DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A: ECONOMIC AND SCIENTIFIC POLICY

Data Protection Review: Impact on EU Innovation and Competitiveness

STUDY

Abstract

The Committee on Industry, Research and Energy (ITRE) has requested an *ad hoc* briefing paper to provide its Members with information and advice regarding the proposed General Data Protection Regulation (2012/0011(COD)). This document presents a rapid assessment of the innovation and competitiveness impacts of the measures affecting: automated processing; control of data processing; and data transfers. It considers a variety of perspectives: profiling; big data; cloud computing; and privacy-friendly technologies and identifies a variety of impacts, and areas for improvement.

IP/A/ITRE/ST/2011-17
PE 492.463

December 2012
EN

This document was requested by the European Parliament's Committee on Industry, Research and Energy (ITRE).

AUTHORS

Jonathan Cave (RAND Europe)
H.R. (Rebecca) Schindler (RAND Europe)
Neil Robinson (RAND Europe)
Veronika Horvath (RAND Europe)
Sophie Castle-Clarke (RAND Europe)
A.P.C. (Arnold) Roosendaal (TNO)
Bas Kotterink (TNO)
Quality Assurance review conducted by Scott Marcus (WIK-Consult) and Joanna Chataway (RAND Europe)

RESPONSIBLE ADMINISTRATOR

Fabrizio Porrino
Policy Department Economic and Scientific Policy
European Parliament
B-1047 Brussels
E-mail: Poldep-Economy-Science@europarl.europa.eu

LINGUISTIC VERSION

Original: EN

ABOUT THE EDITOR

To contact the Policy Department or to subscribe to its newsletter please write to:
Poldep-Economy-Science@europarl.europa.eu

Manuscript completed in December 2012.

This document is available on the Internet at:
http://www.europarl.europa.eu/studies

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS

Art 29 WP	Article 29 Working Party of the Data Protection Directive 95/46/EC
AS	Autonomous System
B2B	Business to business
B2C	Business to customer
BCR	Binding corporate rule
BEREC	Body of European Regulators for Electronic Communications
BEUC	The European Consumers Organisation
BT	British Telecommunications plc
CAGR	Compound Annual Growth Rate
Capex	Capital Expenditure
CEO	Chief Executive Officer
CNIL	Commission nationale de l'informatique et des libertés (National Committee on Individual Liberties – French data protection authority)
Convention	European Convention on Human Rights (European Convention for the Protection of Human Rights and Fundamental Freedoms)
CPO	Chief Privacy Officer
DNT	Do Not Track
Data	Information that is: automatically processed; recorded in order to be automatically processed; recorded in a *filing system* by names or individual characteristics; forms part of an accessible individual record; or is information about individuals held by public authorities.
Data controller	A person[1] who (alone or together with others) determines why and how personal data are to be processed.
Data processor	A person who processes data on behalf of a data controller[2].
Data subject	An identifiable person who is the subject of data
DPA	Data Protection Authority
DRM	Digital Rights Management

[1] Person means 'legal person'

[2] The roles of controller and processor are not always distinct; but the party with the greatest latitude and expertise is considered to be the data controller.

ECHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
ENISA	European Network and Information Security Agency
EU	European Union
FTC	Federal Trade Commission
IaaS	Infrastructure as a Service
ICAO	International Civil Aviation Organisation
ICO	Information Commissioner's Office
IP	Intellectual Property
ITRE	Committee on Industry, Research and Energy (European Parliament)
LBS	Location Based Services
MS	Member States
NGO	Non-Governmental Organisation
OBA	Online Behavioural Advertising
OECD	Organisation for Economic Co-operation and Development
Opex	Operating Expenditure
P3P	Platform for Privacy Preferences
PaaS	Platform as a Service
PbD	Privacy by Design
PETs	Privacy Enhancing Technologies
PGP	Pretty Good Privacy
PIA	Privacy Impact Assessment
PLA	Privacy Level Agreement
PPP	Public-Private Partnership
SaaS	Software as a Service
SAR	Subject Access Request - requests by data subjects for access to the data held about them by data controllers
SLA	Service Level Agreement
TFEU	Treaty on the Functioning of the EU
US	United States

LIST OF TABLES

LIST OF FIGURES

EXECUTIVE SUMMARY

The existing Data Protection Directive 95/46/EC (DPD) has been in force for more than two decades. During that time, data processing has changed extensively, and many other industries and essential services have been built on the use (and abuse) of personal data. At the same time, attitudes towards data privacy have undergone considerable evolution in response to technological and market developments, the globalisation of information-intensive economic activity and accumulated experience with data sharing – especially among the generation that has grown up on-line. Partially in response to these developments, a wide range of legal measures and enforcement arrangements have been enacted in different Member States to give force to the Directive. These have been accompanied by an even wider range of formal and informal data protection (DP) policies (or absence of policies) in other countries where EU citizens' data may be processed and where European firms seek to compete.

The original aims of the Directive were[3]: to ensure a high level of data protection for all individuals in the EU; to achieve an equivalent level of data protection in all Member States in order to ensure the free flow of information within the internal market; and (in the police and criminal justice area) to enhance mutual trust and thus support the exchange of personal data between police and judicial authorities. Subsequent developments – including those mentioned above - have prevented the full attainment of these objectives. In response, the European Commission has proposed a new Regulation, whose implementation would respond to some of these developments and would by its very nature eliminate the current legal fragmentation.

The impacts of the proposal were assessed in terms of the effectiveness with which it was likely to attain its objectives, the efficiency with which it might do so and its consistency with other elements of European policy. This assessment, however, did not consider in detail the rich variety of activities that conduct or depend on data collection and processing, the speed and extent of emerging changes in technological, business and market arrangements and the implications for competitiveness and innovation.

In order to shed further light on these aspects, this briefing examines the likely impacts of the proposed Regulation and two alternative options on the competitiveness and innovation performance of the European data processing value network - those who control and process personal data and those who supply essential inputs or use the services provided.

In particular, the current document concentrates on three activities of participants in the data processing value network: automated data processing and profiling; documenting and demonstrating compliance with the law; and data transfers to non-European jurisdictions.

The main conclusions are summarised in Table 1 and discussed in the text that follows. In brief, the study found that the Regulation offers many potential advantages, but tends to be overly prescriptive in areas where European firms have already demonstrated their ability to reconcile privacy rights with economic development. The Regulation recognises the need to build confidence and facilitate effective governance by documenting compliance, but does so in a way that may create additional burdens and distort the allocation of responsibilities among different stakeholders. This is related to a more general point; the tendency to address current problems in fairly specific (and therefore time-bound) terms. This may inhibit innovation or expose data protection rights to future evolution as the data protection landscape continues to evolve. One example of this

[3] Paraphrased from Section 3.1 of European Commission 2012b.

concerns the delineation of the roles of data controllers and data processors; in some contexts (e.g. cloud computing) the roles are variable or conflated, while in others (e.g. big data analytics) data controllers may be much smaller and less powerful than data processors, and ill-placed to monitor, let alone control, their actions. A further example is provided by the expanded requirements regarding data transfer; the separate treatment of massive and/or frequent data transfers does not seem aligned with the growing variety and ubiquity of data transfers, and the legitimate interest exemption for data controllers does not fully reflect the scope of the agency relationships among data subjects, controllers and processors. Therefore, the study recommends some modifications to increase the flexibility and future-proofness of the Regulation in order to protect competitiveness and harness the privacy-friendly innovative capacity of European industry.

Table 1: What are the conclusions of the study?

Conclusions	
	Generic conclusions on EU DP, innovation and competitiveness
1	The proposed Regulation is likely to produce impacts on market structure, conduct and performance (as regards economic competitiveness and innovation) that go beyond those considered in the Impact Assessment (IA).
2	The tension between privacy and innovation may simply be a matter of timing: many dominant business models involving the use of private information began as unstructured free services; the implicit exchange of service for information access emerged together with user communities willing to share information.
3	Economic forces have powerfully influenced the privacy landscape; they have motivated both potential threats and attractive solutions. However, available data on economic outcomes are too partial and short-term to reflect fully the costs, benefits and sustainable impacts of privacy measures and market responses to them.
4	The sustainability of privacy protections depends on the extent to which they are taken up in the market and adapted to the specific and evolving requirements of data subjects and others able to influence or benefit from use of personal data. This creates a feedback loop: legal measures change the technological and market environment, which in turn changes the basis for legal intervention.
5	Europe's privacy policy differs systematically from that of its main competitors; thus economic competition is bound up with contention among different privacy models. The costs and restrictions imposed by privacy law play out in a global economic context.

Conclusions	
6	To the extent that European firms are better able to meet European legal requirements than foreign firms, they will enjoy a privileged position in domestic markets. This may not provide the benefits of competition, however, if a) foreign rivals are effectively prevented from competing with European firms (depriving the latter of the benefits of market discipline); or b) the hurdles facing the overseas and/or globally-based providers currently dominating European information-intensive services (e.g. search, social networking) are so high that European citizens and businesses alike cannot build on world-class platforms.
7	The lower level of privacy protection available in foreign markets does not necessarily reflect either a diminished desire for privacy by foreign users or an inability by foreign firms to protect their users' privacy. It may instead represent a lock-in; end-users do not demand what they cannot get, and firms do not offer services for which there is no apparent demand. The advent of European service providers who have already sunk the costs of delivering privacy protection following the European model may release this lock-in, leading to a general uplift in privacy provision. European firms will reap first-mover advantages, and European firms and citizens may jointly benefit in the medium- to long-run as privacy becomes an active basis for competition.
8	If global privacy standards become a race to the top, the additional burdens (over and above the cost of competing) of compliance will disappear and some costly regulatory measures can be dropped.
9	To the extent permitted by regulation, privacy-friendly innovations may be expected in terms of technology (e.g. PETS[4]), contracts[5] and business models[6].
	Conclusions on automated processing
10	The proposed blanket restrictions on profiling harm competitiveness by undercutting existing business models; profiling is increasingly important for back-office efficiency, new service discovery and customer quality of service delivery e.g. targeting to mutual benefit, and represents an area where existing protective measures stimulated innovations[7]. This can be protected by limiting the freedom from automated processing to identified natural persons.
11	The consent requirement is likely to prove more burdensome to small firms than large ones due to the ease with which the latter can get high degrees of consent from their installed base.

[4] E. g. Privacy by design - see Section 3.6.
[5] E.g. Privacy Level Agreements – see Section 3.5.1.
[6] E.g. Privacy as a service – see Sections 2.2.3 and 4.5.5.
[7] E.g. anonymous profiling – see Section 3.3.3.

Conclusions	
	Conclusions on data controller responsibility
12	The documentation requirements imposed separately on data controllers and processors will create duplicative administrative burdens for smaller firms – and possibly for regulators forced to handle the flood of new information. This can be eased by restricting the scope of information provided to that necessary to verify compliance and enable market discipline and to permit shared compliance among contractual partners.
13	The requirements may not be equally proportionate in balancing costs and benefits in all sectors and may therefore distort business and service models and market relationships away from the forms dictated by technological and market forces, especially in emerging areas such as cloud and big data.
	Conclusions on data transfers
14	The asymmetry of treatment on the basis of data transfer size and frequency is likely to affect small and innovative firms more than large incumbents. It may also undercut control by data subjects who are not in a position to know whether specific transfers of their data are covered and whether the advantages outweigh the risks. In addition, the administrative costs of fine-grained consent may be particularly high.
15	The provisions may pose significant obstacles in relation to cloud and big data, where many data transfers are large-scale and frequently international – though this can be compensated to some extent by the growth of capacity that reduces the need for such transfers. This can be circumvented by avoiding such transfers, but this would have the effect of reducing competition between data controllers and processors located in different countries, and reducing the operational cost and big data scale advantages of greater mobility.
	Conclusions on the preferred option
16	Option 1 will encourage foreign providers to adapt their practices in European markets, ensuring that privacy and other aspects of service quality develop together and that European firms benefit from healthy domestic competition.
17	Option 1 also creates the basis for unlocking the inefficient privacy equilibrium of low expectations and inadequate provision in overseas markets in a way that provides both immediate and medium- to long-term benefits, allowing European firms to compete overseas and European citizens to benefit from the emergence of privacy as a basis for competition leading to further improvements in the European legal framework and enhanced international harmonisation as differences disappear.
18	Finally, Option 1 helps to reconcile the false tension between economic recovery and effective privacy protection by allowing Europe to build on a unique advantage (privacy friendly technologies and business models) while enhancing trust and thus the economic utility of online economic activity for Europe's citizens.

Table 2: Summary of impacts

	Art. 20: profiling	Art. 28: responsibilities	Art. 44(1)(h): migration
Competitiveness			
Profiling, Behavioural Advertising, Cookies and Social Media	Bad for EU B2B vs. US B2C	Onerous for small data processors and controllers	Reciprocity, level playing field
Big Data	As with profiling; May favour larger firms	Uncertainty due to unclear data processing and controlling roles	Can limit efficiency-enhancing migration Can reassure users
Cloud Computing	Seems to require *logged-in* model	Difficult for cloud-hosted services; may ease DPA work	No significant impact[8]
Privacy friendly technologies	Trust frameworks, better data sharing	Good if standardised	No significant impact
Innovation			
Profiling, Behavioural Advertising, Cookies and Social Media	Bad for EU innovations based on PBD; not neutral	No significant impact	May inhibit app development for global markets
Big Data	Inhibits BD development; may encourage compliant BD by big firms	Potential *effective anonymisation* tools	Can limit size of data sets: ambiguous
Cloud Computing	Rules out freemium models	Potential chains of responsibility	No significant impact
Privacy friendly technologies	Digital identities; but some uncertainty	No significant impact (logging techniques)	No significant impact

[8] Data migration is central to the development of the cloud. The proposed Regulation limits the scope of existing protections to "frequent or massive" data transfers and thus does not substantially change the protections and restrictions applying to cloud computing *per se*.

Table 3 Summary table

Option	Option 0	Option 1	Option 2
Effectiveness linked to objective 1: internal market dimension of data protection			
1.1 Harmonising and clarifying rules to provide neutral competitive environment	+/- Harmonisation reduces national asymmetries, but some competitive distortion	+/+ Harmonised, clarified rules; scope limited to direct risks, competition balances protection, value of Personal Identifiable information (PII)	-/+ Variation by self-regulatory body; *choice of rules* levels playing field, adaptation
1.2 Consistent enforcement across jurisdictions, sectors and firms	+/- Consistent across jurisdictions, some variation by sector and firm size/type	+/+ Retains single Regulation, clarified enforcement	+/-- Consistent across jurisdictions, but likely to vary across sectors; possibly weak enforcement
1.3 Cutting red tape	+ Some reduction through unified requirement; additional burdens for processors	+++ Burdens minimised and used as incentives	++ Lowest burden, but not necessarily aligned with data subject interests
Effectiveness linked to objective 2: fundamental right to data protection			
2.1 Individual control of data and trust in digital environment	+ Provides personal control, but may not be effectively exercised due to consent problems	++ Limits complexity of data subject choices; consent may still be problematic for e.g. cloud, big data	++ May allow more understandable PLA[9], but potential for confusing choice.
2.2 Protection when data are processed abroad	++ Enhanced incentive for offshore compliance; protection depends on size and frequency of transfers; may inhibit mutual recognition	+++ Size and frequency asymmetries removed; incentive for providers to make contractual protections explicit	+ Indirect control possible through *Safe Harbour* types of arrangements, conditional co-regulation.
2.3 Accountability and responsibility	++ New obligations on data controllers and processors	+++ Accountability obligations aligned with data subject interests; increased role for PLAs	- Limited by market forces.

[9] Privacy Level Agreement – see Section 3.5.1.

Option	Option 0	Option 1	Option 2
Efficiency			
Minimising costs and other burdens	++ Decreased localisation costs, but undercuts existing business models (esp. profiling) and imposes data handling burdens on processors and regulator; costs may be lower for large, incumbent firms.	+++ Decreased localisation costs, enhanced revenues from profiling, cloud, big data and sales of PETs, lower documentation costs, wider geographic market scope for small and innovative firms	+ Costs minimised by industry input to rulemaking; costs lower for firms with significant market power unless competition rules applied to self-regulatory bodies.

