one player gets a lead and then becomes a market leader, often with a large market share.[150] Economists have at least three related names for this phenomenon: first-mover advantage (an early entrant can gain significant market share),[151] network effects (where the usefulness of a product to one user increases as the number of other users increases),[152] and tipping effect (where one seller gets enough of a lead on competitors that the market *tips* to a very large market share).[153] Paul Geroski has described the phenomenon of competition *for* the market, rather than the traditional competition *in* a market.[154] He writes: "[I]nnovative entry involves producing new products or services, and, for this reason it usually also involves a different business design."[155] Such entry is costly and risky.[156] If there is a rule, such as the RDP, that reduces the profitability of such entry, then we can expect a lower amount of innovation in those new business designs.

Competition law encourages technical innovation that creates dynamic efficiency.[157] As Judge Learned Hand explained, "[t]he successful competitor, having been urged to compete, must not be turned upon when he wins."[158] As discussed in more detail below, competition law compensates successful innovators for the development risk by generally giving them the right to exclude competitors from their assets.[159] A per se mandate of the RDP cuts against this basic principle of competition law, and will tend to reduce innovation where there is competition *for* the market.

Depending on the breadth of the RDP, Article 18 can specifically reduce investment by first parties in innovative data products. One example of an innovative first party is Angie's List, which since 1996 has compiled reliable reviews about service providers ranging from

150. FATUR, *supra* note 20, at 85–86.

151. Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CALIF. L. REV. 479, 495 (1998).

152. *Id.* at 483.

153. *Id.* at 505.

154. P.A. Geroski, *Competition in Markets and Competition for Markets*, 3 J. INDUS., COMPETITION, & TRADE 151, 162 (2003).

155. *Id.* at 163.

156. *Id.*

157. *See supra* note 142 and accompanying text.

158. United States v. Aluminum Co. of Am., 148 F.2d 416, 430 (2d Cir. 1945).

159. *See* FATUR, *supra* note 20, at 81.

plumbers to doctors.[160] Angie's List, unlike its competitors, ensures trusted reviews by not accepting anonymous reviews and only counting reviews from active members.[161] If a second player can force companies such as Angie's List to transfer valuable customer data "without hindrance," then there is a reduced incentive to innovate and compile unique data. Under the RDP as currently drafted, future companies like Angie's List that benefit millions of consumers may never get started.

There are thus plausible precompetitive justifications, including incentives for innovations, for services that do not provide an EIM. The D.C. Circuit feared that "per se rules might stunt valuable innovation" by "not giv[ing] newly integrated products a fair shake."[162] Under the rule of reason approach, companies can prove that efficiency justifications outweigh competitive harm caused by restricting data transfers.[163] Under the per se approach of RDP, companies may decide not to engage in risky investments in innovation because of lower expected returns.

C. Failure to Write an EIM Is Generally Not Exclusionary Conduct Under Competition Law

In the discussion of competition law thus far, we have started with points that we thought would be intuitive to readers whose main field is not antitrust—market power is needed before competition law intervenes, and there are likely important static and dynamic efficiencies to allowing software companies to decide what functions to include in their products and services. We now turn to the somewhat more technical discussion of when competition law will find exclusionary conduct—the sort of action to exclude a competitor, such as a second party seeking to use data, that will trigger scrutiny under competition law.

The alleged exclusionary act at issue is lack of interoperability, or failure to write an EIM. Competition law could characterize, or describe, the decision of a software company not to write an EIM in at least three related ways. First, and most appropriately, the decision not to write an EIM might be described as what E.U. law calls "refusal

160. ANGIE'S LIST, http://www.angieslist.com/ (last accessed Oct. 4, 2012). One author, Lagos, has worked for Angie's List.

161. *Id.*

162. United States v. Microsoft Corp., 253 F.3d 34, 89, 92 (D.C. Cir. 2001).

163. *Id.* at 92.

to supply" and U.S. antitrust law usually calls "refusal to deal."[164] Second, the decision of the first party might violate the essential facilities doctrine, which is a type of refusal to supply.[165] Third, the decision of the first party might be considered an anticompetitive tying arrangement, on the theory that the software service is foreclosing competition by tying its offering with a non-interoperable software module.[166]

Our view is that failure to supply an EIM would typically comply with competition law under any of these theories. Competition law starts with a presumption that companies have freedom to decide with whom they will deal.[167] In a 2004 case, *Verizon Communications Inc. v. Law Offices of Curtis V. Trinko*,[168] the Supreme Court of the United States discussed "the few existing exceptions from the proposition that there is no duty to aid competitors."[169] E.U. courts similarly require a showing of exceptional circumstances when examining a refusal to supply. In addition to holding a dominant position in the primary market, the European Commission has announced three enforcement priorities for a refusal to supply claim: "the refusal relates to a product or service that is objectively necessary to be able to compete effectively on a downstream market, the refusal is likely to lead to the elimination of effective competition on the downstream market, and the refusal is likely to lead to consumer harm."[170] In its 2007 decision, *Microsoft v. Commission*,[171] the E.U. Court of First Instance stated that three conditions are needed to meet the "exceptional" requirements for proving a refusal to supply:

> [I]n the first place, the refusal relates to a product or service indispensable to the exercise of a particular activity on a

164. *See* Guidance, *supra* note 88, ¶ 75–90, at 18; Verizon Commc'ns, Inc. v. Law Offices of Curtis V. Trinko, 540 U.S. 398, 408–09 (2004).

165. *Trinko*, 540 U.S at 410.

166. *See* Guidance, *supra* note 88, ¶¶ 47–62, at 15–16.

167. In U.S. antitrust law, this presumption derives from the oft-cited Supreme Court statement in *United States v. Colgate & Co.*, where the Court stated: "In the absence of any purpose to create or maintain a monopoly, the [Sherman] act does not restrict the long recognized right of trader or manufacturer engaged in an entirely private business, freely to exercise his own independent discretion as to parties with whom he will deal." 250 U.S. 300, 307 (1919).