Table 4: What are the main recommendations of the study? (Option 1)

Recommendations in light of competitiveness and innovation considerations	
1	Article 20 of the proposed regulation should be recast to clarify that the legal and significant effects required for exemption from automated data processing and decisions apply to identifiable persons (*data subjects* rather than *natural persons*).
2	Article 28 should be modified to limit required documentation to data protection policies and implementation and monitoring measures, and to permit trust hierarchies to permit data controllers to certify data processors or vice versa depending on the size, resources and relative discretion of the parties.
3	Article 44(1)(h) should be modified to remove the reference to 'massive or frequent' data transfers. In addition, the legitimate interests of data controllers should explicitly include transfers necessary for efficient data management and those explicitly agreed in service level or privacy level agreements. The justification for this change is that international data transfers are fundamental to cloud computing.

1. INTRODUCTION

In view of the on-going discussions on 2012/0011(COD) "Personal data protection: processing and free movement of data (General Data Protection Regulation)", the Committee on Industry, Research and Energy (ITRE) has requested an *ad hoc* briefing paper to provide information and advice to the Members of the ITRE Committee.

This paper presents the results of a rapid evidence assessment of the innovation and competitiveness impacts of European data protection legislation to provide the Committee with independent expert advice relevant to the identification of priority measures and actions in response to the legislative proposal.

It offers a balanced picture of the variety of views held among professionals in this field as well as the authors' independent assessment in a readily accessible and concise manner. The analysis has been informed by a systematic literature review, semi-structured expert interviews and an online survey. It builds on available data, reports, studies and the authors' expertise and provides specific discussions on a range of issues outlined in section 1.2 below. As far as possible, the analysis is based on existing case law, concrete figures and statistics, complemented by illustrative examples.

1.1. Why this study is relevant

A previous study[10] commissioned by the ITRE Committee established that data processing industries in the US and the EU have taken different paths, partially in response to differences in data protection standards and legal measures at federal US level[11] compared with EU (and Member State) level. A direct quantitative comparison of the economic (competitiveness and innovation) effects is difficult: the sectors are organised in different ways and involve different stakeholders; key data are not consistently measured and prone to breaks and differences in coverage; and market boundaries are not reflected in available databases. However, it is both possible and relevant to map the ways in which the 95/46/EC Data Protection Directive has influenced innovation and competitiveness of EU industries relative to their US counterparts and the extent to which the proposed data protection Regulation (COM 2012/0011) can be assumed to increase or decrease such industrial differentiation.

Some systemic differences are obvious from the outset. For instance, the EU data processing industry appears to concentrate on serving the business-to-business layer (B2B), while US data processing firms are more likely to interact directly with end-users. B2C entities such as Google and Facebook are both data controllers and data processors[12], providing platforms through which data are collected and through which they can obtain direct feedback, communicate and implement privacy policies and obtain consent. In contrast, the connections among European data subjects, controllers and processors may be less direct; for instance, the B2C role may be filled by a telecom provider Internet service provider, who may not have the same degree of control over the user interface and user experience, or the same ability to control how data are transferred and processed and may face greater difficulty in brokering agreement between data processors and data subjects and in obtaining end-user consent.

---

[10] Cave et. al. (2011).

[11] See 2.3.3 for a discussion of eleven US Federal laws that affect electronic privacy in terms similar to those covered under the EU framework.

[12] These and other terms are defined in the Table beginning on page 7.

There are also differences with respect to the location of data storage and processing; the EU primarily[13] defines protections in general terms applicable to a wide range of business and service models, while the US tends to use specific provisions tied to particular sectors and/or forms of data and tends to separate data access and data integrity to a greater degree. The effects of this fragmentation (the use of sector-specific privacy rules in the US, in comparison to an over-arching approach in the EU) may be failure to provide the expected levels of protection or uncertainty as to the level of protection available to existing or new business arrangements and services. Finally, while the EU obliges data processors and controllers to ensure that data subjects enjoy the benefits of data protection even if the personal data is processed outside of the Union, US data management regulations do not appear to offer similar protection.

1.2. Problem statement

The problem addressed in this briefing is narrower in scope than the ones addressed by the proposed Regulation. Concisely phrased it is: the impact of current and proposed privacy provisions may inhibit competitiveness and innovation, and from our point of view in any case they underutilises the potential of market forces to balance privacy protection with economic benefits.

To put this in context, the problem addressed by the proposed Regulation is essentially to complete the work of the existing Directive[14] while responding to new challenges[15]. This briefing's emphasis on competitiveness and innovation is highlighted by the Impact Assessment (IA)[16] that accompanied the proposed Regulation; it considered competitiveness impacts in terms of costs, innovation and international competitiveness, but from a fairly limited perspective:

- The analysis of affected value networks was described in broad brush terms;
- Costs were primarily restricted to compliance[17] costs – other cost consequences including the costs of acquiring and reusing data and of providing services to end-users, and the indirect impact of changed patterns of market fragmentation on the whole gamut of costs were not considered;
- Innovation was discussed primarily in terms of the inhibiting effect of fragmentation and regulatory uncertainty on formal innovation (*invention*) by individual competing firms, with less attention paid to collaborative and bottom-up innovation, the 'natural experiments' conducted in different countries and service contexts, innovations in business models and market architectures and the possible efficiency gains from *appropriate differentiation* - i.e. different types of protection in different contexts; and
- The analysis of competitiveness within the single market emphasised harmonisation, but did not consider non-neutral impacts of harmonised rules on different entities (e.g. commercial and non-commercial, small and large); the analysis of international competitiveness concentrated on the ability of European firms to compete with non-

[13] The EU also has some sector-specific data processing regulations, decisions and case law e.g. financial sector [Council of the EU (2006)] and air passenger information [EC Court of Justice (2006)]; some of their provisions may differ from those in the proposed Regulation.

[14] This is threefold: to ensure a high level of data protection for all individuals in the EU; to achieve an equivalent level of data protection in all Member States in order to ensure the free flow of information within the internal market and (in the police and criminal justice area) to enhance mutual trust and thus support the exchange of personal data between police and judicial authorities. See European Commission (2012a).

[15] These include technological developments, globalisation and differences in Member States' transposition and enforcement of Directive 95/46/EC.

[16] European Commission (2012b).

[17] Likely levels and distributions of compliance were also not considered.

European counterparts *in European markets* but did not take into account the general equilibrium effects of competition in global markets[18] or the possibility that presumed privacy preferences might differ from those expressed in the European and non-European markets.

Against this background the briefing paper will address three specific aspects of the proposed Regulation whose impacts on competitiveness and innovation are likely to go beyond those foreseen in the Impact Assessment and which therefore might suggest a reconsideration of its provisions.

This briefing paper concentrates on provisions related to profiling (Article 20), the documentation of processing activities and responsibilities (Article 28) and the transfer of personal data to third countries (Articles 6(1)(f) and 44(1)(h)).

This briefing paper also attempts to provide some data on the performance of selected US and EU companies whose businesses rely on, require or make use of data processing in order to investigate as far as possible whether due to the two different approaches undertaken any type of correlation with innovation and competitiveness (both inter- and intra-company/market) can be drawn.

1.2.1. Automated data processing and profiling

Article 15 of Directive 95/46/EC grants the right to every data subject to not be subject to automatic processing ('automated individual decisions') producing legal effects or significantly affecting the data subject. This right is further developed in article 20 ('measures based on profiling') of the proposed Regulation.

1. Has this affected the direction of EU data processing innovation and can it be assumed that this impact will continue? Which impacts are foreseen by the stronger requirements in the proposed data protection Regulation as compared with Directive 95/46/EC?

1.2.2. Data controllers' obligation to control data processing

Article 17(2)-17(4) of Directive 95/46/EC obliges the data controller to ensure that a data processor is able to fulfil the protection requirements of the Directive with regards to the data subject. This obligation is further developed in Article 28 of the proposed Regulation[19].

2. Has this control requirement given rise to any particular business model development in the controller or processor layers in the business-to-business interactions in the EU? Which effects are foreseen by the rephrased Article 28 with respect to these business models? In particular, what advantages can be had for the protection of data subjects by providing incentives for the development of particularly beneficial privacy friendly business models through the proposed delegated acts to be adopted by the Commission?

1.2.3. Data migration

Data controllers should ensure that data subjects' right to data protection is not impeded by the transfer of data to a third country. However, Directive 95/46/EC contains an exception from this principle in Recitals 30, 39 and Article 7(f), which should be compared

[18] In other words, the spill over impacts from one market to another and the competitiveness of European firms in non-European national markets or truly global markets.

[19] This Article also imposes recordkeeping burdens on data processors.

with Recital 38 and Articles 6(1)(f) and 44(1)(h) of the proposed data protection Regulation containing an exception based on controller interest[20]. The restrictions on transfers in Directive 95/46/EC implicitly acknowledge that transfers to third countries lacking equivalent provisions lead to reduced data protection.

3. Have the restrictions on transfers of data in any way affected the direction of EU innovation in the data processing sector? If Directive 95/46/EC can be shown to have affected actual innovation in business models used by EU data controllers, can this effect be assumed to be magnified by the new Regulation?

1.3. Objectives

The present investigation is concerned with a subset of the objectives of the proposed Regulation[21]. The most relevant objectives are those connected with completing the achievement of the original Directive 95/46/EC objectives in light of current and coming developments (which include the changing services, business models and market structures in the data processing industry[22]).

1.3.1. General objectives

The general objectives considered in this briefing are limited to the first and second objectives cited in the proposed Regulation[23].

1. Enhancing the internal Single Market dimension of data protection.
2. Increasing the effectiveness of the fundamental right to data protection.
3. Establishing a comprehensive EU data protection framework and enhancing the coherence and consistency of EU data protection rules, including in the field of police cooperation and judicial cooperation in criminal matters.

The third is mentioned here but not considered further because its attainment is not materially and directly bound up with the competitiveness and innovation impacts of the Directive.

1.3.2. Specific objectives

The specific objectives associated with the general objectives listed above are likewise related to those cited in the proposed Regulation, but modified in light of the restricted scope of this document.

Specific objectives linked to general objective 1:

1.1. Harmonising and clarifying EU data protection rules and procedures to provide a neutral competitive environment in which different sizes of firms, business models and services can compete on their merits provided fundamental data rights are respected;

1.2. Ensuring consistent enforcement of data protection rules across jurisdictions, market sectors and firm characteristics; and

---

[20] See Table 14 in ANNEX 3.

[21] See in particular Section 4/Table 1 in European Commission (2012b); the objectives defined here have been recast to reflect the focus of this study on specific activities (profiling, data controllers' documentation responsibilities and data migration) and on competitiveness and innovation.

[22] See Section 2.2.

[23] See European Commission (2012a)

1.3. Cutting inappropriate red tape to ensure that the burdens of compliance – and demonstrating compliance – are efficiently distributed to minimise deadweight loss[24], encourage innovation and ensure that responsibility for privacy-enhancing action rests on those best-placed[25] to discharge them.

Specific objectives linked to general objective 2:

2.1. Ensuring that individuals have effective and appropriate control of their personal data and trust the digital environment[26];

2.2. Ensuring that individuals remain protected including when their data are processed abroad;[27] and

2.3. Ensuring that accountability and responsibility optimise the incentives of those involved in processing personal data.

1.4. Options

Because this document takes the proposed Regulation as its starting point, the range of options considered is limited and their definition is implicit. Briefly, they comprise[28]:

- Option 0 is the proposed Regulation;
- Option 1 consists of the proposed Regulation with the following modifications
  - Article 20 is recast to clarify that the legal and significant effects required for exemption from automated data processing and decisions apply to identifiable persons (*data subjects* rather than *natural persons*);
  - Article 28 is modified to limit required documentation to data protection policies and implementation and monitoring measures, and to permit trust hierarchies to permit data controllers to certify data processors or vice versa depending on the size, resources and relative discretion of the parties; and
  - Article 44(1)(h) is modified to remove the reference to 'massive or frequent' data transfers. In addition, the legitimate interests of data controllers include transfers necessary for efficient data management and explicitly agreed in service level or privacy level agreements. The justification for this change is that international data transfers are fundamental to cloud computing.
- Option 2 - enhanced self and/or co-regulation involving European and non-European DPAs and industry stakeholders; this option is discussed in Chapter 4 but not formally considered, because its scope and complexity go beyond the scope of this briefing.

1.5. Structure of this report

The remainder of this document is structured as follows:

- Chapter 2 discusses the overall context; it provides:
  - an overview of the framing of economic impacts used in this report;

[24] Deadweight loss refers to the loss of gains from trade that results when the price paid by consumers differs from the price received by suppliers – when this happens, output is too small, because a consumer would be willing to pay more for an additional unit than the cost of supplying it.

[25] This may include reallocation of responsibilities by contractual or other means.

[26] Recognising that some data subjects may not be able or willing to exercise full control in all circumstances, and that more trust is not always better – e.g. where individuals should guard their own privacy.

[27] Recognising that individual interests are not necessarily protected by prohibitions on data migration.

[28] See also Section 2.

  - an analysis of the legislative context including the provisions and implementation of the current Directive, the relevant Articles of the proposed Regulation, a comparison to the most relevant aspects of US data/privacy protection (in view of the importance of US-based firms in the data processing industry and of technical and business developments originating in US markets), and a discussion – from this perspective – of the Impact Assessment.

- Chapter 3 presents evidence derived from desk research, survey and interviews – in view of the complexity and interconnectedness of the data processing value network, this is presented in the form of four different perspectives or case studies corresponding to existing or emerging lines of business (profiling, big data, cloud computing and privacy-enhancing technologies); a final section discusses the challenges and tensions arising from those cases and develops crosscutting themes.
- Chapter 4 summarises the findings along Impact Assessment lines – while this report does not attempt a full Impact Assessment, it is nonetheless helpful to consider the impacts of the proposed Regulations and a modified version in terms of the three highlighted aspects (profiling, data controllers' responsibilities and data migration) and the four perspectives (profiling, big data, cloud computing, privacy-friendly technologies) identified in Chapter 3. These will be used to compare the options from the perspective of impacts on economic competitiveness and innovation and to select a preferred alternative.

2. BACKGROUND AND CONTEXT

2.1. Introduction

The proposed General Data Protection Regulation brings a number of legislative changes compared to the currently applicable Directive (95/46/EC), with the aim of adapting data protection legislation to the needs of the information society. Developments in ICT and associated changes in market structure and conduct have brought new challenges and will continue to do so. The increasing complexity and rapid evolution of the data processing market potentially renders portions of the Directive obsolete and exacerbates the consequences of differences in national implementation of its provisions[29].

On the economic side, the traditional roles of data processor and data controller on which the assignment of responsibilities under the Directive rested, are changing and overlapping. Moreover, technological development and the self-organising complexity of the Information Society compromise the extent to which data subjects, controllers and processors can be assumed to be capable of overseeing, understanding or controlling the dissemination and processing of personal data and the uses to which such data are put. Therefore, Section 2.2 discusses the links among privacy provisions, competitiveness and innovation and describes salient aspects of the *data protection value network* through which these linkages operate, in order to expose the mechanisms by which the provisions of the Directive and the Regulation will affect market-mediated outcomes.

Prior to the presentation of the Regulation proposal, stakeholders were consulted to share their views and opinions and an Impact Assessment was carried out to assess the different options for addressing the main regulatory issues. During the consultation phase, which lasted for more than two years leading up to the presentation of the proposal in January 2012, the views of a range of stakeholders were collected; for the most part, these were limited to comments in general terms on definitions and requirements, calling for strengthening of concepts and providing more clarity on scope. Those consulted generally agreed that the general principles of data protection were still valid,

> *"but that there is a need to adapt the current framework in order to better respond to challenges posed by the rapid development of new technologies (particularly online) and increasing globalisation, while maintaining the technological neutrality of the legal framework."*[30]

The Impact Assessment[31] addressed three main problems:

- Barriers for business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement;
- Difficulties for individuals to stay in control of their personal data; and
- Gaps and inconsistencies in the protection of personal data in the field of police and judicial cooperation in criminal matters.

---

[29] For example, with regard to consent, some Member States have adopted opt-in laws, others adopted opt-out laws and still others have considered annual consent procedures. [Korff (2002), Robinson et. al. (2009), Olavsrud (2012)].

[30] European Commission (2012b), p. 4.

[31] European Commission 2012b sections 3.2, 3.3 and 3.4.

This briefing paper is concerned only with the first of these. The IA, however, emphasises legal consistency over specific requirements for businesses concerning their obligations and rights.

The IA considered several options. The first option was soft action to encourage standardisation and self-regulation by businesses. This option may still form part of the delegated acts to be implemented by the European Commission, which can set requirements for standardisation and self-regulation and allow businesses to comply in a flexible manner – it parallels Option 2 (see Section 1.4) of the current document.

The second option was a modernised legal framework. This option relates directly to Option 0 (see Section 1.4) of this briefing paper and is meant to facilitate transfer of data to third countries, strengthen control by data subjects and reinforce data controllers' responsibility and accountability; topics specifically addressed in the proposed Regulation.

A third option was detailed legal provisions at an EU level, applicable to specific sectors and possibly related to the delegated acts mentioned in Article 28 of the proposal.

The preferred option was Option 2, the modernised legal framework, which is taken as the starting point for this briefing paper. Its expected impacts were seen as substantial and positive. It would decrease administrative burdens, for instance, by introducing a one-stop shop for data protection compliance. Reduction of administrative burdens was deemed to stimulate competition and innovation. Moreover, this option would lead to considerably greater legal certainty for data controllers and citizens and consistency of data protection enforcement throughout the EU. Implementation was also "expected to contribute to the Commission's objective of simplifications and reduction of administrative burden and to the objectives of the Digital Agenda for Europe[32], the Stockholm Action Plan[33] and the Europe 2020 strategy."[34]

The Impact Assessment Board (IAB) reviewed the IA, calling for improved evidence of fragmentation and inconsistent enforcement of existing data protection provisions, better consideration of proportionality and subsidiarity and a clear and robust background for the estimates of costs and benefits. In particular, the IAB requested a stronger analysis of the competitiveness implications for SMEs.

The instrument of a Regulation can replace the diverse data protection laws of individual EU Member States and adapt them to the new institutional framework of the Lisbon Treaty, while respecting Article 16 of the Treaty on the Functioning of the European Union and Article 8[35] of the EU Charter of Fundamental rights, which state that everyone has the right to personal data protection in all aspects of life.[36]

Amongst the most important changes are a number of newly introduced concepts, such as privacy by design and data protection by design, the right to data portability, and the right to be forgotten. Furthermore, a number of existing concepts have been strengthened, such as the definition of consent, in particular the requirement that it has to be obtained

---

[32] European Commission (2010a)

[33] European Commission (2010b)

[34] European Commission (2012b), p. 5.

[35] The more general right to respect for privacy is laid down in Article 7 of this Charter.

[36] According to the 2011 Eurobarometer on Attitudes on Data protection and electronic identity in the EU, 1) 60% of Europeans who use the internet (40% of all EU citizens) shop or sell things online and use social networking sites. 2) People disclose personal data, including biographical information (almost 90%), social information (almost 50%) and sensitive information (almost 10%) on these sites. 3) 70% said they were concerned about how companies use this data and they think that they have only partial, if any, control of their own data. 4) 74% want to give their specific consent before their data is collected and processed on the Internet. Source: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

explicitly, and rights not to be subjected to automated decisions and profiling. In the context of enforcement, the powers of Data Protection Authorities (DPAs) will be strengthened and a supervisory authority at EU level will be introduced. Data controllers have been granted more freedoms and opportunities with regard to the processing of personal data. However, these freedoms are balanced by increased responsibility and accountability for those processing personal data.

Section 2.3 analyses the proposed legal changes by discussing the provisions and implementation of the current Directive, contrasting these with the proposed Regulation, comparing the EU structure with the US situation and summarising the most relevant findings of the Impact Assessment that accompanies the proposal.

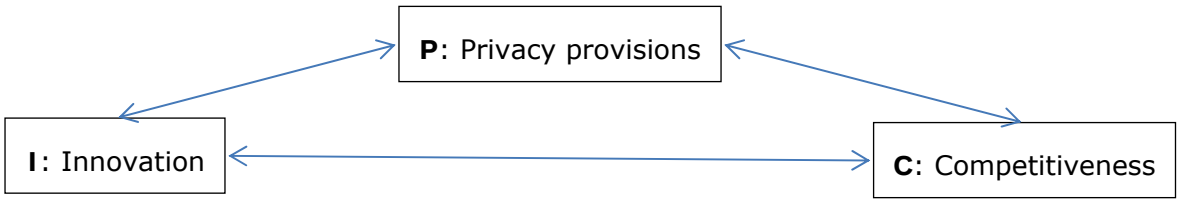
2.2. Economic and market framing

The questions in the previous section are deceptively simple, amounting in essence to: whether specific provisions of the existing Directive have affected the competitiveness and innovation performance of the European data protection industry, and whether the new Regulation is likely to continue or reverse those changes? However, the complexity and dynamism of the markets that use personal information and that supply data processing and privacy compliance services are such that it is useful briefly to set the stage[37] by sketching the data processing value network and the broad channels through which privacy protections can affect competitiveness and innovation. To calibrate the effects, Section 2.2.4 briefly summarises recent findings on the importance of privacy protection to the market valuation, reputation and other sources of enterprise value safeguarding personal data and other aspects of business processes covered by the Regulation. These can be taken as indicative of the direct impacts of improved compliance and a privacy-respecting business culture; they also provide insight into the extent to which the logic underlying the use of informational remedies (e.g. breach disclosure) and associated discipline by financial and/or service markets can be relied upon.

2.2.1. The relation between privacy, competitiveness and innovation

The previous report[38] focused on the two-way relation between Internet innovation and privacy. In this briefing, we extrapolate from innovation to the competitive Internet-based economy and from privacy per se to European privacy provisions (Directive 95/46/EC and the proposed Regulation). This can be visualised in the following diagram and Table 5 overleaf:

Figure 1: The relationship between privacy, competitiveness and innovation



[37] The underlying concepts are spelled out in greater detail in the precursor ITRE study Cave et. al. (2011).

[38] Cave et. al. (2011).

Table 5: Relation among competitiveness, innovation and privacy provisions

Link	Example	Direction	Detail
C→P	Privacy-aware business models	Positive	Privacy as a service: offering privacy protection bundled with other services, or separately as an add-on service (possibly from a certified third party).
		Negative	3rd party monetisation: supporting service provider revenues or subsidising prices charged to service users by reselling (processed, perhaps anonymised) data.
P→C	Legal constraints on conduct	Positive	Race to top in privacy policies: countries, industries and firms competing via privacy provisions, policies and performance to attract privacy-aware customers and businesses. Self- and co-regulation: industry groups adopting privacy-friendly codes of conduct or standards in lieu of regulation, to capture the advantages of flexible and effective protection matched to changing circumstances, possibly with government enforcement support.
		Negative	Race to bottom in business location: countries competing to attract businesses by minimising privacy law compliance burdens and the strength of protection. Fixed and marginal compliance costs –costs may inhibit entry and exit (reducing innovation and efficiency) or be passed on to consumers without the opportunity for meaningful choice.
I→P	Response to user demand for privacy	Positive	Privacy-enhancing technologies: technological solutions to privacy protection, developed in order to provide cost-effective compliance e.g. privacy by design.
		Negative	Data-mining: use of big data analytics and data mashing (combining multiple data sources) in ways that allow *approximate targeting* or allow anonymisation to be reversed. Behavioural profiling: processing of personal data to produce targeted offers, environments and other services with the aim of increasing the costs of consumer choice.
P→I	Innovation to ease compliance or bypass provisions	Positive	Anonymous profiling (Article 15 of Directive 95/46/EC): the development of tools that increase the effectiveness of advertising and targeting in ways that do not involve the identification of individuals
		Negative	Anonymous profiling (Article 20 of proposed Regulation) provisions that prevent specific activities independently of whether they result in or depend on identification.

Link	Example	Direction	Detail
C→I	Innovate or die	Positive	Patent races: use of competitive forces to increase pace and utility of innovation
		Negative	Predatory innovation: IPR protection used to exclude rivals, preventing innovation or increasing its cost. Lock-in – restricting portability and interoperability to prevent search, limit competition.
I→C	Improved productivity, market power	Positive	Extensive competition: developing new goods and services Intensive competition: reducing costs and increasing performance of existing services
		Negative	Patent thickets and pools: patents structured to prevent entry, facilitate collusion Interoperability barriers: preventing rivals from sharing access and extending market power to lock in or exclude suppliers and resellers or customers.

2.2.2. The data processing value network

Any consideration of the impact of policy on economic outcomes must start from a rough definition of the relevant industry (ies) and market(s). The boundaries of the data processing industry are indistinct and variable. Here, we indicate the different sources of data processing demand and supply.

Personal data are used by firms in various ways. An increasing range of firms across many sectors depend on processing of protected personal data for a variety of purposes.

The demand side of the data processing market includes a range of business uses, models and associated stakeholders:

- Efficient management of their operations - by analysing some types of personal data it is possible to drive efficiencies in storage, processing e.g. through Customer Relationship Management – CRM;
- Identification, development and (in some cases) marketing and delivery of services other than data processing ('downstream services' in this document) to their users. For example many B2C web-based email providers[39] will analyse users' email traffic data in order to develop heuristic models to allow filtering of spam, messages containing malicious code and other unwanted or dangerous messages.
- Direct value capture/monetisation by reusing data or providing them to third parties for reuse, sometimes using the proceeds to provide 'free' or subsidised downstream services, e.g. via ad-supported business models[40] where services are provided for free to consumers in (sometimes implicit) exchange for monetisation by the service provider of access to those customers.

Therefore, the demand for personal data collection, storage, management, curation and processing is high and likely to increase, augmented by non-commercial demand from data subjects, who themselves store and process increasing amounts of their own data.

[39] E.g. Yahoo!

[40] Examples include Google search services and Facebook social networking; advertisers are willing to support these services because profile-influenced advertising provided is more profitable than untargeted advertising; this in turn allows providers to invest in continual innovation.

Certainly, the European data protection legal framework and the privacy preferences that helped to shape it are powerful influences on this demand.

The supply side of the data processing market includes a range of business models and associated stakeholders:

- Internalised all-in-one data control and processing - firms and other entities who provide their own data processing services;
- Outsourced data processing with integrated compliance - firms who supply data processing to others and who include privacy compliance bundled with other services;
- Outsourced data processing with retained compliance - firms who supply data processing services to data controllers who remain responsible for their own compliance (e.g. by uploading only encrypted data);
- Third-party compliance services - firms who offer privacy protection, privacy-enhancing or compliance certification services either directly to data controllers or as a third-party application available on data processing platforms.

But the growing demand for data processing goes well beyond personal data. Therefore, data protection provisions affect both the conditions under which these data processing stakeholders operate and the allocation of demand and supply across the different models, as identified above. Many entities, therefore, find themselves operating under one or more of the demand and supply roles identified above; data, data processing and compliance certification and other services are exchanged among them according to an increasingly-complex web of interactions. This complexity and fluidity motivates the use of the term *data processing value network*, which is used in this document in preference to simpler – but potentially misleading – terms such as data processing sector, industry or value chain.

2.2.3. How data protection provisions affect market outcomes

The data protection provisions prevent certain activities, change the costs of others and protect or even change consumer attitudes towards privacy and the privacy policies and performance of different service providers[41]. In this way, they affect: the structure of the data processing value network (who obtains services from whom); the level and profitability of activity; the resulting pace and direction of innovation; and the effectiveness of privacy protection. Critical aspects of the provisions in this respect include:

- Balance of business: data processing firms for whom personal data makes up a small or avoidable portion of their workflow (e.g. cloud platform providers) may (have) respond(ed) to data protection provisions by dropping that line of business, in the process depriving personal data controllers of associated cost and performance advantages[42].
- Economies of scale and scope: national differences[43] in data protection implementation and enforcement militate against internalised and retained-compliance models for multi-regional firms, but in favour of localised suppliers of integrated or third-party compliance services. Trans-European or globalised firms whose downstream services depend heavily on personal data will find national differences a barrier to entry and/or an incentive to

[41] See Asay (2012) and Westin (2003).

[42] This is difficult to evaluate empirically, since by definition those who process personal data are those for whom the benefits outweigh the costs and other burdens.

[43] Between Member States under 95/46/EC and between European and non-European countries under the Regulation.

limit cross-border operations to a cluster of countries with highly similar data protection provisions.

- Fixed vs. variable compliance costs: requirements that can be met by a once-and-for-all change (e.g. privacy-by-design) tend to favour larger entities – who can spread the costs over a large client base - and inhibit entry, especially by small firms. In contrast, variable compliance costs (incurred on a per-record or per-user basis) do not inhibit entry or exit (since they vary with scale of operation and stop when activity stops), but do tend to be passed on in market price or create cost disadvantages. However, a *privacy as a service* business model might emerge in which larger firms invest in one-off costs of privacy protection and resell privacy-enhancing services. The firms who buy these services can thus convert regulatory compliance from fixed (CAPEX[44]) to variable (OPEX[45]) cost. This depends on innovation (of suitable models for providing compliance to third parties) and affects competitiveness. The degree to which it is taken up depends on the (technological and operational) costs of attaining certified compliance *capability* and the legal and regulatory liabilities associated with actual *performance*.

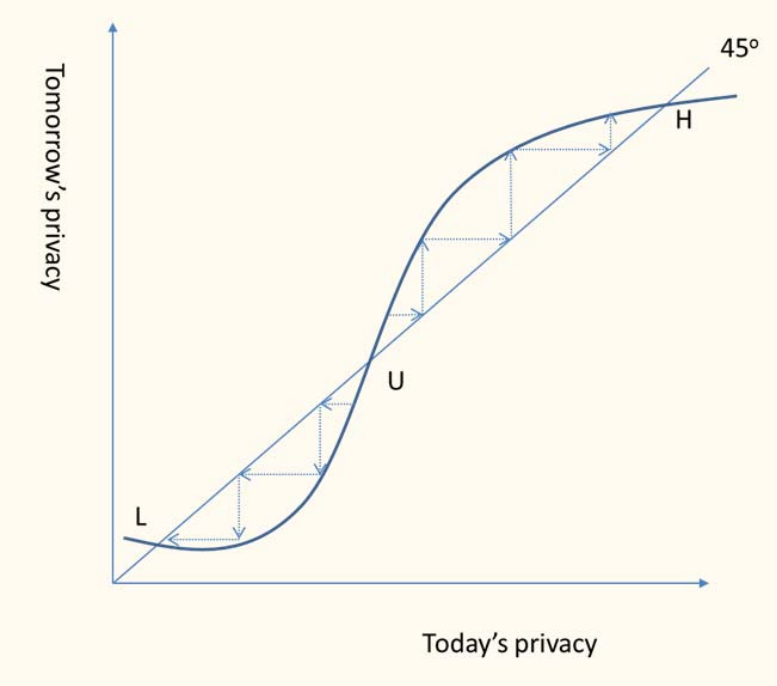
The second comment concerns the way data protection provisions affect market participation and behaviour. Compliance with the data protection provisions is likely – in the first instance at least – to be costly to compliant firms. But it brings hidden advantages. As noted in the first study, stated and actual individual privacy preferences and willingness to pay for protection often differ; this has been attributed in part to the counterfactual nature of the threat and the protections available. Thus, there is a chicken-and-egg relationship between demand for and supply of privacy-respecting. In this case, there are likely to be two very different stable market regimes, reflecting either low demand matched with low levels of protection or high demand for privacy met by data controllers and processors at efficient[46] prices. The following diagram illustrates these possibilities. The horizontal axis shows today's level of demand for privacy protection; the vertical axis shows tomorrow's demand. The relation between the two is S-shaped, because the demand for privacy protection (which we assume is priced at cost) will depend on the level of protection currently available; when most service providers offer only minimal protection, users are not aware of the threat (either because their awareness has not been raised by competitive advertising or because there are few alternatives) and firms have little incentive to compete in this way. As the level of protection increases, consumers notice it more, and it becomes more profitable for firms to compete on the basis of privacy, leading to the steep increases in the middle of the diagram. Eventually diminishing returns set in as users are able to secure privacy protections sufficient to meet their informed needs and the curve levels out again. The points where the curve meets the 45° line are equilibria – privacy protection levels that persist over time. Points where the curve cuts the 45° line from above (L and H) are *stable* – slightly higher levels of protection will not be sustained, and slightly lower levels will lead to greater demand. The middle intersection (U) is unstable.