168. 540 U.S. 398 (2004).

169. *Id.* at 411.

170. Guidance, *supra* note 88, ¶ 81, at 18–19.

171. Case T-201/04, Microsoft v. Comm'n, 2007 E.C.R. II-3619.

> neighbouring market; in the second place, the refusal is of such a kind as to exclude any effective competition on that neighbouring market; in the third place, the refusal prevents the appearance of a new product for which there is potential consumer demand.[172]

The threshold for showing a refusal to supply is thus clearly much higher than for finding a violation under Article 18. For instance, refusal to supply applies only to something "indispensable" to a neighboring market, and the refusal must "exclude any effective competition" for that other market.[173] The Commission also expects to enforce the Regulation only where the refusal leads to consumer harm, and the analysis here has shown multiple respects where the RDP is instead likely to create consumer harm as understood in competition law.[174]

The concept of essential facilities is closely related to the idea of refusal to supply.[175] This idea of essential facilities might seem like a good fit with the RDP: The data subject and the second party might need access to the data held by the first party to bring competition to markets that rely on that data. The essential facilities doctrine, however, has experienced serious criticism from scholars and the United States Supreme Court.[176] Even advocates for the essential facilities doctrine, moreover, would apply it in far more restrictive circumstances than contemplated by the RDP. For instance, former FTC Chairman Robert Pitofsky has written in support of the doctrine, in connection with a 2002 E.U. competition case.[177] He writes:

> [T]o establish antitrust liability under the essential facilities doctrine, a party must prove four factors: (1) control of the essential facility by a monopolist; (2) a competitor's inability

---

172. *Id.* ¶ 332, at 3726.

173. *Id.*

174. *See supra* Part II.A–B.

175. Mats A. Bergman, *The Role of the Essential Facilities Doctrine*, 46 ANTITRUST BULL. 403, 413 (2001).

176. *See, e.g.*, Robert Pitofsky et al., *The Essential Facilities Doctrine Under U.S. Antitrust Law*, 70 ANTITRUST L.J. 443, 443-47 (2002) (describing the controversies related to right of access to an essential facility controlled by a monopolist and referencing Supreme Court decisions applying the essential facilities doctrine).

177. Robert Pitofsky, *The Essential Facilities Doctrine Under U.S. Antitrust Law* (submitted to the European Commission), *available at* http://www.ftc.gov/os/comments/intelpropertycomments/pitofskyrobert.pdf (last modified June 20, 2007).

practically or reasonably to duplicate the essential facility;
(3) the denial of the use of the facility to a competitor; and
(4) the feasibility of providing the facility to competitors.[178]

These factors are much stricter than Article 18. The factors require a finding of monopoly, and there must be a "denial of the use of the facility," which is a greater degree of exclusionary conduct than simply a failure to write an EIM.[179] Furthermore, the owner of the facility has the opportunity to dispute whether the access is feasible,[180] the sort of efficiencies argument that is applied under a rule of reason. Similarly, scholars such as Brett Frischmann and Spencer Waller, who write in favor of open access principles and the essential facilities doctrine, would require a high threshold before applying the doctrine.[181]

Along with refusal to supply or essential facilities, one might characterize the RDP as preventing a tying arrangement. One might believe that the first party is tying its product, such as a social network, to a tied product, the software that governs export of data. The analogy is not precise—generally there is no separate product for an EIM. The idea of a tie, however, may be useful in suggesting that there could be an obligation of the first party to tie its product to an EIM that provides portability rather than to an EIM that lacks portability.

As with the other alleged exclusionary conduct, however, Article 18 is much stricter than the conclusions about tying that competition law has arrived at after years of analysis and case law. In finding that Microsoft had in fact illegally tied Windows Media Player with the Windows operating system, the E.U. Court of First Instance set forth the factors needed to prove a tying violation.[182] The court first required that the tying and tied products be two separate products,[183] which is not the case with a software service and its EIM. Second, the

178. *Id.* at 5-6; *see also* MCI Commc'ns Corp. v. Am. Tel. & Tel. Co., 708 F.2d 1082, 1132–33 (7th Cir. 1983) (listing the same four factors).

179. *MCI Commc'ns*, 708 F.2d at 1132–33.

180. Pitofsky, *supra* note 177, at 6–8.

181. Brett Frischmann & Spencer Weber Waller, *Revitalizing Essential Facilities*, 75 ANTITRUST L.J. 1, 19 (2008) ("We see an important but limited role for the essential facilities doctrine in antitrust law with respect to infrastructure.").

182. Case T-201/04, Microsoft v. Comm'n, 2007 E.C.R. II-3619, ¶ 842, at 3876; *see also* Ponsoldt & David, *supra* note 86, at 443, 446 (reiterating the four factors and the holding in the case).

183. Case T-201/04, Microsoft v. Comm'n, 2007 E.C.R. II-3619, ¶ 842, at 3876.

court analyzed whether "the undertaking concerned is dominant in the market for the tying product."[184] Once again, competition law only steps in to protect consumer welfare where there is dominant market power, in contrast to Article 18. Third, the court analyzed whether "the undertaking concerned does not give customers a choice to obtain the tying product without the tied product."[185] Although a first party may not create an EIM that operates "without hindrance," customers retain the legal and often practical ability to export their data to a different online service. Fourth, the court analyzed whether "the practice in question forecloses competition."[186] This factor allows a court to consider the dynamic effects on the market; as discussed in Part II.B.2, these dynamic factors may well favor less of an RDP than Article 18 provides. In addition, the court analyzed Microsoft's proposed objective justification for its product decision: the possibility that its conduct had efficiencies or was justified by reasons other than an intent to dominate the market.[187] The Court did not find such an objective justification in the facts of that case.[188] Under the different facts of the leading *Microsoft* decision in the United States, the D.C. Circuit eloquently discussed the reasons to give software providers flexibility in deciding what features and functions to include in a product: "[I]ntegration of new functionality into platform software is a common practice," and integration "is common among firms without market power."[189]

In conclusion on competition law, exclusionary practices trigger enforcement only where there is a particularized showing in a specific market of harm to consumers.[190] Competition law acts only where there is strong market power, and efficiencies and other justifications can be given to justify behavior that otherwise may appear exclusionary.[191] This accumulated wisdom and experience in competition law,

184. *Id.*

185. *Id.*

186. *Id.*

187. Case T-201/04, Microsoft v. Comm'n, 2007 E.C.R. II–3619, ¶¶ 1144–47, at 3963–64.

188. *Id.* ¶¶ 1155–58, at 3966–67.