[44] Capital expenditure (CAPEX) is business expenditure required to secure future benefit e.g. creating new data centres

[45] Operational expenditure (OPEX) is business expenditure required for current operations e.g. extra payment to a cloud service provider for privacy-compliant data handling.

[46] i.e. prices for privacy protection that equate marginal costs of provision and data subjects' willingness to pay.

Figure 2: The dynamics of privacy



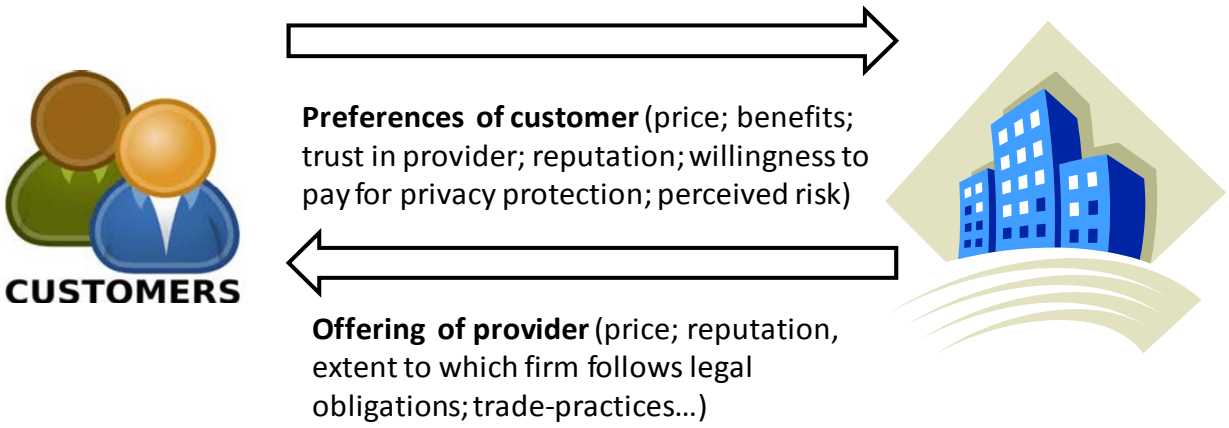
In this case, higher – and more uniform - levels of mandatory protection can kick-start a positive feedback between increased awareness and sensitivity on the part of the public and increased protection offered by (potential) data controllers and processors – in other words, a statutory minimum level set above U will lead to the high-privacy equilibrium H.

2.2.4. Measuring these effects

The potential market impact of privacy rules (broadly stated) can be inferred from the size of the affected sectors and lines of business, the impacts of privacy breaches on firm value and more broadly-based assessments of the holistic or *public good* influence of reputations relating to privacy safeguards. This section provides a preliminary assessment by recapping the calibration developed in the previous sections and briefly summarises some findings from the empirical literature on stock market impacts and the business literature on the impact of IT performance.

Primary quantitative evidence of the extent to which privacy – and privacy laws – affect competitiveness and innovation, expressed financially via theory of the firm, is hard to come by. As noted in Table 3, this effect flows through a range of channels, and combines positive and negative effects, leading to weak econometric relationships, even when the effect of confounding factors can be taken out of the picture.

Figure 3: Examples of signals to and from customer and provider



However, the empirical evidence can be interpreted on the basis of a simple logic model: privacy laws increase the costs of careless treatment of personal information and may inhibit data controllers' and data processors' ability to monetise their access to data subjects' information. Therefore, incidents such as privacy breaches impose immediate costs (reparations, notification, legal liability and sanctions, technological improvements) and may carry a longer-term risk of loss of reputation. These effects are, of course, uncertain; stock market prices can provide a rough indicator by pricing the risk. They can be examined in various ways; the literature has concentrated on event studies following particular incidents – which naturally emphasise the direct or cost consequences - and on interview-based studies looking at dispersed effects[47].

Despite its conceptual limitations, the use of stock market prices to measure the consequences of neglect of privacy can shed some light on the impacts of the Regulation on competitiveness and innovation, especially to the extent that compliance renders such breaches less likely, less common among firms in an industry, or more exceptional when and if they occur. This is particularly true because the proposed Regulation establishes a breach notification regime. Although beyond the scope of this report, case studies would be instructive in illustrating the extent to market shares and the willingness of firms to comply and to innovate are driven by consumer expectations and management fear of loss of shareholder value (caused by disclosure). For example, disclosure may differentially affect established companies rather than start-ups. In the US certainly, many start-ups remain private firms until they have amassed enough (potential) shareholder interest to file an IPO. Moreover, the way firms respond to data breaches may determine whether the impacts are positive or negative[48].

The new economics of privacy has been analysing econometrically the relation between stock market prices and data breach notifications to determine whether disclosure hits companies where it hurts – in their wallet. It is obvious that this forms the theoretical basis for the breach notification regime in the proposed Regulation: the forcible disclosure of breaches should encourage regulated firms to take privacy seriously if they are to avoid

[47] A more detailed econometric study could be conducted using a full set of incidents and measures of their visibility, together with a full panel of firms delivering similar services under different privacy protection regimes; while the data and methods are, in principle available, such a study goes beyond our current scope.

[48] This point was made by a representative of a large EU Telco, and resembles the well-known good news/bad news effect of dividend announcements on stock prices.

substantial fines and adverse stock price movements, raising costs of capital and reducing the value of equity[49].

Acquisiti, Friedman et al (2006) analysed a broad data set to show that a privacy breach affects stock market price strongly on the day of the breach but that this effect rapidly decreases and loses statistical significance.[50] In a survey of 427 senior level decision-makers for the 2012 IBM Global Reputational Risk and IT Study[51], 61% of respondents said that Data Breach/Data Theft/Cybercrime represented the biggest IT-based threat to firm reputation.

But it cannot be assumed either that market valuation tracks consumer valuation, let alone willingness to pay for better protection. In the same study, only 13% of respondents identified stock price as "very much" affected by IT risks: nearly half (46%) indicated that customer satisfaction was the most important business element affected by IT risks.

Therefore, there does not appear to be strong evidence that breach notification provides effective or proportional incentives for firms to take better care of personal data by operational changes or innovation[52]. In any case, the separation between individual firm and sectoral impacts is not clean; incidents, and especially repeated or dispersed incidents, can create a form of reputational contagion or collective loss of confidence. This possibility of collective punishment can weaken the incentives of individual firms.

Another independent variable to explain changing market valuations of groups of firms is policy intervention; policy statements, cases launched by Data Protection Authorities (as with the 2011 cluster shown in Table 6) or other pronouncements intended (somehow) to send a signal to the market. But these cannot be treated symmetrically; European regulators use different types and combinations of enforcement and informational strategies, and will likely continue to do so under the proposed Regulation. Some adopt a market shaping approach, targeting particularly egregious violations whilst others may seek to demonstrate effectiveness by publishing extensive statistical data on notifications, enforcements etc.

[49] This argument can run in reverse; mandated disclosure can lead to inefficient forms of protection designed to minimise shareholders' legal exposure rather than data subjects' legitimate interests.

[50] Acquisti et. al. (2006).

[51] IBM (2012)

[52] Another potential perverse effect arises if a firm's innovative activity links consumer expectations more strongly to privacy performance; the recent massive TK Maxx data breach produced a sharp, but very short-lived drop in stock value, while a much smaller – and less serious - breach by a financial services firm whose business model emphasised privacy protection depressed market capitalisation by as much as 25% for over 6 months [Gatzlaff and McCullough (2011)].

Table 6: Major privacy related events in Europe relevant to Internet innovation, 2008 - 2012

Date	Event	Description
October 2008	T-Mobile losses disk containing 17m customer records	Breach
May 2008	Deutsche Telekom executives involved in privacy breach	Breach
April 2009	European Commission issues infringement proceedings against UK for implementation of rules on electronic privacy	Policy Statement (EU)
May 2009	European Commission issues public consultation on privacy and data protection	Policy Statement (EU)
December 2009	Article 29 WP issues opinion on The Future of Privacy - Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal	Policy statement (EU)
2009	Commission criticises UK ICO for statement on Phorm	Intervention (EU)
December 2009	Facebook comes under criticism for introduction of complex privacy controls	Innovation
February 2010	German Consumer protection minister advises against StreetView	Intervention (MS)
February 2010	Art 29 WP issues Opinion on Concept of Controller and Processor	Policy Statement (EU)
April 2010	FCC indicates Google Wi-Fi Snooping legal	Intervention (national)
April 2010	Commission releases COM 609 (2010): "A comprehensive approach on personal data protection in the European Union"	Policy Statement (EU)
May 2010	Google announces code collects Wi-Fi details	Breach
June 2010	ICO issues statement on NHS data breach	Intervention (MS)
June 2010	UK Police investigate Google Wi-Fi	Intervention (MS)
June 2010	Art 29 WP issues Opinion on Behavioural Advertising	Policy Statement (EU)

Date	Event	Description
July 2010	UK ICO clears Google Wi-Fi snooping	Intervention (MS)
October 2010	Facebook Apps found to leak data	Breach
Jan 2011	ENISA issues report on data breach notifications in electronic communications sector	Intervention (EU)
March 2011	Court in Montpelier rules Google needs to make records 'disappear'	Intervention (MS)
March 2011	CNIL fines Google for inadvertently collecting Wi-Fi data	Intervention (MS)
April 2011	Apple come under scrutiny for storing Location based data on iPhones and iPads	Breach
April 2011	Google announces no new capture of StreetView in Germany	Innovation
May 2011	Sony declares data loss of 25m users (including "thousands of European debit cards")	Breach
May 2011	Sony declares loss of 77m PlayStation Online users	Breach
May 2011	KPN reveals DPI usage	Breach
May 2011	Trident Media Guard leaves open IP addresses	Breach
May 2011	Transposition of revised e-Privacy Directive required	Intervention (EU)
Mid 2011	Regulators from EU and US conduct intensive meetings	Policy statement (EU)
May 2011	Commissioner Reding notes need for common approach	Policy statement (EU)
June 2011	OPTA concludes grounds for more concern over KPN DPI monitoring	Intervention (MS)
July 2011	Art 29 WP statement on Google to reduce retention period for unblurred data	Intervention (EU)
July 2011	Facebook enables facial recognition	Innovation
July 2011	Art 29WP issues Opinion on Consent	Policy Statement (EU)

Date	Event	Description
July 2011	Eurobarometer report on Data Protection and Electronic Identity in the European Union	Policy Statement (EU)
July 2011	Swiss Court orders Google to manually blur all faces in StreetView	Intervention (national)
January 2012	Announcement of proposed General Data Protection Regulation	Policy statement (EU)
September 2012	Google settles FTC privacy case for 22.5m	Intervention (national)
September	Betfair loses personal data of 2.3m customers	Breach
September 2012	Facebook faces fines in Ireland	Intervention (MS)
September 2012	Facebook denies privacy breach	Breach (alleged)
October 2012	Google given four months to improve privacy policy	Intervention (MS)

Moreover, breaches or regulatory action are more likely to affect stock prices if the market believes that they will lead to substantial damage to a company's reputation as a trusted agent and thus to changes in market share and profitability. In other words, a company that bases its marketing on privacy and/or security is more likely to suffer sustained stock price damage than one where privacy or security are less important to revenues[53]. Trust is bound up with many things - not least whether a company takes seriously its adherence to privacy principles or indeed legal obligations. From the perspective of the new customer (arguably the most important type of customer given the emphasis on innovation) other indicators may be equally influential on trust: for example whether the firm has easily accessible pre- and post- customer service (in reality or according to peer reviews and ratings).

Finally, the way a breach or even an adverse regulatory action can affect the fortunes of the firm in the asset market and in the markets where its trading profits arise may depend critically on the way the event is handled (see footnote 48). A forthright, pro-active and transparent response may actually help the firm. This has several implications:

- It may pay a firm to generate 'small crises' in order to demonstrate its commitment to data protection principles;
- A firm may invest in a reputation for scrupulous privacy protection in order to milk the reputation at a later date;
- Firms may offer – or highlight in their advertising – other features in order to reduce consumer sensitivity to privacy performance (in effect using potentially cheaper or more

[53] This could happen if privacy breaches do not harm customers (because the data are less sensitive or because users have adopted data minimisation, encryption, etc.) or if customers have little meaningful choice.

durable ways of securing market share to effectively lighten their data protection responsibilities[54]);

- The extent of effective compliance with data protection rules will likely depend on the degree to which a breach or other adverse event (including regulatory sanction) affects the reputation of individual firms as opposed to the industry as a whole – this in turn can strengthen or weaken incentives to adopt collective compliance measures[55] such as standardisation, information exchange, etc.; and
- Private and publicly-listed firms, firms with different degrees of leverage in their financial structure, large and small firms and firms operating in or far from the markets where their assets are traded are therefore likely to respond to market incentives in very different ways.

Must privacy and innovation be forever posed as conflicting values? Cohen (2012) argues that many portray privacy as being an outdated value standing in the way of "cutting edge imperatives of national security, efficiency and entrepreneurship".[56] However, she advances the case that innovation and privacy should go hand in hand: with freedom from surveillance comes the freedom to play and experiment – the *conditio sine qua non* of innovation.

2.3. Legal and Regulatory context

This section describes and analyses the current (Section 2.3.1) and proposed (2.3.2) legal contexts and compares them to the analogous privacy protections in the United States (Section 2.3.3). For the sake of completeness, a more detailed comparison of the relevant legal texts in Directive 95/46/EC and the proposed Regulation is given in ANNEX 3.

2.3.1. The current Directive and its implementation across Member States

The current Directive has been implemented by all 27 EU Member States. The implementation at a national level, however, left some room for interpretation by the Member States and resulted in slightly different requirements and levels of protection throughout the EU. For instance, the response times for data subject access requests (SARs) vary between 8 business days (Slovakia) and 8 weeks (Austria) or 'without (undue) delay' without further specification or limitation (Finland, Italy, Norway). The lack of a uniform implementation is problematic for companies who have their businesses in several countries. The fragmented data protection landscape leads to legal uncertainty and, in particular, the complexity of the provisions concerning transfer to third countries is seen as an impediment to the operations of economic stakeholders.[57] Also, diversity is a drawback from the perspective of innovation and the introduction of new products and services, which are related to or based upon the processing of personal data. These differences can be substantial; Figure 4[58] shows the variation in the length of time taken to respond to subject access requests (SARs). Table 7 shows in addition the variation in the wording of subject rights and data controller obligations.

---

[54] For example, a firm might offer free or low-cost services hoping that customers would accept reduced privacy protection; the firm would generate greater sales volumes and save on privacy protection cost.

[55] In effect, a strong collective reputational effect encourages free-riding while a strong individual reputational effect discourages cooperation to manage privacy risk. [Cave et. al. (2008)].

[56] Cohen (2013).

[57] European Commission (2012a)., p. 4.

[58] Source: European Commission status of Implementation of Directive 95/46/EC http://ec.europa.eu/justice/data-protection/law/status-implementation/index_en.htm.