189. United States v. Microsoft Corp., 253 F.3d 34, 93, 95 (D.C. Cir. 2001).

190. *See* Guidance, *supra* note 88, ¶ 19, at 9 (listing "[f]oreclosure leading to consumer harm" as one of the general elements of a violation of Article 82, which prohibits abuses of a dominant market position).

191. *Id.* ¶¶ 9–18, 28–31, at 8–12.

designed to address lock-in effects and high switching costs, is different in numerous respects from the Draft Regulation's text for Article 18. It thus appears difficult to justify the current text on the basis of lock-in or other competition law concerns.

III. THE RDP AND PROTECTION OF FUNDAMENTAL PRIVACY RIGHTS

The previous Part concluded that the proposed RDP is not a good fit with E.U. and U.S. competition law. Another major rationale for the RDP is that it protects individual rights in data protection. Among the brief mentions of the RDP in the Draft Regulation, the following is most on point: "As a precondition and in order to further improve access of individuals to their personal data, [the RDP] provides the right to obtain from the controller those data in a structured and commonly used electronic format."[192]

This part of the Essay critically evaluates the proposal to recognize a new right to obtain personal data in a structured and commonly used electronic format. In considering the claimed individual right, we repeat our statement from the Introduction that the idea of data portability is appealing.[193] We hope that it will be implemented as good practice in a range of settings, and we note that major online services have improved data portability over time.[194] The discussion here, however, is how to assess a claimed right of data portability, as implemented in laws such as the proposed Article 18.

In assessing this claim, we briefly examine the extent to which the RDP should qualify as a "human right" or "fundamental right" in the context of global human rights jurisprudence generally and E.U. law more specifically.[195] Whatever sort of right may be implicated, the process for defining the RDP appears to essentially be normal legislation and regulation rather than constitutional deliberation.[196] The definition of the RDP should be based on democratic policy-making rather than rights jurisprudence. Next, the discussion shows how the RDP differs substantially from the pre-existing E.U. right of access, in ways that make the former more than a routine variation on the lat-

192. Draft Regulation, *supra* note 1, at 9; *see also* Zanfir, *supra* note 13, at 151 (stating that restricting data flow is a violation of human rights).

193. *See supra* note 6 and accompanying text.

194. *See supra* note 5.

195. *See infra* Part III.A.

196. *See infra* Part III.A.

ter.[197] Finally, the proposed right raises serious risks for another principle of data protection law: protecting the security of an individual's personal data. In our world of weak authentication and rampant identity theft, moving all of a person's data to another system "without hindrance" creates security risks that can outweigh the portability benefits.[198]

A. The RDP's Uncertain Status Under Human Rights and Fundamental Rights Jurisprudence

To determine whether the RDP is justified on the basis of individual rights, it is helpful to clarify the meaning of "fundamental rights" within E.U. law, as contrasted with human rights jurisprudence more generally, or constitutional rights as understood in the United States. At least for U.S.-trained lawyers, such as the authors, the process for defining a new "fundamental" right in the E.U. appears much closer to standard legislation and regulation than it is to a new constitutional provision.

It is well beyond the scope of this Essay to provide a full discussion of how to identify a new human right. Drawing on the work of noted moral philosopher Joseph Raz, however, there are reasons to be cautious in concluding that the RDP should qualify. In two recent articles, Raz critiques the practice of multiplying the number of human rights.[199] He states: "An ever growing number of rights are claimed to be human rights" and lists numerous examples, such as a right to globalization, the right to comprehensive sexual education, and a right to a secure, healthy, and ecologically sound environment.[200] The range of the newly claimed rights should encourage caution before accepting each newly asserted right. Raz notes that "philosophers tend to take it for granted that human rights are important rights."[201] He also emphasizes that a key function of human

197. *See infra* Part III.B.

198. *See infra* Part III.C.

199. Joseph Raz, *Human Rights Without Foundations* (Univ. of Oxford Faculty of Law Legal Studies Research Paper Series, Working Paper No. 14/2007) [hereinafter Raz, *Without Foundations*], *available at* http://ssrn.com/abstract=999874; Joseph Raz, *Human Rights in the Emerging World Order*, 1 TRANSNAT'L LEGAL THEORY 31 (2010) [hereinafter Raz, *Emerging World Order*].

200. Joseph Raz, *Without Foundations*, *supra* note 199, at 2; *see also* Joseph Raz, *Emerging World Order*, *supra* note 200.

201. *Id.* at 3.

rights is to define conditions that are so serious that violations justify international intervention.[202] Compared to protection against genocide or other rights that justify international intervention, a right to portability in data does not seem to be at the same level of importance.

Instead of this sort of human right, however, the Draft Regulation contemplates that the RDP would be a "fundamental" right, as part of the well-developed jurisprudence in the E.U. about fundamental rights in the area of data protection.[203] In the European Convention on Human Rights ("ECHR"), issued in 1950, Article 8 established the right for respect of "private and family life."[204] Courts have understood Article 8 to include the protection of personal data.[205] The Treaty of the European Union ("TEU"), which became effective in 1993, states: "Fundamental rights, as guaranteed by the [ECHR] and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law."[206] The Treaty on the Functioning of the European Union ("TFEU"), which supplements the TEU, provides: "Everyone has the right to the

202. *Id.* at 9–10.

203. *See, e.g.*, Draft Regulation, *supra* note 1, at 1, (discussing the E.U.'s dual goals of protecting the fundamental right to data protection and guaranteeing the free flow of personal data between Member States); *see also Commission Staff Working Paper for Impact Assessment*, at 29 SEC (2012) 72 final (Jan. 25, 2012). The paper states:

> In today's digitised society, communication and interaction rely on digital media and communications channels. Web 2.0 tools, including social media, play an increasingly important role for social interaction and exchange. Not being able to use these media effectively restricts the exercise of fundamental rights in the social reality."

Id.

204. European Convention on Human Rights as amended by Protocols Nos. 11 and 14, 5 C.E.T.S. 1, 10–11 (2002), *available at* http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/CONVENTION_ENG_WEB.pdf. Specifically, the ECHR states that "[e]veryone has the right to respect for his private and family life, his home and his correspondence." *Id.*

205. *See, e.g.*, S. & Marper v. United Kingdom, 2008 Eur. Ct. H.R. 1, 29 ("The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention.").

206. Consolidated Version of the Treaty on the Functioning of the European Union art. 6, May 9, 2008, 2008 O.J. (C 115) 19 [hereinafter TFEU].

protection of personal data concerning them."[207] These provided the basis for the Data Protection Directive of 1995,[208] and for the Draft Regulation proposed in 2012.[209]

Compared with the U.S. procedures for creating a new constitutional right, which requires amending the Constitution, the E.U. procedures for defining data protection rights are substantially closer to ordinary legislation and regulation. Under U.S. law, an amendment to the Constitution requires a strict super-majority process, typically with two-thirds of the Senate and House of Representatives and then ratification by three-quarters of the states.[210] By contrast, the right to protection of personal data under Article 16 of the TFEU is defined and subject to modification by the "European Parliament and the Council, acting in accordance with the ordinary legislative procedure" of the E.U.[211] The Draft Regulation states that it is based on Article 16 of the TFEU,[212] and thus proceeds under ordinary legislative procedure. In addition, Paragraph 3 of Article 18 of the Draft Regulation delegates a large portion of the details of defining the RDP to the Commission.[213]

The discussion here shows that the procedure for defining a new "fundamental" right within the E.U. is different from defining a new human right that justifies international intervention, or a new constitutional right in the U.S., which requires a difficult-to-enact super-majority vote.[214] The existence and scope of the RDP is defined by

207. TFEU, *supra* note 206, art. 16, at 55. In addition, the E.U. ratified the Treaty of Lisbon in 2009; with that ratification, the E.U. Charter of Fundamental Rights of 2000 shifted from having persuasive authority to having binding authority on the Member States. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, *Declarations Concerning Provisions of the Treaties*, Dec. 13, 2007, 2007 O.J. (C 306) 249.

208. *See supra* note 17.

209. *See supra* note 1.

210. U.S. CONST. art. V, § 5.

211. TFEU, *supra* note 206, art. 16, at 55.

212. Draft Regulation, *supra* note 1, Explanatory Memorandum § 3.1, at 5.

213. Draft Regulation, *supra* note 1, art. 18(3), at 53. For U.S. trained lawyers, this delegation to the Commission may appear to resemble regulation, covered by the Administrative Procedure Act, rather than to legislation requiring concurrence of the legislature and the executive.

214. *See supra* notes 202 and 210 and accompanying text.

"the ordinary legislative procedure."[215] There are vital issues of human dignity and freedom involved in defining fundamental rights, but there is no pre-existing constitution or other text that inevitably dictates how fundamental rights will be shaped in the regulatory process.[216] The definition of a new right in the area of data portability is legitimately open to factual and policy debates that inform "the ordinary legislative procedure."[217] Efforts to understand the new proposed RDP, and critique it where necessary, should be addressed on the merits, and not by a simple assertion that fundamental rights are involved and so discussion is at an end.

B. The RDP Goes Well Beyond the Existing E.U. Right of Access

European legal instruments such as the Data Protection Directive issued in 1995 provide individuals a right to access their personal data.[218] The access right in that directive included "communication to [the individual] in an intelligible form of the data undergoing processing."[219] The Draft Regulation says that the RDP is included "[a]s a precondition and in order to further improve access of individuals to their personal data."[220] Our view, however, is that the new requirements in Article 18 are not a precondition for the access right and in fact go quite far beyond existing access requirements.

---

215. Draft Regulation, *supra* note 1, at 17.

216. The "how" behind protecting fundamental rights is an open question, as the ECHR has grappled with shaping these rights through judicial means. *See, e.g.*, Copland v. United Kingdom, 2007-I Eur. Ct. H.R. 1, 9 (finding that the fundamental right of privacy extends to data collection in the workplace (for example, an employee's Internet usage)); K.U. v. Finland, 2008 Eur. Ct. H.R. 1, 10-11 (attempting to balance the fundamental right to privacy of one data subject (an anonymous person posting an advertisement online) against the same right of another data subject (the person whose privacy was violated by the anonymous poster)); *see also Research Div. of the Eur. Court of Human Rights Report on Internet: Case-Law of the European Court of Human Rights*, at 5–10, (2011), *available at* http://www.echr.coe.int/NR/rdonlyres/E3B11782-7E42-418B-AC04-A29BEDC0400F/0/RAPPORT_RECHERCHE_Internet_Freedom_Expression_EN.pdf (discussing case-law of the European Court of Human Rights regarding different data-protection and retention issues relevant for the Internet).