Figure 4: Implementation of Subject Access Request (SAR) rules

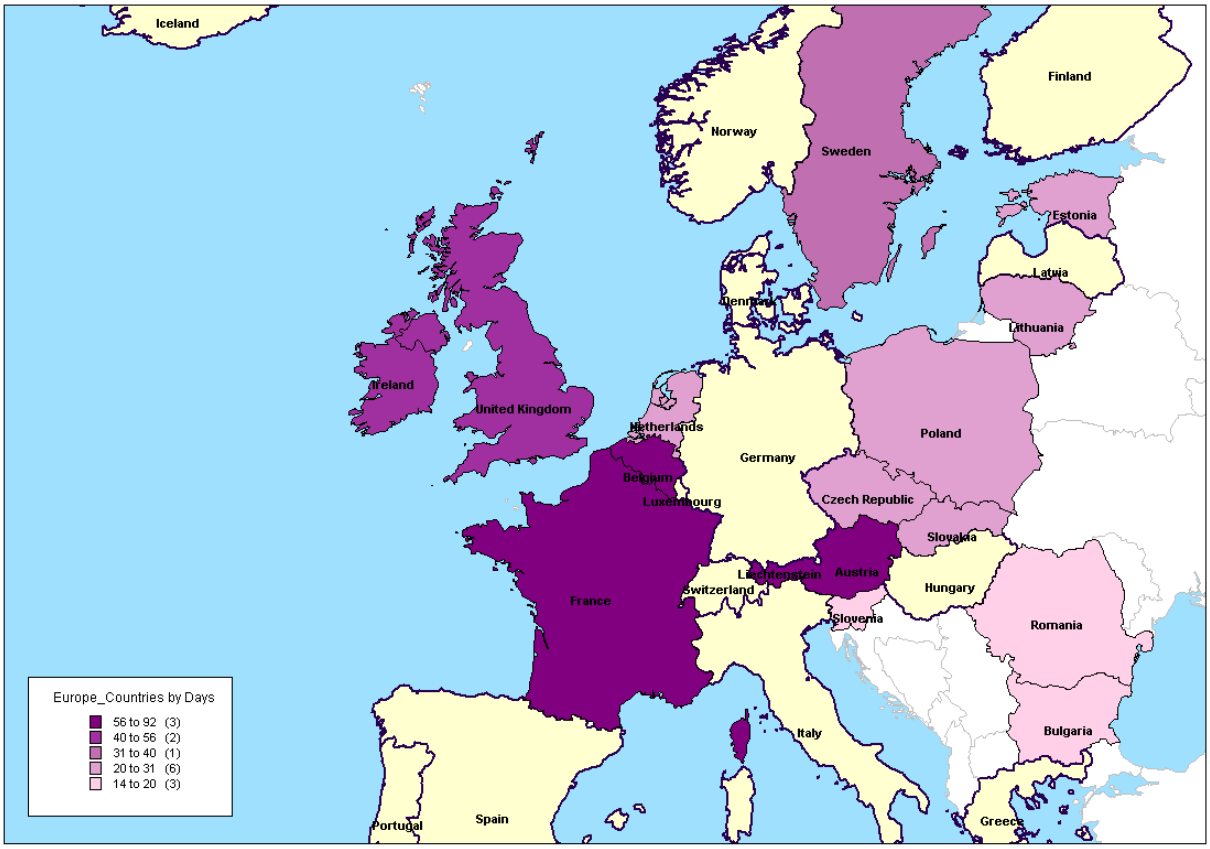


Table 7: Regulatory period for response to Subject Access Requests (SARs)

Country	Time to react (days)	Qualitative threshold
Austria	56	Within eight weeks of receipt of the request
Belgium	?	link not working
Bulgaria	14	
Cyprus	?	link not working
Czech Republic	30	
Denmark	-	Without delay. If a reply is not received within 4 weeks of receipt of the request, the controller shall inform the subject of the grounds for delay and the time at which the decision can be expected to be available.
Estonia	20	The Data Protection Inspectorate shall decide to register or refuse to register the processing within twenty working days as of the date of submission of the registration application.
Finland	-	Without undue delay
France	?	Two months
Germany	-	Period not specified in federal data protection law
Greece	-	Without undue delay and in an intelligible and express manner
Hungary	?	(in Hungarian only)
Ireland	40	As soon as may be and in any event not more than 40 days after compliance by the individual
Italy	-	Reduce the delay for the responses
Latvia	-	No timeframe specified
Lithuania	30	Upon receiving a request from the data subject, the data controller must send a reply to him within 30 calendar days.
Luxembourg	-	Upon application to the controller, the data subject or his beneficiaries who can prove they have a legitimate interest may obtain free of charge, at reasonable intervals and without excessive waiting periods:
Malta	-	The controller of personal data, at the request of the data subject, shall provide data without excessive delay and without expense.
Netherlands	28	Within four weeks

Country	Time to react (days)	Qualitative threshold
Poland	30	Within the period of 30 days, the controller shall be obliged to notify the data subject about his/her rights, and provide him/her with the information referred to.
Portugal	-	The data subject has the right to obtain from the controller without constraint at reasonable intervals and without excessive delay or expense.
Romania	15	It is the data controller's obligation to communicate the requested information, within 15 days of receipt of the petition.
Slovakia	30	The controller shall satisfy the requests of the data subject under Section 20 and notify him in writing at the latest within 30 days of receipt.
Slovenia	15	No later than 15 days from the date of receipt of the request.
Spain	-	Unspecified
Sweden	?	?
United Kingdom	40	40 days

2.3.2. The proposed new Regulation

As indicated, the proposed Regulation contains a number of changes. Data protection by design and privacy enhancing technologies are important elements throughout the proposed Regulation. In these elements, the underlying data protection principles, such as collection and use limitation and the accountability principle[59] are reflected. In order to simplify processes for compliance, "organisations would only have to deal with a single national data protection authority in the EU country where they have their main establishment. Likewise, people can refer to the data protection authority in their country, even when their data is processed by a company based outside the EU[60]." Furthermore, EU provisions must apply if personal data is handled abroad by companies that are active in the EU market and offer their services to EU citizens. In this respect, consumer organisations across the EU and US (e.g. the Transatlantic Consumer Dialogue) have welcomed the proposal for tightening provisions. Some US consumer organisations use the example of the EU initiative to push for enactment of the US Internet Consumer Privacy Bill of Rights.

For the purpose of this briefing paper, three specific provisions will be discussed. These provisions concerns measures based on profiling, the documentation of processing activities and responsibilities, and the transfer of personal data to third countries. Each section begins by quoting the relevant text from the proposed Regulation.

[59] These principles were originally laid down in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23 September, 1980.

[60] European Commission 2012c

Measures based on profiling (Article 20)

Article 20

1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.

2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing: (a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or

(b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or

(c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards.

3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal data referred to in Article 9.

4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.

Article 20 lays down the right of users not to be subject to measures based on profiling, complementary to the right to object to processing of personal data. The use of profiling techniques for automated decision making processes concerning an individual, such as inclusion or exclusion from options or content, is, thus, prohibited.

The scope of the proposed Article 20 is broader than the scope of the earlier provision in Article 15 of the Directive 95/46/EC. Under the current Directive, it is possible to create profiles providing the subjects cannot be identified. Because Article 20 of the Draft Regulation refers to *natural person* rather than *data subject*, profiling could be restricted regardless of whether data subjects could be identified and therefore whether the data would constitute personal data.

It now concerns measures based on profiling, instead of automated individual decisions. It seems that all kinds of advertising, inclusion and exclusion, etc., are *measures*, but may be subjected to discussion when called *decisions*. Measures stand for any action towards a goal.[61] Even though the exact scope of the terms *decision* and *measure* is unclear and not clarified in the proposal, measures seem to cover a much wider scope of activities. As a result, many more practices of automated processing are brought within the scope of the

[61] Costa and Poullet (2012).

provision. Moreover, the prediction of behaviour is indicated as a specific category of measures to be covered by the provision. A point of discussion remains with regard to the meaning of 'legal effects or significantly affects' resulting from these measures.

The advertising industry has emphasised the positive impact on the economy brought by targeted advertising practices. It is, thus, indicated that when it is assumed that targeted advertising is brought within the scope of this article and made impossible to function, the benefits will be taken away. A report on requests for evidence from the UK Ministry of Justice mentions a potential detrimental impact on an industry worth £15.9bn in expenditure.[62] Others see the provision as an opportunity to diminish unsolicited emails, which should have a positive economic impact[63] because of the reduced burden on information systems and reduced loss of working time spent on reading or deleting spam.

Profiling is seen as an important instrument to facilitate the provision of 'free' services. In this respect, advertisers promote a reading of the proposed Article 20 not as a prohibition on profiling but as a right to object to profiling. Moreover, numerous ICT services base the quality of their services on profiling, for instance, to provide recommendations to users by comparing their interests to those of other customers.

Profiling provisions also have repercussions for a number of other industries. These sometimes lament what they see as a one size fits all approach to profiling in the proposal. The financial sector, for instance, uses profiling measures to detect anomalous use of credit cards and fraud protection and argue that these measures might jeopardise using data in the interest of the consumer.[64]

Documentation in relation to protection requirements (Article 28)

Article 28

1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility.

2. The documentation shall contain at least the following information:

(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;

(b) the name and contact details of the data protection officer, if any;

(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);

(d) a description of categories of data subjects and of the categories of personal data relating to them;

(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;

(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of

---

[62] Summary of Responses to Call for Evidence on Proposed EU Data Protection Legislative Framework carried out by the Ministry of Justice, p. 23.

[63] Summary of Responses to Call for Evidence on Proposed EU Data Protection Legislative Framework carried out by the Ministry of Justice, p.23.

[64] Hill & Knowlton blog *"why should the financial sector care about data protection" at:* http://blog.hkstrategies.be/2012/03/why-should-the-financial-sector-care-about-european-data-protection-reform-2/

transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;

(g) a general indication of the time limits for erasure of the different categories of data;

(h) the description of the mechanisms referred to in Article 22(3).

3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority.

4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors:

(a) a natural person processing personal data without a commercial interest; or

(b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities.

5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative.

6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Article 28 specifies the contents of the documentation as required by Article 22 of the Regulation. It elaborates on Article 17(2)-17(4) of Directive 95/46/EC. The aim is to ensure compliance with the data protection requirements. In particular, the documentation is meant to be able to demonstrate compliance upon request and to have all responsibilities and processing activities documented. According to the Commission's proposal, these measures would cut red tape and save EU businesses billions of euros while enhancing their competitiveness. At the same time, non-compliant businesses, whether based in the EU or conducting business in the EU, could face fines up to 2% global turnover, which obviously displeases especially US firms.

Specific requirements that follow from this provision concern the relationships between businesses in the controller or processor layers. The level of detail in the proposed Regulation is seen as an administrative burden, so some organisations:

> *"support the proposal put forward by the European Data Protection Supervisor,[65] to introduce an obligation to keep an inventory of all processing operations that would encompass general information, namely the contact details of the controllers (and joint controllers and processors if applicable), the contact details of the data protection officer and the description of the mechanisms implemented to ensure the verification of the measures undertaken in order to ensure compliance. More specific information should be part of an additional obligation to inform data protection authorities upon request."[66]*

The delegated acts as mentioned in sub 5 of the provision allow for the drafting of specific requirements. These may be beneficial from an economic perspective, for instance, by allowing for standardised formats (also sub 6) and fewer obligations when certain requirements are met. As Mrs Viviane Reding, Vice–President for the Commission, stated at

[65] Opinion of the European Data Protection Supervisor on the data protection reform package, 7 March 2012.

[66] BEUC Position paper, Data Protection; proposal for a Regulation, p. 24-25.

the European Interparliamentary Committee Meeting on the EU framework, held in Brussels on 9 and 10 October 2012:

> *"As the Regulation is technologically neutral, the delegated acts will allow it to be flexible to accompany, not hinder, technological advancements without the need for a full reform of the Regulation".*

However, Data Protection Authorities are often worried about a power grab by the Commission through delegated acts (executive measures that can be taken by the Commission to address technological developments, for instance). The Article 29 Working Party has some reservations concerning delegated acts and stresses the need for a balance between the need for legal certainty and flexibility. In some cases, delegated acts may be helpful to provide legal certainty, whereas in other case, Guidelines provided by the European Data Protection Board (EDPB) may be sufficient.[67]

Transfer of data to third countries (Articles 6(1)(f) and 44(1)(h))

Art 6(1)(f)

1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: […]

(f) processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

Article 44(1)(h)

1. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may take place only on condition that:

(h) the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent or massive, and where the controller or processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations and based on this assessment adduced appropriate safeguards with respect to the protection of personal data, where necessary.

Today, a transfer of personal data from the EU to third countries requires establishment of an adequate level of data protection (Art. 37 et seq.), since data controllers have to ensure that the right to data protection of the data subject is not impeded. The newly proposed Article 44(1)(h) requires the data controller to assess the risks associated with the transfer of personal data to a third country which has no agreement in which the sufficient level of protection is recognised (Safe Harbour).[68] Article 44(1)(h) and Article 6(1)(f) of the proposed regulation extend the third country transfer provisions of recital 30 and 39, and

---

[67] Article 29 Data Protection Working Party, Opinion 08/2012 providing further input on the data protection reform discussions, 01574/12/EN, WP 199, p. 10.

[68] The EU-US Safe harbour agreement allows companies that comply with 7 principles (Notice, choice, onward transfer, security, data integrity, access, enforcement) to register as compliant with the EU Data Protection Directive. It has however been strongly criticised for not being sufficiently supervised. In particular, In April 2010, German data protection authorities issued a resolution requiring extra diligence for German data exporters interacting with US Safe Harbour-certified entities—effectively calling into question the sufficiency of the Safe Harbour program to meet EU guidelines—and threating possible sanctions.

Article 7(f) of the existing Directive 95/46/EC. After assessing the risks, appropriate safeguards have to be taken to ensure the security of the processing. The full responsibility for the data processing in the third country is, therewith, with the data controller.

In cases of data transfers to non-EU authorities or public bodies, it may not be necessary to establish this level of data protection. The exceptions include those already in place e.g., defending a claim or safeguarding the vital interests of a data subject. There is, however, a new exception that will ease data transfers to e.g. the US Department of Justice or the US Securities and Exchange Commission (SEC) in certain proceedings:

> *"where the transfer is necessary for the purposes of the legitimate interests pursued by the controller or the processor, which cannot be qualified as frequent, or massive ..." (Art. 44 (1) h).*

Under Directive 95/46/EC, the legitimate business interest of the data controller could not be used to justify transferring data for processing in third countries if those countries did not provide adequate protection. The proposed Regulation does allow such transfers if there is a legitimate business interest, subject to the documentation requirements described above in relation to Article 28 (namely documentation of data processing and the contact details of responsible parties). So, compared to Directive 95/46/EC, processing (transfer) to third countries is now allowed under responsibility of the data controller, whereas under the Directive it was only allowed on a limited number of conditions. Equivalent levels of protection can also be established by means of existing mechanisms such as Standard Contractual Clauses or Binding Corporate Rules. Implementing binding corporate rules will be extremely simplified as the Regulation provides specific guidance for the content of such rules and requires approval of these rules by only one EU data protection supervisory authority.[69] This means that there are more options for transfer of data, but that responsibilities have increased accordingly.

2.3.3. Comparison to the US

Overall comparison

When compared to the US, the EU has a different approach towards privacy and data protection rights. At an EU level, the rights are implemented in the Charter of Fundamental Rights of the European Union, in Articles 7 and 8 respectively and the European Convention on Human Rights and Fundamental Freedoms contains the right to respect for private and family life in Article 8. Moreover, national constitutions of the EU Member States recognise the right to privacy. In the US, privacy in general[70] is not protected at the Federal Constitutional level. Nevertheless, a number of US States have implemented the right in their State Constitutions. Besides, the OECD "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" have provided a background for data processing in the US as well.[71] In February 2012, the White House presented their views on privacy protection including a Consumer Privacy Bill of Rights.[72]

---

[69] IT Law group commentary on DPR http://www.itlawgroup.com/resources/articles/230-proposed-eu-data-protection-regulation-january-25-2012-draft-what-us-companies-should-know-.html

[70] As noted in Chapter 1, US privacy protections in respect of electronic data tend to be defined in relation to specific data types and/or sectors (e.g. data pertaining to children, health or credit data, etc.). A brief overview of eleven relevant US Federal laws that regulate data management and affect privacy is provided in Annex C.

[71] As an OECD Member State, the United States has enacted privacy laws to provide a harmonised framework in the interest of economic development http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[72] US Government (2012).

The approach towards the right to privacy from an enforcement perspective is different. While in the EU, the right as such or specific parts as implemented in data protection laws can be invoked, the US usually approaches the right from the angle of consumer protection. Unfair practices or conflicts with the Fair Information Principles[73] affect the consumer, so there has to be protection against businesses. This is also the reason why the Federal Trade Commission (FTC) plays an important role in the regulation of privacy and data protection related issues, such as profiling and monitoring practices.

Due to the different approaches, the EU provisions cannot be applied to US businesses without complementing and/or reciprocal provisions on the US side. Since there is no data protection at a federal level in the US and the generally applicable common-law tort of invasion of privacy only helps to compensate harm a posteriori, the US Department of Commerce, together with the European Commission, developed a Safe Harbour Framework.[74] US companies can declare their compliance with EU data protection standards by joining the Safe Harbour Agreement. When doing so, US companies are allowed to process personal data related to EU citizens for the execution of their businesses.