217. Draft Regulation, *supra* note 1, at 17.

218. Council Directive 95/46/EC, *supra* note 17, art. 12, at 42.

219. *Id.*

220. Draft Regulation, *supra* note 1, § 3.4.3.3, at 9.

As discussed above, Paragraph 1 of Article 18 in many cases provides the right to obtain data "in an electronic and structured format which is commonly used and allows for further use by the data subject."[221] Note that the old access requirement of communication "in an intelligible form"[222] expands to a requirement under the RDP that the format be electronic and structured, and allow for further use by the data subject.[223] Paragraph 2 further requires information in an automated processing system to be provided "in an electronic format which is commonly used, without hindrance" from the entity operating the system.[224]

The RDP differs in at least two important ways from the previous right of access. First, data protection regulators have previously stated that controllers could work with the data subject to narrow an access request.[225] For instance, in response to a request that an individual get all data about herself, the controller could speak with the individual to determine what specific information the individual was seeking.[226] This ability to define the scope of a request is considerably less burdensome on the controller than the requirement to provide all of an individual's personal data through an automated process, and to do so "without hindrance."[227] Second, data protection regulators have previously made clear that the right of access did not require the controller to create a computer system in advance to give automatic responses to access requests.[228] By contrast, the RDP appears to require

221. Draft Regulation, *supra* note 1, art. 18(1), at 53.

222. Council Directive 95/46/EC, *supra* note 17, art. 12, at 42.

223. Draft Regulation, *supra* note 1, art. 18(1), at 53.

224. *Id.* art. 18(2), at 53.

225. *Data Protection Good Practice Note: Checklist for Handling Requests for Personal Information (Subject Access Requests)*, INFO. COMM'R'S OFFICE (2007), http://www.ico.gov.uk/for_organisations/data_protection/subject_access_requests.aspx.

226. *Cf. id.* (explaining that organizations can and should provide all information requested that they hold under the ordinary course of business, but that they can also speak to the requester to clarify her request).

227. Draft Regulation, *supra* note 1, art. 18(2), at 53.

228. *See Subject Access Requests: How Do I Respond?*, INFO. COMM'R'S OFFICE, http://www.ico.gov.uk/for_organisations/data_protection/subject_access_requests.aspx (last visited Nov. 14, 2012) (explaining that data controllers have up to forty days to respond to a request). Data Protection Act, ch. 29, pt. II, §§ 7(8), 7(10) (1998) (stating that "a data controller shall comply with a request under this section promptly and in any event

creation of the EIM in advance, so that data can automatically be exported from a system the controller must build for that purpose.[229]

Not only are the requirements of the RDP different from those for the right of access, but the Draft Regulation itself provides support for the idea that the RDP is a new right that is distinct from, and goes beyond, the right of access. At a formal level, Section 2 of the Draft Regulation is entitled "Information and Access to Data,"[230] and contains Article 15, entitled "Right of access for the data subject."[231] Separately, Section 3 is entitled "Rectification and Erasure,"[232] and Article 18 the "Right to data portability."[233] The fact that the RDP is in a different section of the Draft Regulation and has a different name is evidence that the RDP is not merely a small modification to the existing right to access.[234]

The way the term "data portability" is used in other contexts further shows the gap between data portability and the E.U. definition of the right of access. Notably, the Data Portability Project was created

---

before the end of the prescribed period beginning with the relevant day" and "the prescribed period" means forty days or such other period as may be prescribed").

229. *See supra* note 121 and accompanying text.

230. Draft Regulation, *supra* note 1, art. 2, at 48.

231. *Id.* art. 15, at 50–51.

232. *Id.* § 3, at 51.

233. *Id.* art. 18, at 53.

234. Moreover, publicity materials produced by the E.U. delineate between mere access and data portability. *See Fact Sheet: Why Do We Need an EU Data Protection Reform?*, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf (last visited Nov. 14, 2012) (explaining that the proposed regulation will provide "[e]asier access to one's own data and the right of data portability, that is, easier transfer of personal data from one service provider to another"). The European Commission also released a fact sheet on how data protection reform strengthens citizens' rights. *Fact Sheet: How Does the Data Protection Reform Strengthen Citizens' Rights?*, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf (last visited Nov. 14, 2012). According to the fact sheet:

> The Commission also wants to guarantee free and easy access to your personal data, making it easier for you to see what personal information is held about you by companies and public authorities, and make it easier for you to transfer your personal data between service providers—the so-called principle of "data portability."

Id.

in 2007,[235] and incorporated in the U.S. as a non-profit in 2009.[236] A major effort of the project has been a series of ten model questions issued in 2010 "that sites can answer to explain how people can bring data in and take it out."[237] The questions promote transparency, so that an organization can clearly communicate its policies and practices to the public.[238] The ten questions cover a diverse set of issues, including the creation of a new identity on the site, the ability to import data to the site, and whether there is automatic updating for actions taken on other sites.[239]

Two aspects of the project's model questions are relevant to our comparison of the right of access and the meaning of data portability. First, the project clearly states that it does not believe there are correct answers to the questions, and that the model questions promote transparency rather than dictate practices.[240] Second, quite a few of the questions, such as the identity and updating questions just noted, address issues other than those covered by the longstanding E.U. definition of the right of access.[241]

The meaning of any right to data portability is still in the early stages of development, and the ten questions asked by the Data Portability Project differ substantially from the E.U. right of access. In short, the RDP is substantially different from the pre-existing right of access in E.U. law. If the RDP is included within E.U. law as a fundamental right, it should be recognized as a distinct and new right.[242]

---

235. Elias Bizannes, *History of the Project*, DATAPORTABILITY PROJECT (Mar. 21, 2009), http://wiki.dataportability.org/display/dpmain/History+of+the+Project;jsessionid=6FCCA7230CE8C7011A88D7824DCC3B8E.

236. Elias Bizannes, *So What Has the DataPortability Project Been Doing?*, DATAPORTABILITY PROJECT (Mar. 30, 2009), http://blog.dataportability.org/2009/03/30/so-what-has-the-dataportability-project-been-doing/.

237. Elias Bizannes, *Why Every Site Should Have a Data Portability Policy*, TECHCRUNCH (June 23, 2010), http://techcrunch.com/2010/06/23/data-portability-policy/.

238. *Id.*

239. *Id.*

240. *Id.*

241. *Id.*; *see also supra* notes 218–219 and accompanying text; Data Protection Act, ch. 29, pt. II, § 7 (1998) (defining the "Right of access to Personal Data").

242. One additional issue in defining the RDP is how to address the substantial number of exceptions under E.U. law to the right of access. *See, e.g.*, *Helping U.S. Companies Export*, INT'L TRADE ADMIN., http://export.gov/safeharbor/eu/eg_main_018380.asp (last visited Nov. 14, 2012) (outlining the various exceptions for right to access). Where access re-

The new right to data portability appears more closely akin to the personal data ownership theory—"attaching property rights to personal information."[243] The ability to transfer information "without hindrance" gives users ownership over their information. The idea that personal information is property has been widely debated,[244] with some questioning whether personal data ownership has "compatibility with the European Legal System."[245] "So far, personal information has not been deemed 'property' . . . in the EU."[246]

We do not take a position for or against the personal data ownership theory or the right to data portability as a fundamental right. Instead, we simply point out that the lack of consensus suggests that the norms for data portability have not been established.[247] It is risky to create a new fundamental right before there is general agreement of the norms defining that right.

C. The RDP Is in Tension with an Individual's Right of Data Security

Within the framework of the E.U.'s existing fundamental right to data protection, a new right to data portability is in significant tension with the individual's existing right to data security.[248] With the RDP, one-time access to a site, such as by a hacker, can turn into a lifetime's download of data from that site. Defining the RDP, therefore, should be done with full awareness of risks to the right to data security. Un-

---

quests are made one at a time, and the controller can speak with the data subject to define the request, then the controller can apply the exceptions where appropriate. *Cf. supra* notes 225–226 and accompanying text (explaining how a request for information could be narrowed). By contrast, it may take a considerable amount of regulatory definition and software effort to build each access exception into a new RDP, so that a person's records are exported "without hindrance." Draft Regulation, *supra* note 1, art. 18(2), at 53.

243. David Krebs, *Regulating the Cloud: A Comparative Analysis of the Current and Proposed Privacy Frameworks in Canada and the European Union*, 10 CAN. J.L. & TECH. 29, 38. Thanks to Bartosz Marcinkowski for suggesting this similarity to the authors.

244. *Id.*

245. Nadezda Purtova, *Property in Personal Data: A European Perspective on the Instrumentalist Theory of Propertisation*, 2 EUR. J. LEGAL STUD. 3, *3 (2010), *available at* http://www.ejls.eu/6/84UK.pdf.

246. Krebs, *supra* note 243, at 38.

247. *Id.*

248. Security of processing data is guaranteed by Article 17 of the 1995 Data Protection Directive, and Article 30 of the 2012 Draft Regulation. Council Directive 95/46/EC, *supra* note 17, art. 17, at 43; Draft Regulation, *supra* note 1, art. 30, at 60.

fortunately, Article 18 as drafted makes no mention of the right to data security.

Security has long been recognized as an important issue when defining the ability of an individual to access data.[249] The Federal Trade Commission ("FTC") in 1999 formed an advisory committee on Access and Security.[250] The committee report recognized that "there is a very real tension between access and security."[251] Notably, "privacy is lost if a security failure results in access being granted to the wrong person—an investigator making a pretext call, a con man engaged in identity theft, or, in some instances, one family member in conflict with another."[252]

Security is a materially bigger risk with the RDP. Before, access was often one-off, with the individual asking for particular information and receiving a limited amount of data.[253] With the RDP, an individual's lifetime of data with a service can be downloaded all at once.[254] The quantity of personal data at risk is therefore far greater. The affirmative requirement to create an EIM also means that the downloading is automated rather than the one-at-a-time responses to access requests that have been the norm to date.[255] The Article 18 requirement of downloading data "without hindrance" adds an additional layer of risk.[256] This language could be interpreted to prohibit a site from double-checking a user's identity if the request comes from a new IP address or otherwise appears to present a higher risk of identity fraud.[257]

---

249. *See* FINAL REPORT OF THE FEDERAL TRADE COMMISSION ADVISORY COMMITTEE ON ONLINE ACCESS AND SECURITY 19–25 (May 15, 2000) [hereinafter FEDERAL TRADE COMMISSION REPORT], *available at* http://www.ftc.gov/acoas/papers/finalreport.htm (discussing security of personal data held by web pages).

250. *Id.* at 3.

251. *Id.* at 14.

252. *Id.*

253. *See Data Protection Good Practice Note, supra* note 225 (providing examples of one-time data requests, such as requests for a product serial number).

254. *See* Draft Regulation, *supra* note 1, art. 18(1), at 53 (granting the user the right to a copy of all the data held by a controller).

255. *See supra* notes 121 and 228 and accompanying text.

256. Draft Regulation, *supra* note 1, art. 18(2), at 53.

257. *Cf. Data Protection Good Practice Note, supra* note 225 (noting that an organization can provide the information requested when it is sure of the requester's identity).

Double-checking a user's identity, however, is often appropriate before releasing large amounts of what may be sensitive data. For online banking transactions, the Federal Financial Institutions Examination Council has emphasized the importance of a layered security system.[258] Notably, banks often set a daily limit on online consumer transactions, such as $1000. That practice suggests the wisdom of considering something more cautious, at least for sensitive information, than an immediate transfer of all information without hindrance. Layered security in the banking industry includes other practices such as: out-of-band authentication before completing internet transactions, sophisticated challenge questions, and suspicious activity detection.[259] Similar techniques could prove instrumental in protecting consumer privacy in a world with the RDP.