Compliance is indirectly enforced. Members of the Safe Harbour arrangement have to certify their adherence to the programme by annual declaration to the Department of Commerce and by publication of a privacy policy statement. The FTC has the power to investigate allegations of false self-certification. An American firm that breaches its data protection commitments cannot be sued in the U.S. for breach of privacy or data protection provisions as it bears no legally-defined data protection duties[75]. However, if the firm belongs to the Safe Harbour, the FTC can investigate its public statements and determine whether they were unfair and deceptive.[76] The system of a Safe Harbour Framework as well as Binding Corporate Rules both have been supported by the FTC.[77] In particular, the approach to require specific firms that want to do business involving data from EU citizens to be complaint with EU Data Protection Legislation as opposed to requiring this from the entire US seemed a welcome solution.[78]

Detailed US Privacy Provisions

This section describes a selection of sector- or data-specific US Federal laws that protect or modify privacy rights. As noted in Chapter 1, the US has a range of laws regulating data management (e.g. HIPAA, HITECH, GLBA, SOX, and FISMA). They do not specifically restrict data location, but their national scope may influence the decisions of data controllers. In particular, there may be concerns arising from regulations that give government or private parties access to stored data. These include the following.

a) Access by government

ECPA (the Electronic Communications Privacy Act[79]) provides some protection against government access to electronic information stored in devices owned by third parties (e.g. Internet service providers) including electronic mail and other computer information. However, the privacy protections provided by ECPA for other data management

[73] E.g. as stated in Federal Trade Commission (1998).
[74] Bodogh (2011).
[75] Except sector-specific obligations as noted in section Detailed US Privacy Provisions.
[76] Birnhack (2008).
[77] Serwin (2010).
[78] Schaffer (2002).
[79] Burnside (1987).

activities (e.g. those used in Cloud Computing) are difficult to predict. Thus, it is really difficult to assess the protections provided by the ECPA in a way that allows meaningful comparison with European law.

EGA (e-Government Act) is a law that seeks to accelerate and harmonise US government use of information technologies. Section 208 of the EGA requires all federal agencies to conduct *privacy impact assessments* (PIAs) for all new or substantially changed technologies that collect, maintain or disseminate personally identifiable information (PII), or for a new collection of information that is collected, maintained, or disseminated using information technology.

FISMA (Federal Information Security Management Act) seeks to provide "a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets," and also to "provide for development and maintenance of minimum controls required to protect Federal information and information systems." It does not apply to the government systems most likely to contain personal information (e.g. routine personnel files), but is notable in mandating an annual compliance report that covers inter alia the agency's privacy policies.

UPA (The USA PATRIOT Act[80]), as originally enacted in 2001 and amended in 2005, includes provisions allowing FBI access to any 'business record' (which may include data protected under the European framework). Although a court order is required, FBI authority under the UPA is sufficient to extend to records maintained by Cloud provider, so Cloud users' privacy can't be protected.

b) Access by private parties

CCPA (Cable Communications Policy Act[81]) protects cable television subscriber records but does not directly prevent use of third party data processing service providers.

FCRA (Fair Credit Reporting Act[82]) limits use of credit reports to a 'permissible purpose' and compels certified erasure of many data after a specified period. However, if a creditor stores a credit report with a Cloud provider and a third party obtains the report from the Cloud provider the legal limit on use could be violated.

GLBA (Gramm Leach Bliley Act[83]) prevents financial institutions from disclosing consumers' personal financial information to unaffiliated third parties, but does not restrict disclosure to (ICT) service providers.

HIPAA (Health Insurance Portability and Accountability Act[84]), as the name implies, controls personal health data; it defines who can view stored data and when the data must be destroyed. It imposes only partial limits on compelled disclosures. For instance, a legal demand by a private party to a Cloud provider for disclosure of protected health information would lead the users' privacy information to be disclosed.

HITECH (Health Information Technology for Economic and Clinical Health Act) is a recent statute intended to extend the list of security and privacy provisions in HIPAA[85], by adding a data breach notification provision for electronic health records, requiring public notification (via the media) if more than 500 people are affected by a release of 'unsecured'

[80] McCarthy (2002).
[81] Parsons and Frieden (1998).
[82] McNamara (1977), Camden (1989), Weitzner et. al. (2008).
[83] Akhigbe and Whyte (2004).
[84] Dwyer et. al. (2004).
[85] http://www.cms.hhs.gov/regulations/hipaa/cms0003-5/0049f-econ-ofr-2-12-03.pdf.

data. It is notable as the first US statute explicitly to refer to encryption as a means of securing data.

SOX (Sarbanes-Oxley Act) defines which business records a company must store and for how long; these may include personal data. While laws like HIPAA is squarely concerned with data privacy (access to at least some kinds of personal data), SOX is concerned with data permanence and authenticity, requiring data controllers to prove that stored data have not been altered between deposition and retrieval. This separation (of requirements and contents) contrasts sharply with the EU framework in which data integrity and data access are considered together.

VPAA (Video Privacy Protection Act[86]) limits some disclosures of customer data. Service providers' terms of service sometimes allow providers to see, use, or disclose information and may lead to a violation of the law. Whether the increased risk of privacy violation outweighs the costs of ensuring compliance (e.g. by changing SLA terms) is an empirical question for which adequate data do not exist.

[86] EPIC.org, "Video Privacy Protection Act," http://epic.org/privacy/vppa/.

3. CASE STUDIES

3.1. Introduction

The previous Chapter described the legal provisions and the principles underlying them. This provides a foundation for analysing the way these provisions are understood by the stakeholders, influence their actions and ultimately affect competitiveness and innovation. We now turn to this topic, which we explore by means of four concrete perspectives on the operation of the Data Protection Directive and proposed Regulation:

- Profiling, Behavioural Advertising, Cookies and Social Media;
- Big Data;
- Cloud computing; and
- Privacy-friendly technologies (PETs).

These do not constitute cases in the conventional sense because they do not correspond to distinct market segments, technologies or business models. For instance, Profiling often entails analysis of very large data sets; such data tend to be stored in the cloud, and may even be manipulated there to enable smaller enterprises to make use of state of the art hardware and software; accompanying encryption and other protective technologies, or anonymisation/pseudonymisation techniques to allow the data to be processed and transferred constitute privacy-enhancing technologies.

These perspectives do provide complementary insights as to how the provisions of the Directive and Regulation are perceived and how they are expected to affect competitiveness and innovation. Moreover, the individuals interviewed and surveyed to gather evidence (and much of the literature consulted) reflected one or another of these perspectives. For this reason, we continue to refer to them as cases.

The data processing value network (see Section 2.2) is highly diverse; although the EU privacy protection regimes applies across the board, the competitiveness and innovation impacts of its provisions are highly sector-dependent. In particular, they strongly reflect the ways electronic personal data are collected, managed, protected and exploited. Therefore, the effects of the current and pending provisions are likely to differ. Moreover, different domains of data processing (in the broad sense) are associated with a range of current and emerging economic sectors. To adequately reflect this richness, and to throw into sharp relief the different effects of privacy protection in different contexts, we organised our evidence collection according to a set of relevant cases. Of course, the interviews, survey and literature were not confined to individual cases, and the cases themselves overlap to a degree. Therefore, the findings of this chapter also reveal both interactions among different sectors of the data processing industry and general principles spanning those sectors.

Each case study is organised along the same lines: a description of the nature of the case and an overall portrait of the associated economic activity; an assessment (based on desk research, the survey and key informant interviews) of the impacts of the current and proposed provisions organised in terms of automated processing, data controller responsibilities and data transfer; an integrated discussion of the impacts on competitiveness and on innovation; and an identification of tensions among different provisions or between policy and commercial imperatives observable within the case.

Because much of the interview evidence is qualitative, and in view of the difficulty of obtaining concrete data from the subjects or public sources and the even greater difficulty of predicting changes in the data processing industry, we do not develop a quantitative econometric analysis. Some calibration and analysis was provided in the background (Section 2.2, especially 2.2.4).

3.2. Case Study Selection

The cases were selected on the basis of initial expectations of: the differential importance of the processing, responsibility and migration provisions; the maturity of the sector; the level of public privacy concern in relation to the sector; and the importance of personal data (compared to other types) in the data processing activities involved. These considerations resulted in the selection of four case study areas, as indicated in Table 8.

Table 8: Case study selection

	Impacts on			
Criterion	**Profiling, Behavioural Advertising, Cookies and Social Media**	**Big Data**	**Cloud computing**	**Privacy-enhancing technologies**
Provisions				
Automated processing (Art. 20)	High	Medium	Medium	High
Data controller responsibilities (art. 28)	High	Medium	High	Medium
Data transfer (Art. 44(1)(h))	High	High	High	Low
Maturity	Medium	Low	High	Medium
Public concern	High	Low	High	Medium
Centrality of personal data	High	Low	Low	High

3.3. Profiling, Behavioural Advertising, Cookies and Social Media

3.3.1. Introduction

Profiling techniques are widely used in sectors such as banking, health and retail. Applications range from combating fraud, service customisation to marketing. In e-commerce activities, profiling is the dominant way to tailor services to key audiences. Companies that use behavioural advertising techniques include legacy advertising companies and social media platforms, which use advertising techniques in the delivery of services. Personalisation and customisation are seen as intrinsic parts of a competitive internet economy. Behavioural advertising is fast becoming a key business model in the internet economy. Targeting uses cookies and other technologies that enable recognition of web browser instances and reduce user input requirements. The use of technologies to recognise devices and thereby collect data is regulated in the ePrivacy Directive (Directive 2002/58/EC) as amended by Directive 2009/136/EC. However, when the collected information is used as a basis for providing targeted advertisements, this falls under the

proposed Regulation, in particular Article 20 on profiling. In this case study, the expected impact on innovation and competitiveness resulting from the Regulation will be described from the perspective of the advertising and social media industry.

An independent study conducted by Deloitte and published in January 2012 estimates that Facebook's activities generated gross revenues of €32 billion supporting 232,000 EU27 jobs. An estimated €2.2 billion (32,900 jobs) of this came from Facebook's function as a platform for app developers. Other parts relate to advertising. The use of data for personalisation and customisation is also a driving factor for the e-commerce industry. Generally the use of data helps improve the efficiency of services. According to some advertising companies[87], these gains amount to as much as 500% in specific cases, while an average efficiency improvement of about 40-50% across all sectors can be seen.

3.3.2. Impact by provision

Automated processing and profiling (Article 20)

Article 20 extends the scope of the Directive 95/46/EC provisions in relation to automated individual decisions to cover a range of new factors including location, personal preferences and behaviour, without specification of the purposes of the profiling activities. According to interviewees, the failure to adequately distinguish between processing with legal or significant effect and content customisation could indiscriminately subject a potentially enormous range of activity (and yet-to-be-invented applications) across every industry sector to the stricter consent provisions of Article 7 and the provisions relating to prior authorisation as defined in Article 33 and 34. Practices such as anonymous targeting, affiliate marketing, and web analytics (an important tool for competitiveness) will be made impossible. The broad framing of the provision may have unintended consequences and negatively affect many legitimate practices.

The way the provision is formulated may force business to obtain consent for all personal data-processing activities. This is expected to have two main drawbacks. First, the requirement of consent requires a shift to a customer relationship based on logins and accounts, which results in the collection of more rather than fewer personal data due to the effective prohibition of processing based on anonymous or pseudonymous data without consent. Secondly, US based, globally operating, web based platform companies with massive user bases such as Google, Facebook, Amazon and eBay will be in a much better position to obtain consent. With strong B2C relationships, social reinforcement and critical mass acceptance, more frequent transactions covered by a single act of consent and important economies of scale they are more likely to achieve high consent rates than smaller companies and innovative start-ups, let alone predominantly B2B EU companies, who lack the end-user relationship required to achieve consent. The consent requirement may foster a more fragmented and closed EU internet where advanced targeting is dominated by US based platforms, instead of the open Digital Single Market envisaged in the Digital Agenda for Europe.

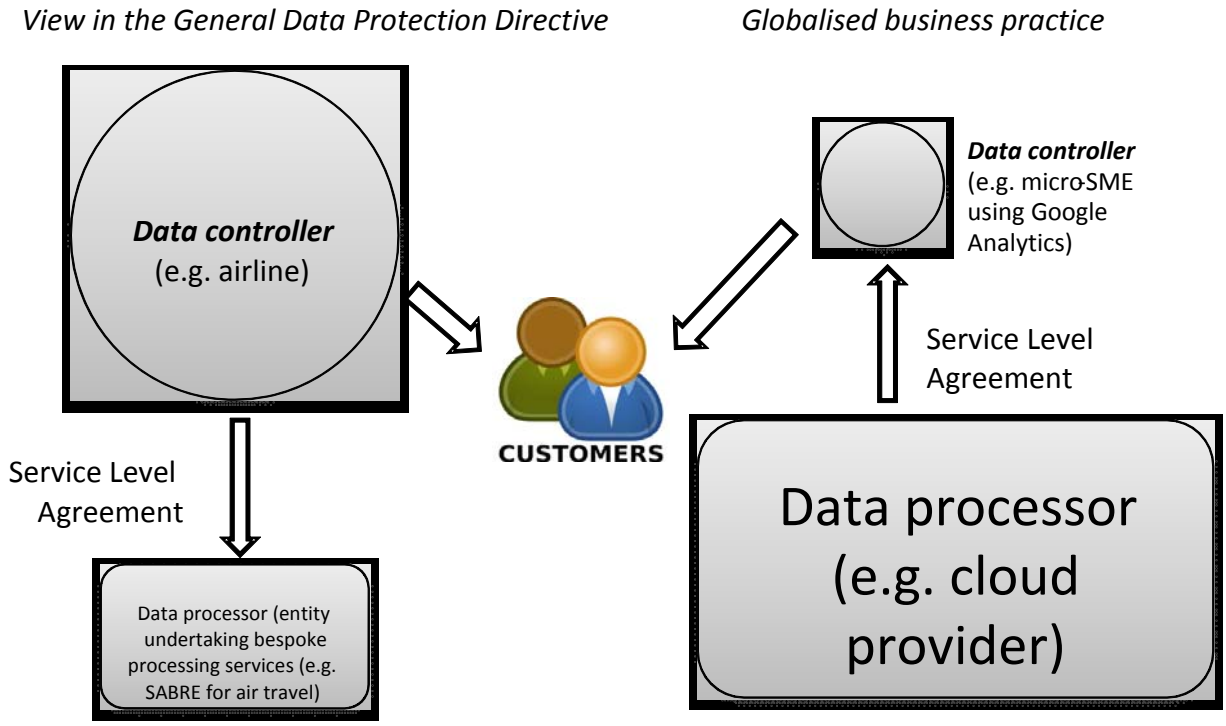
It is important to clarify this provision; businesses do need to conduct internal statistical analyses of customer behaviour. This should not be unduly constrained by the Regulation if innovation is to thrive in the EU context.

[87] Interviews conducted under Chatham House rule.

Responsibility of the data controller (Article 28)

The current design of the processor-controller-relationship is problematic. The underlying assumption that the controller is a powerful party and the processor is a smaller service provider does not cover important situations where the data controller is very small (e.g. users of Google analytics), and in particular may not be able to oversee the activities of the processor (Google).

Figure 5: Generalised model of the evolving controller-processor relationship



Moreover, the relationship between controller and processor seems to be seen as a bilateral relation, while in practice controllers often have relationships with several processors. There seems to be no *a priori* reason why processors should be subject to the same administrative obligations as controllers, but equally no fixed presumption tipping the burden one way or the other. The administrative processor related obligations (Article 28(1), (3) and (4)) to keep the same documentation as controllers are seen as particularly burdensome.

There is also fear amongst businesses that Article 28 will create excessive bureaucracy by obliging controllers and processors to maintain documentation of all processing activities. This obligation can be seen as a form of data retention, which contradicts the general principle of data minimisation. Flexibility is desired; these businesses feel strongly that the Regulation should frame the right incentives without being overly prescriptive, allowing controllers to implement the processes in the context of services they provide.

Data transfer to third countries (Article 44(1)(h))

A stronger basis leading to wider recognition of the Safe Harbour Agreement in the Regulation would be welcomed; the resulting legal certainty of compliance with EU data protection legislation would stimulate greater reciprocal market access (allowing European companies to take advantage of US facilities and to offer services in both the US and Europe without needing to fragment their service provisioning, while strengthening competition in Europe and thereby improving the services available to European end-users). The newly introduced 'business interest' ground for legitimate transfer/processing to third countries lacking equivalent protection is not expected to produce significant impacts, because it does not apply to frequent or massive processing.