The 2000 FTC report stressed a key risk with online access: the lack of effective authentication on the Internet.[260] This lack of good authentication continues today, precisely for the online services that are the main subject of the RDP. A recent prominent example was when *Wired* reporter Mat Honen had much of his lifetime archive of files remotely wiped by a hacker.[261] In that instance, the hacker appeared to use "social engineering" to get into Honen's account—the hacker persuaded the customer service representative to reset passwords and thereby give the hacker full access to Honen's files.[262]

Any individual right in the area of data portability should thus be considered together with the individual's right for the data to be protected securely. Fundamental rights to flow data more quickly should be considered together with fundamental rights to block access to those who are not entitled to get it.[263]

---

258. FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL SUPPLEMENT TO AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT 2 (2012), *available at* http://ithandbook.ffiec.gov/media/153051/04-27-12_fdic_combined_fil-6-28-11-auth.pdf.

259. *Id.* at 4.

260. FEDERAL TRADE COMMISSION REPORT, *supra* note 249, at 4, 14–18.

261. Mat Honen, *How Apple and Amazon Security Flaws Led to My Epic Hacking*, WIRED (Aug. 6, 2012, 08:01 PM), http://www.wired.com/gadgetlab/2012/08/apple-amazon-mat-honan-hacking/all/.

262. *Id.*

263. For discussion of how there can be conflicting rights of an individual in the area of data flows, see Peter Swire, *Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment*, 90 N.C. L. REV. 1371, 1402–14 (2012).

IV. INTEROPERABILITY ITSELF AS A RATIONALE FOR THE RDP

The previous Parts have responded to the claims that Article 18 and the RDP are justified to address lock-in problems or protect the fundamental rights of the data subject. As discussed above, there are serious questions that a broad version of the RDP is justified under either competition or fundamental rights law. One additional argument for the RDP is that there may be reasons to support interoperability itself, apart from competition law or fundamental rights reasons. As we have stated throughout this Essay, we support interoperability in a wide range of settings.[264] Our understanding of Article 18, however, is that the RDP as proposed is quite different from previous legal efforts to protect interoperability. Proponents to date have not addressed this new aspect of the RDP, which places an affirmative mandate on the first player to create an EIM, and thus differs from previous efforts to ensure that it is lawful for second players to build products that can operate with the first player.

Apart from current doctrines of competition law or fundamental rights, interoperability itself might be a rationale for Article 18. Some scholars, for instance, believe that competition law currently inadequately protects against abuses from dominant networks.[265] Tim Berners-Lee, credited with inventing the World Wide Web,[266] is a notable supporter of interoperability. By increasing data flow between websites, he sees the potential for "unexpected, serendipitous re-use of data, that is, when somebody uses that information for a completely different purpose."[267] In their 2012 book *Interop*, John Palfrey and Urs Gasser write: "Interoperability should be an explicit goal in national and international discussions of business, law, and policy because the upsides of interoperability are massive: it fosters innovation and competition, enhances diversity, gives consumers choice, and can lead to unexpected benefits over time."[268] For proponents of openness in

264. *See supra* note 6 and accompanying text.

265. *See, e.g.*, Salil K. Mehra, *Paradise Is a Walled Garden? Trust, Antitrust, and User Dynamism*, 18 GEO. MASON L. REV. 889, 944 (2011).

266. *Tim Berners-Lee, Inventor of the World Wide Web, Knighted by Queen Elizabeth II,* MIT NEWS (July 16, 2004), http://web.mit.edu/newsoffice/2004/berners-lee-knighted.html.

267. Sarah Powell, *Guru Interview: Sir Timothy Berners-Lee, KBE*, EMERALD MANAGEMENT FIRST, at 2 (2006), http://first.emeraldinsight.com/interviews/pdf/berners-lee.pdf.

268. PALFREY & GASSER, INTEROP, *supra* note 61, at 8. Palfrey and Gasser emphasize downsides as well as upsides of interoperability. Gasser & Palfrey, *Breaking Down*, *supra* note 61, at 15–18.

computing, interoperability is a desirable goal when it prevents social networks such as Twitter and LinkedIn from locking in users by giving them the right to transport their data from those networks.[269]

One notable legal source that supports interoperability is the 1995 Court of Appeals for the First Circuit opinion in *Lotus Development Corp. v. Borland International*.[270] In that case, the court held that Lotus could not use copyright to protect its menu command hierarchy—a type of interoperability information.[271] Borland was thus permitted to copy Lotus's menu command hierarchy to build its own spreadsheet program.[272] The case specifically interprets the U.S. copyright law in a way that prevents the first party, Lotus, from blocking the second party, Borland.[273] The case can also be viewed as consistent with a broader message: The second party has and should have considerable freedom to find ways to write its own code so as to promote interoperability. There is a major distinction, however, between this freedom of the second party and the RDP. Article 18 imposes an affirmative mandate on the first party to write the EIM.[274] This affirmative obligation on the first party is a long step past the *Lotus v. Borland* holding of freedom to act by the second party.

European Union law on this point is similar. The 1991 E.U. Computer Programs Directive provides a copyright exception that allows second parties to first observe and study and then copy information necessary to achieve interoperability with the first party's product.[275] As described by noted copyright scholar Pamela Samuelson, U.S. and E.U. law both provide "first, that interfaces necessary to interoperability may be unprotectable by copyright law, and secondly, that reverse engineering of computer programs, insofar as it is necessary to discerning interface information, does not infringe software

269. PALFREY & GASSER, INTEROP, *supra* note 61, at 237 (discussing how social networks restrict horizontal interoperability).

270. 49 F.3d 807 (1st Cir. 1995).

271. *Id.* at 815.

272. *Id.* at 819.

273. *See id.* at 819 (finding that Lotus's menu command was uncopyrightable subject matter and therefore Borland could copy it without infringing on Lotus's copyright).