Some services, in particular social media, serve as platforms on which developers can build new applications, in turn allowing (often very numerous and small) companies to develop and deploy innovative products and services. Further restrictions on personal data transfer to third countries would prevent EU innovators from building applications on non-EU platforms or basing application development on personal databases pooling EU and non-EU data. As noted above, this kind of activity produces over €2 billion of revenues on the Facebook platform alone.

3.3.3. Impacts on competitiveness and innovation

The current drafting of the Regulation shows no recognition of positive uses of profiling, such as fraud prevention and security, and does not differentiate between the technology and its uses. Interviewees expressed the view that Article 20 violates the technology neutrality principle alluded to in Recital 13, which is critically important in crafting future-proof regulation. Given the numerous other safeguards in the draft Regulation, profiling techniques need not be treated differently from any other type of personal data processing, minimising the risk of future disruptive changes to remove or alter this provision.

The previous Directive 95/46/EC was directly responsible for a range of innovations – such as anonymous profiling – that remove the tension between privacy protection and enhanced services for end-users. This innovation has spread to the US, demonstrating both the innovation stimulus created by suitably-neutral provisions and the diffusion that enhances both competitiveness and the levels of protection available to all (including EU citizens) in a globalised Internet context. The broad scope of Article 20 – and in particular the prohibition of anonymous data processing for profiling purposes - can reverse this innovation and choke off the flow of similar innovation, suppressing privacy-friendly innovations based on Privacy by Design.

The impact of Article 28 may be limited. This will depend on further guidance as to the administrative requirements and incentives for compliance.

Article 44(1)(h) will also have very limited impact, due to its restriction to massive or frequent transfers/processing.

Overall, as regards profiling the proposal will mean less innovation and fewer business models to crunch data. Current limitations on using data acquired with advanced targeting remain in force, reducing the scope for innovative indirect targeting in the EU. The new Regulation tightens this to threaten privacy friendly approaches such as anonymous targeting.

3.3.4. Tensions and concluding remarks

The proposed one-stop-shop system has the potential to create incentives for international organisations to establish and invest in Europe, which means that European citizens will be able to seek redress in the EU. However, the one-stop-shop system will only work as intended if the relationship between national data protection authorities and the 'competent supervisory authority' is properly defined and enforceable

3.4. Big Data (BD)

3.4.1. Introduction

Big data describes the scale of datasets and information management and processing technologies made available through the development of ubiquitous computing and storage capacity. The term also refers to novel ways in which organisations combine digital data sets and then use statistics and other data mining techniques to extract from them both hidden information and unforeseen correlations. As the EU BD analysis industry is at an early stage of development, the proposed Regulation will have a paramount impact on the extent of take-up of BD technologies by EU firms, which are currently reluctant to invest in the area.

Big data analytics is one of the fastest-growing sectors in IT, "worth more than $100 billion and growing at almost 10% a year, which is roughly twice as fast as the software business as a whole"[88]. The big data storage and processing market is mainly dominated by diversified US-based corporations (SAG, Oracle, IBM, Microsoft, SAP, and HP) and 'pure play' companies using open source networks and software (e.g. Vertica). The sector therefore comprises: suppliers of hardware and processing capacities for storage and analysis; data mining and visualisation application developers; and those using BD services to produce other products, services and processes. European BD suppliers may be able to penetrate this sector as projected growth in BD-orientated appliance, cloud services and directly-commissioned BD services shifts demand from technical capacity (where US firms dominate) to business value (system performance, availability, security, and manageability). Sectors that can benefit from BD include finance, healthcare, government, research and energy (smart grids). These result both from the optimisation of processes within companies (dealing mostly with non-personal transactional data, therefore largely uncontroversial from a privacy point of view) and a plethora of applications ranging from design of behavioural incentives for environment-friendly behaviour to retail consumer profiling. Examples are provided in Table 9.

BD is related to the other case studies in this report: big data themselves are increasingly stored and processed in the Cloud; correlations discovered through BD analytics are used for profiling in sectors including behavioural advertising and predictive analysis, while data protection requirements incentivise development of privacy-friendly analytical techniques for BD.

[88] "Data, Data, Everywhere" *The Economist* Feb. 25th 2010 at: http://www.economist.com/node/15557443.

Table 9: Market potential of Big Data in various sectors

Sector	Application	Market size/ Market potential through Big data
Finance and Banking	Fraud detection, determination of creditworthiness	Savings of up to $ USD400 billion per year in the US (McKinsey 2012)
Retail	Transactional data: supply chain and inventory management Purchasing data: consumer profiling, data mashing, predictive analytics	£32 million in the UK retail sector and £45.9 billion across the economy through supply chain maximisation between over the next 5 years (CEBR 2012)
Research	Correlations between large raw datasets , e.g. genomics, particle research (CERN);	No data available
Cybersecurity	Data mining including IP addresses, Discovery of malicious code; Internet telemetry to understand trends and pattern in outbreaks of cybersecurity threats; predictive analysis	No data available
Government	Operational efficiency; tax fraud detection	€250 billion value per year for the EU public sector (McKinsey 2012)
Healthcare	Insurance fraud detection; administrative efficiency; coordination of care; research (e.g. data analytics in genomics); increasing awareness (e.g. Google flu monitor); population health management (e.g. obesity monitor on the data.gov website)	£1.5 billion annually in the UK (CEBR 2012)
Mobile	Branching out into location-based services; Value generation from high granularity data	$100bln to service providers and $700bln to consumers (McKinsey2012)
Smart Grids	Increased efficiency in aligning demand and generation, inferring behavioural patterns and constructing individual profiles; Household-level data: use by government for tax compliance/behavioural incentivising for environment-friendly behaviour	$187 billion in the EU over the next 30 years (JRC 2011)

3.4.2. Impact by provision

Automated processing and profiling (Article 20)

BD analysis inherently entails automated processing; business models built on big personal data thus generate tension between the principles of data minimisation and purpose specification on one side and the business need for input on the other. Such activities largely constitute profiling under Article 20. Some legal uncertainty remains around whether some data suited to BD are covered, e.g. IP addresses.

The current regulatory environment potentially inhibits industry growth around BD activities; consent is potentially impractical at big data scale and in any case has not

necessarily provided adequate protection, as pointed out by an interviewee, a number of companies making use of BD analytics chose to ignore the legislation altogether. These observations would point towards an approach similar to that outlined in Option 1 of this briefing.

Responsibility of the data controller (Article 28)

Lack of clarity in distinguishing the data processing and controlling roles can increase legal uncertainty in the BD context as well as other segments of the data processing industry. It partially reflects the sources of mined data: when data involving multiple parties are uploaded to social networking sites and used by (non-automated) apps, for instance, the uploaders are simultaneously data subjects and controllers (and even processors) of data concerning other identified individuals.

Big data analytics generally use anonymised data, which can allow re-identification through data mashing.[89] The proposed Regulation leaves the data controller responsible for these data unless they are effectively anonymised - the impact thus depends on the definition of (and certifiability of compliance with) acceptable baseline standards of anonymisation, as pointed out by an interviewee:

> *"industry is going exactly the opposite way and […] there is a trend in identifying what counts as anonymisation in order to free the processing of such data".*

Data transfer to third countries (Article 44(1)(h))

Big data-based services usually depend on data collected from global platforms (such as social networking services) and service/product delivery to global markets to create value from innovation. Any geographical limitation to data collection or redistribution (in the form of BD outputs) can prevent companies from obtaining the critical mass of data or customers necessary to developing such services – or can limit the robustness and utility of BD conducted on smaller samples. Therefore, much depends on the legitimate business interest clause introduced by the Regulation.

3.4.3. Impacts on competitiveness and innovation

Competitiveness

BD analysis can enable companies to boost revenues by 5-6% through improved management decision-making alone, and by up to 60% in certain sectors.[90]

The scalability of big data affects the two-sided market for data: companies benefit from data already in their possession but can also buy and sell data on secondary markets; health sector companies can exchange clinical data on interventions for e.g. cash, additional clinical data or data on risky behaviours. This aspect (emergence and influence over secondary data markets) is particularly evident in oligopolistic markets such as telecoms or utilities where market power and coverage produce larger datasets. According to an interviewee, it could potentially enhance the competitiveness of EU firms, although even widespread availability of BD tools tends to favour larger companies with data from a large customer base compared to SMEs. At the same time, the fixed costs of regulatory compliance can be amortised over a larger base for larger companies. This should

[89] Ohm (2010); Cavoukian and el Emam (2011).

[90] Brynjolfsson et. al. (2011), McAfee and Brynjolfsson (2012).

encourage (especially larger) companies to scale up data-protection-compliant BD activities, particularly since larger firms have better means to purchase tools and services for analytics. A secondary market for data also creates incentives to collect and retain larger sets of data than it would be necessary for strictly operational reasons. Exchanging datasets between large companies, e.g. in utilities would result in a strengthened position in their home markets and could be leveraged to increase influence in the input markets (for instance, by including data in transaction terms with suppliers or creating common depositories), to the extent allowed for by competition legislation. This surplus created by monetising consumer data could be shared with consumers in the form of lower prices or increased quality of the service. Interviewees have voiced the perception that regulation has not uniformly anticipated BD-based business models: as a result, companies such as Telcos subject to sectorial regulation compete with generally-regulated service providers in providing location-based services, leading to different compliance requirements for provision of identical services.

The young and small applications developers who populate the EU market have to operate in a business ecosystem defined – and currently dominated - by large, mainly American companies that can take advantage of the opportunities offered by home markets with more permissive data protection regimes for developing and privacy-proofing products as well as for leveraging network effects and revenues obtained through applications with lower standards in order to bear the costs of compliance in Europe. While this ecosystem is not necessarily adverse to innovation and the EU has a promising BD start-up population, data protection difficulties drive growing companies abroad or discourage new start-ups – even where they could ultimately provide services that are both compliant and competitive with incumbent products. Small companies are more agile in navigating a changing regulatory landscape and can be more prone to take on innovation-related risks, as their costs of failure and reputation loss are more limited than those faced by large firms. Therefore, even though they may not be able to take advantage of economies of scale in relation to data access, they could carve out a role by developing innovative services to ensure and/or certify policy compliant data interoperability to large-scale data controllers. This would enable larger firms to specialise in combining datasets whilst making compliance more commercially sustainable.

Innovation

Diverse legal standards regarding limitations on data processing can give companies with access to BD insights and practices developed in jurisdictions with laxer provisions a competitive advantage. At the same time, according to several interviewees Data Protection provisions have clearly motivated the development of privacy-enhancing solutions such as privacy-friendly data mining in the mobile industry or pattern-recognition surveillance systems[91]. Interviewees voiced a belief that as BD analytics services are often outsourced to specialised companies, these will have a strong incentive to deploy innovations allowing them to bundle compliance with their BD services allowing new business models to emerge. It is crucial to consider the structure of the costs of compliance. If we consider compliance costs to be mainly fixed (and sunk) costs –– an increase in their level – which is absorbed in profit margins but not shared with the consumer[92] - can raise barriers to market entry, disadvantaging smaller companies and

[91] Danezis and Gurses (2010).

[92] More precisely, in a competitive market price is set by *marginal* cost; changes in fixed costs are paid out of the firm's producer surplus. If fixed costs are too high, firms may exit, but sunk costs (which cannot be recovered by exit) do not drive firms out of the market. A firm that cannot cover its sunk costs may lose money, but would lose more if it exited.

start-ups. At the same time, fixed costs can induce step-change innovation within firms, for instance encouraging changing encryption routines to data. Ultimately these practices can reduce the cost of access to the innovation. Open-source[93] or compulsory licensing[94] of these practices (for instance included among the conditions for approving a solution as compliant) therefore has the potential to reduce the social costs of innovation to near-zero levels. On the other hand, similarly to the economics of cloud computing, measures requiring a shift of compliance costs to marginal costs[95] (for instance resulting in outsourcing services paid for by demand), would result in firms sharing the extra costs with consumers. Measures resulting in raising the marginal costs of all firms are likely to result in increased competition, ultimately an incentive for increased innovation.

In addition, interviewees have emphasised that compliance that ensures the proper collection and management of personal data can increase the value and protection of such data, which could be promoted by (open) standardisation. On the other hand, open access to data collected by the public sector (e.g. data.gov and data.gov.uk) can extend fundamental rights of access by making properly managed data available to all parties. This could be further magnified by compliant – but relatively more open - access to datasets owned by companies. Competition between companies, therefore would take place in a level playing field regarding access to data, and be more determined by the competitiveness of their (compliant) products, The net effect of open access measures is therefore difficult to gauge between the likely effects on competition and the disincentives to innovation in data collection resulting from it although these measures would not prevent companies from reaping the benefits of innovation for business models and management by using intra-company transactional data.

3.4.4. Tensions and concluding remarks

While BD analytics results in higher quality of services delivered to the consumer, the existence and operation of BD algorithms behind the development and operation of these is largely unknown to data subjects, raising questions of access, accountability, reliability and transparency, posing the question of a trade-off between product quality expected by consumers and BD processing required for its delivery. It is however difficult to configure methods for regulatory control over fast-changing algorithms or applying regulation to computer code.

Data protection principles in certain cases conflict with sectorial regulation of BD-using industries. Certain sectors, such as the aviation and financial industries are required to process personal data in the fight against fraud and terrorism. Modifying provisions on data protection but not these specific requirements can reduce the quality of customer service and increase legal uncertainty[96]. Therefore, harmonisation within EU law is, similarly to the

[93] A variety of open-source solutions to privacy compliance have been developed for particular contexts, including healthcare (e.g. iTrust – see Massey et. al. 2010) and in more general settings (e.g. SAML, OpenID and the WS-Federation specifications – see Cavoukian 2008).

[94] This is recommended in Schwartz (2000). The use of compulsory licensing is common in e.g. pharmaceuticals for drugs to treat serious diseases; an individual or company seeking to use a patent can do so without seeking the patent holder's consent by paying a set fee for the license. The TRIPS (WTO Agreement on Trade Related Intellectual Property) devised a solution to the challenge posed by the Doha Declaration which was brought into force in May 2006 in EU law under Regulation 816/2006.

[95] In other words, making compliance available as a service paid for to the extent that it is actually needed, rather than as a fixed charge that may be disproportionate for small firms or those serving privacy-insensitive users. See discussion of fixed vs. variable compliance costs on page 27.

[96] European Commission (2007) (Sources: IATA position on the proposed Regulation, European Banking Federation Position on the proposed Regulation).

recognised need for harmonisation across Member States, perceived by stakeholders as fundamental for legal certainty and avoiding unnecessary compliance costs for business.

Interviewees have expressed a strong perceived need for the public sector and DPAs to reconsider the role of public-private partnership in an area extremely close to fundamental rights and are likely to be fundamentally changed with the changes in the magnitude of personal data processed through BD applications. At the same time, implementing documentation obligations on the volumes of data managed by BD could have a similarly large effect on the workload and processing capacity of DPAs. In conclusion, there is a fundamental contradiction between the operational principles of big data-based innovation and those of data protection. Limited data access can disadvantage companies in the global competitive environment where other companies can provide the same services and operate on the same platforms. Almost all interviewees felt that enforcement has the potential to level the playing field between larger and smaller companies as well as European and foreign ones on the EU market but not at the global level. Defining all potentially re-identifiable data as personal can limit innovation in big data; – legislation such as outlined in Option 1 of this briefing could address this limitation. In general, a risk-based approach and definition of standards could allow the definition of data that does not fall under the scope of the Regulation.

3.5. Cloud Computing

3.5.1. Introduction

For the purpose of this case study cloud computing is defined in accordance with the US National Institute of Standards and Technology:

> *"a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*[97]

Cloud computing is growing worldwide; this is expected to continue. Between 2009 and 2010 the worldwide market for public cloud services grew by 26.7%, from $58.6 billion to $74.3 billion. The European public cloud B2B market reached €3.5 billion for Software as a Service (SaaS) and €1.1 billion for Hardware as a Service (HaaS) in 2011.[98] However, cloud spending is limited. In 2011, public cloud services accounted for just 1.6% of total business IT spending. This is expected to change; according to a recent estimate by the International Data Corporation public cloud revenues will reach €11 billion by 2014 –3.6% of the total IT market.[99] At present, large enterprises (over 250 employees) represent more than 80% of current cloud spending – they are expected to continue to out-invest SMEs in the future. The finance and manufacturing sectors invest the most in cloud services at present.[100]

According to a 2011 IDC survey, e-mail was the most used cloud service in 2011, followed by security, accounting/back office, databases and online storage including back-up and/or disaster recovery.[101] 78% of the cloud-using organisations surveyed reported cost savings – primarily due to increased mobility and productivity. Privacy, security and data protection

[97] Mell and Grance (2009).
[98] Bradshaw et. al. (2011), p. 10.
[99] Bradshaw et. al. , (2011) p. 10.
[100] Bradshaw et. al. , (2011) p. 10
[101] IDC (2012) p. 20.

legislation are of significant importance for both European cloud service providers and European cloud users. Although industry security concerns may have diminished to some extent in recent years,[102] the 2012 IDC survey revealed that the second most important barrier to cloud adoption is security and data protection.