274. *See* Draft Regulation, *supra* note 1, at art. 18(2), at 53 (directing the first party to provide data "without hindrance").

275. Council Directive 91/250/EEC, *supra* note 29.

copyrights."[276] As with *Lotus v. Borland*, E.U. law allows the second party to build upon interoperability information without fear of infringing on the first party's copyrights, as long as certain provisions are met.[277] There is currently no requirement on the first party, however, to write an EIM to help the second party create interoperability.

The concept of interoperability has an undeniable appeal: Consumers will gain the ability to do new things and send data seamlessly to new products and services.[278] At the same time, some major market trends suggest that consumers often prefer systems that are "walled gardens," with limits on interoperability.[279] Apple has achieved the largest market capitalization in the world precisely by offering products with limited interoperability.[280] The iPhone initially allowed only Apple-developed apps.[281] Today, its App Store places considerably more restrictions on app developers than the competing Android operating system.[282] In another example of a walled garden, Facebook retains restrictions on what apps are allowed on its platform.[283] These restrictions can actually contribute to security and privacy, by reducing the risk that the apps will gain unwanted access to personal data.[284] In addition, other social networks, such as Twitter and Pinterest, have over time created Facebook apps that allow users to spread the

276. Pamela Samuelson, *The Past, Present and Future of Software Copyright Interoperability Rules in the European Union and the United States*, 34 EUROPEAN INTELL. PROP. REV. 229, 229 (2010).

277. Council Directive 91/250/EEC, *supra* note 29, art. 6, at 45.

278. *Cf.* PALFREY & GASSER, INTEROP, *supra* note 61, at 237–38 (describing current interoperability cloud-based environments that allow consumers to do new things).

279. For extended discussion of walled gardens and their advantages and disadvantages, including with respect to Apple, see JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET, AND HOW TO STOP IT 1–5 (2009).

280. Apple's market cap in August 2010 was nearing $620 billion. Steven Russolillo, *Apple's Market Value: To Infinity and Beyond!*, WALL ST. J. MARKETBEAT (Aug. 20, 2012, 11:58 AM), http://blogs.wsj.com/marketbeat/2012/08/20/apples-market-value-to-infinity-and-beyond/.

281. ZITTRAIN, *supra* note 279, at 1–5.

282. Chuck Gray, *Android VS iPhone*, LIBRARYPOINT (July 19, 2012, 09:04 AM), http://www.librarypoint.org/android_vs_iphone.

283. *Facebook Platform Policies*, FACEBOOK, http://developers.facebook.com/policy/ (last visited Nov. 12, 2012).

284. *See* Gray, *supra* note 282 (noting that Apple has superior security as compared to Android because its app restrictions cut down such risks).

unique data compilations of those social networks through the Facebook platform.[285] These examples of consumer preference for and competitive cooperation within walled gardens suggest caution before enacting the RDP that uniformly imposes interoperability mandates on both small and large providers of online services.

V. CONCLUSION

This Essay fills a surprisingly large gap in the debates about the proposed E.U. Data Protection Regulation. The gap may exist in part because data portability is an attractive concept—we as consumers would like to be able to move "our" stuff from one system to another.[286] In addition, data portability is a proposed new fundamental human right,[287] and many authors would rather support human rights than criticize them.

The proposed Article 18, however, has serious flaws from both a competition and privacy perspective.[288] Competition law in the E.U. and U.S. focuses on the welfare of consumers.[289] As discussed here, however, the proposed RDP appears to reduce consumer welfare.[290] Interoperability is often hard to achieve, and the RDP would impose substantial costs on suppliers of software and apps, to write the software to export data from one system "without hindrance" so that the data can be imported smoothly into a second system.[291] The costs of this mandated code would be passed on to consumers. As a matter of competition law, Article 18 is over-broad, applying to small enterprises, to enterprises with no monopoly power, and to markets with no barriers to entry.[292] More generally, Article 18 conflicts with the competition law rules about exclusionary conduct; it creates a per se prohibition where competition law would apply a rule of reason approach, considering efficiencies as well as possible harm to competition.[293]

285. *See, e.g.*, *Post Your Tweets to Facebook*, FACEBOOK, http://apps.facebook.com/twitter/ (last visited Nov. 12, 2012).

286. *See supra* note 6.

287. *See supra* Part III.A.

288. *See supra* Parts II–III.

289. *See supra* note 87.

290. *See supra* Part II.

291. *See supra* Part II.B.1.

292. *See supra* Part II.A.

293. *See supra* Part II.C.

The proposed Article 18 also suffers serious difficulties as a matter of data protection law.[294] There is no well-defined or established right to data portability—no jurisdiction has experimented with anything resembling the proposed Article 18, and the Draft Regulation would apply the new mandates to over half a billion residents of the European Union.[295] Article 18 is explicitly drafted under standard legislative procedures rather than through some constitutional process, and most of the important details are delegated down even further to the Commission.[296] These sorts of bureaucratic proceedings are not usually the source of a new fundamental human right. In addition, Article 18 poses serious risks to a long-established E.U. fundamental right of data protection: the right to security of a person's data.[297] Previous access requests by individuals were limited in scope and format.[298] By contrast, when an individual's lifetime of data must be exported "without hindrance," then one moment of identity fraud can turn into a lifetime breach of personal data.

As authors writing in the United States, we are not close enough to negotiations about the Draft Regulation to know what changes may be feasible before the Regulation becomes final. The goal instead has been to provide a thoughtful critique of the proposal. In a final Regulation or subsequent Commission actions, we hope the competition and privacy critique provided here can inform decisions about how to foster the best possible information economy, for the benefit of consumers and while reducing the likelihood of unexpected and negative consequences.

294. *See supra* Part III.

295. *See supra* Part III.

296. *See supra* Part III.A.

297. *See supra* Part III.C.

298. *See supra* Part III.C.