These concerns – in concert with the privacy provisions – have led to innovation. In the past, users' privacy, security and automated data processing rights were reflected in Service Level Agreements (SLAs) although these have proved ineffective and inefficient for a number of reasons.[103] In order to enable cloud services providers clearly to communicate to potential customers the level of privacy protection to be expected, provide a tool for monitoring compliance with legal requirements and best practices and provide a basis for contractual protection against financial damages from non-compliance, the Cloud Security Alliance (CSA) has proposed Privacy Level Agreements (PLAs) in order to simplify and harmonise effective compliance with data protection legislation across cloud service providers.

> *"In the PLA (typically an attachment to the Service [Level] Agreement) the Cloud Service Provider will clearly declare the level of privacy and data protection that it undertakes to maintain with respect to the relevant data processing, in a format similar to that which is used by other Cloud Service Providers. Cloud Service Providers have realised the importance of privacy disclosures, and they are devoting time and resources at improving their privacy disclosures, in order to reassure the customers about their data handling practices."*[104]

It is thought that in the future, the most competitive cloud providers will not only provide high levels of data protection but will also *demonstrate* this to potential customers. Therefore, compliance may drive both innovation and competitiveness (although many interviewees view the legislation as predominantly restrictive; the tension between these opposing schools of thought is explored below).

3.5.2. Impact by provision

Automated processing and profiling (Article 20)

Profiling is a fundamental part of business-to-consumer cloud computing, under the *freemium*[105] model. As one interviewee stated, "this is the present and future of an economy driven by advertising and marketing activities." As noted above, Directive 95/46/EC allowed automated processing of unidentifiable personal data, which led to anonymisation or pseudonymisation, encryption and fragmentation[106] prior to processing. However, Article 20 of the proposed Regulation applies much more stringent restrictions to all forms of profiling; this has raised several concerns within industry. The first of these relates to the way profiling is distinguished from other personal data processing and the distinction in practice between personal and non-personal data. Essentially, the Regulation does not acknowledge positive uses (such as research on customer behaviour which fuels innovation) of profiling, which is singled out for particularly stringent restrictions.

---

[102] The 2012 industry Northbridge survey on the future of cloud computing found that only 3% of respondents considered cloud computing to be too risky ever to use compared to 10% in 2011. Similarly, only 12% believed that cloud computing needs to mature, compared to 26% in 2011, and finally 50% stated they have complete confidence in cloud computing compared to only 13% in 2011.

[103] Cave et. al. (2012), p. 45.

[104] See https://cloudsecurityalliance.org/research/pla/.

[105] Freemium services are provided gratis up to a certain level, beyond which the user has to pay.

[106] Hon et. al. (2011), p.11.

Ultimately, data driven innovation is likely to be suppressed – at least in the EU. Moreover, while industry recognises the need to restrict certain types of non-identifiable data processing this does not extend automatically to all kinds of profiling.

The second concern relates to the consent provision. Some industry stakeholders view consent to profiling as inherently untenable, because it requires knowing who the data belong to – which can only be achieved in a *logged-in* Internet environment; the unauthenticated Internet user would cease to exist. Of course this is less significant for services which already operate within a logged-in model, such as Facebook. According to interviewees "personalisation and customisation are intrinsic parts of a competitive internet economy across all sectors" which would be made "impossible" under the draft Regulation in its current form. Therefore, the prevention of profiling is perceived to be beyond the scope of the Regulation, and is anticipated to be amended before it is finalised (particularly given the importance attributed to anonymisation in various official documents[107]). With this in mind, several interviewees felt that the Regulation should (and will) resemble legislation akin to Option 1 of this document.

Responsibility of the data controller (Article 28)

Article 28 of the proposed Regulation does not clearly distinguish data controllers and data processors; this is a particular issue for cloud computing given the overlap between the two roles, and the large number of sub-processors involved in the data processing value network. According to several interviewees, the extension of data controller obligations to data processors is unjustifiably burdensome and will introduce additional costs – especially for those in countries who do not already adhere to documentation requirements. One interviewee believed this would simply introduce red-tape to business-to-business relations without enhancing data subjects' protection. In other words, from this perspective Article 28 only serves to introduce additional burdens to demonstrate compliance, rather than to contribute substance to a legal framework that will directly enhance the protection of data subjects. As such, it is viewed by some as unnecessary, burdensome and indeed unjustifiable. This idea is explored further below.

However, it is important to note that several interviewees welcomed the proposed change: it will ease the work of Data Protection Authorities; it is good practice to document business practices (even if they remain internal); and it is important to have control of data processing throughout the value chain. One workable model within the cloud may be for the data controller to guarantee the data processor, who then guarantees the first sub-processor, who then guarantees the second sub-processor and so on. Within this model, the data controller would serve as point of contact if any issues are raised. However, it is important to note that this trust hierarchy model may reduce cloud flexibility and increase lock-in, especially for cloud-based long term data repository services.

Data transfer to third countries (Article 44(1)(h))

The transfer of data to third countries is of primary significance to the cloud, which operates across national boundaries. The current Directive was viewed by some as out-dated and ill-suited to the realities of cloud computing in 2012, given that it views international data transfers as the exception rather than the rule. However, as with the case of profiling (see Section 3.3.2) there was a general consensus among the interviewees

[107] In May 2012 the ICO began a public consultation on a new anonymisation code of practice. See http://www.ico.gov.uk/news/latest_news/2012/ico-consults-on-new-anonymisation-code-of-practice-31052012.aspx.

that allowing transfers to third countries without adequate protection for 'legitimate business interests' (without any further clarification) will change very little, not least because it only applies to one-off non-standard transfers. The limitation in Article 44 to transfers that 'cannot be qualified as frequent or massive' was viewed by one interviewee as indicative of an obsolete perspective missing, for instance, the great bulk of recent developments in relation to sensitive financial data. Ultimately, it is unclear why it should be more difficult to transfer large amounts of data as opposed to limited amounts of data. As such, as with Article 20, several interviewees anticipate this Article to be amended before the Regulation is finalised.

However, one interviewee did highlight other changes in the legislation which will have greater impact – and which demonstrate a move towards allowing the free-flow of information to a certain extent. The first of these is the recognition of sectoral adequacy. Just as the Safe Harbour Agreement is restricted to companies within certain sectors, the proposed Regulation recognises both sectoral and geographic adequacy. The second significant change is the explicit recognition of Binding Corporate Rules (BCRs). This would be enhanced for the cloud computing sector if BCRs were not restricted exclusively to transfers between organisations under the same control.

3.5.3. Impacts on competitiveness and innovation

Many competitiveness and innovation impacts have been identified above in relation to individual articles. However, it is essential to acknowledge significant disagreement among the interviewees regarding the extent to which compliance will enhance innovation and competitiveness. Some believe that stringent European legislation will enhance innovation and competitiveness; cloud service providers may 'race to the top' in terms of actual and demonstrated compliance with robust data protection laws in order to attract privacy-sensitive business and security-weary cloud users. This should stimulate innovation and competitiveness among cloud service providers but perhaps more in the B2B segment; as other research illustrates that consumers act irrationally when it comes to privacy protection online[108].

Secondly, changing legislation in several areas may stimulate innovations to improve efficiency and/or compliance e.g. with Subject Access Requests (SARs) and *the right to be forgotten*. Thirdly, the harmonising nature of the proposed Regulation may create a level playing field, thereby allowing for a competitive market all over Europe. Not only this, but it will reduce the administrative burden associated with complying with various national legislation across Europe.

On the other hand, many interviewees could only see the restrictive nature of the legislation. One interviewee believed that in terms of innovating to comply, organisations could only innovate to comply with tools to enhance compliance – rather than legislation to enhance the data protection of the individual. These tools are seen as additional burdens rather than aids to compliance. From this point of view, the proposed Regulation will stifle innovation (particularly in the areas of personalisation and aggregated profiling). Moreover, the over-bureaucratic provisions regarding third data transfer discourage using the EU for data hosting purposes and the internet would be transformed from a space of freedom to a logged-in environment, which may see Europe get left behind.

[108] See Acquisiti and Grossklags (2004).

3.5.4. Tensions and concluding remarks

The vast majority of interviewees believed that it is both necessary and desirable for the European Commission to stimulate privacy friendly business models although several interviewees had slight reservations. One agreed to the principle, but felt that as the law is not final, it is difficult to imagine such a model. Another felt that while such intervention would be welcomed, it should allow the scope for innovation in terms of building privacy controls into products.

Several interviewees believed that Article 20 and the Articles associated with international data transfer would need to change in order to be acceptable. Ultimately if the legislation is not sustainable, it does not perform its purpose which is the protection of data subjects. In terms of cloud specificities, one interviewee commented there is not one single instrument within the proposed Regulation which deals with issues related to the cloud in their entirety – resulting in transactions needing to be regulated through multiple Articles. Although the Regulation must remain technology neutral, this would be a welcome addition.

3.6. Privacy Friendly Technologies (PETs)

3.6.1. Introduction

Privacy provisions have stimulated PETs innovation in at least two ways; to take advantage of greater awareness and serve stakeholders compliance needs, and to facilitate bypass of inefficient provisions. As regards the first of these, Directive 95/46/EC led to several privacy friendly technologies (e.g. Privacy by Design approaches). Their market uptake is still relatively limited, because in most cases the technology is provided as a service to businesses or organisations, sometimes even on a non-profit basis. As regards the second type, privacy friendly technologies developed to solve compliance problems with the Data Protection Directive including anonymous profiling (see 3.3.2). In this application area, businesses have a commercial interest and a growing economic position. Some of the companies developing and deploying these technologies have more than 5000 employees, of which about 80% are based in the EU. Smaller initiatives such as the Dutch Qiy Foundation[109] consist entirely of EU employees. Because Directive 95/46/EC concerns the EU market, almost all innovation takes place in the EU itself. Some technologies have successfully been exported to the US as well.

EU data protection legislation has specifically encouraged technologies that promote user control, improving awareness (and hence importance) of privacy friendly products. However, the approach taken in the proposed Regulation can be interpreted as branding market intelligence as a bad thing, which may send out the wrong signal given EU ambitions in such a key innovation area. Instead, it should be designed to emphasise that the aim is to stimulate innovation in privacy friendly alternatives to existing technologies.

3.6.2. Impact by provision

Automated processing and profiling (Article 20)

Companies that innovate in the domain of privacy enhancing technologies may be helped by this provision; examples include firms that develop and deploy trust frameworks allowing users to decide how much data to share and with whom. Privacy, in this respect, is the result of a different design of the processing network, based on Privacy by Design

[109] An organisation which provides digital identities in a personal domain http://www.qiyfoundation.org/en/.

principles. The quality of profiling can be improved, because data subjects have control and share their interests themselves within the trust framework. Through a process of creative destruction, this may turn out to offer better commercial and end-user outcomes than anonymous profiling.

Another aspect relates to the development of digital identities to facilitate and effectively anonymised digital communications. New business models are currently being developed in this field, where the EU has an important position.

The general issue of creative destruction has a more general implication as well; Regulatory changes or regulatory uncertainty may inhibit innovation to the extent that entrepreneurs and other innovators perceive a risk of stranded investment, leading to *excess inertia*[110].

Responsibility of the data controller (Article 28)

Transparency is accorded utmost importance, again because it facilitates user control. From the privacy friendliness perspective the requirements proposed in Article 28 are very important. Even the documentation expected from data controllers was not, among our interviewees, expected to lead to unreasonable burdens. However, it would be a logical and welcome step for the EC to develop standardised processes. These could be formalised in delegated acts. These acts should also consider if part of the requirements can be met by automated means. For the most part this could be done with the help of logging techniques.

Data transfer to third countries (Article 44(1)(h))

This Article is not expected to have a significant impact. It permits only very restricted forms of data transfer. More significance can be brought by Corporate Binding Rules or by explicit recognition of Safe Harbour Agreements, and these remain in place in the current proposal. The drawback of these instruments, however, is that they are only within the reach of large companies, while most innovation and competition in the field of privacy friendly technologies comes from start-up companies.

3.6.3. Impacts on competitiveness and innovation

The new Regulation could stimulate the emergence of a new PET industry – or at least spur its development. Awareness of and attitudes towards privacy among citizens and commercial and civil society organisations are not as different (between the EU and US, for instance) as the respective legal provisions. As it becomes clear that data protection regulation is important and has an effect on business models, these initiatives will grow and increase their importance and market position, especially as larger companies join initiatives and in order to use products and services provided by the small start-ups. In the EU, such interested companies, such as PostNL, Deutsche Telekom, Telefonica, and SwissCom, come mainly from the telecommunications sector.

[110] In industries with network externalities (such as interoperability) the benefits of participation typically increase with the number of participants. This affects the dynamics of innovation; a firm that develops a new protocol will lose its investment if other firms do not adopt the same or compatible approaches, leading to excessive risk aversion compared to the optimal pace. By the same token, a desire to capture first-mover advantages by leading the market towards adoption of a proprietary solution can lead to excessive volatility; too many and too rapid innovations (again compared to the optimal pace and number). This, in turn, makes innovation effectively 'one-sided' if new approaches are abandoned before users have a chance to discover how best to use them. See Katz and Shapiro (1994).

A public-private example is provided by the UK's MyData initiative[111]. It grants individuals direct access to their personal data held by participating businesses. The requirement to provide access seems to promote innovation in this area.

3.6.4. Tensions and concluding remarks

It is expected that the Regulation will stimulate innovation in the field of privacy friendly technologies as businesses are forced radically to change their business practices. Small amendments to current practices will no longer suffice. Big companies start to join the new initiatives, which is a good sign for innovation. As more resources become available to smaller start-ups with fresh ideas and views on product development, the innovation in this area will receive a further boost.

For some sectors where privacy friendly technologies are applied, however, the proposal in its current form means a step back, because technologies developed since Directive 95/46/EC came into force will no longer be allowed. For companies that process big amounts of data and that have in the past shown their willingness to adopt more privacy friendly approaches, this is a disincentive. If obtaining consent from users is the only remaining option than existing and new business models in this area will be severely curtailed. Attention should rather be paid to innovations that hold the potential to enhance current levels of privacy protection. Developers and users of these technologies should be encouraged to continue on this path strengthening, not weakening the European, competitive edge in this domain.

[111] United Kingdom Cabinet Office (2012).

4. EMERGING FINDINGS AND PRELIMINARY RECOMMENDATIONS

4.1. Introduction

As noted at the outset, the impacts of current and proposed EU privacy measures can affect competitiveness and innovation in a variety of ways. This chapter collects the findings from the previous chapters as they relate to the competitiveness and innovation impacts of the proposed Regulation (Option 0) and a version in which Articles 20 and 28 are modified (Option 1). As noted in Section 2.3.1, there is a three-way relation between privacy, competitiveness and innovation. For the sake of clarity, we separate them here, treating impacts on the competitiveness of firms in 4.3 and innovation in 4.4. But it is useful to bear in mind that *extensive* competition (competition *for* the market) almost always involves innovation while *intensive* competition (competition within an existing market) tends to emphasise cost reduction and the enhancement of consumer willingness to pay by bundling valued attributes (like privacy), raising barriers to consumer search or switching and reducing production costs including costs of compliance.

Moreover, privacy is affected by developments that evolve through the data processing value network. This can be illustrated by considering how dominant business models that collect and reuse personal data (e.g. search and social networks) came into existence.

As noted in the prior report, this kind of business model is less likely to start under a privacy regime based narrowly on the precautionary principle. This is not simply a claim that such regulations raise costs and legal uncertainty and that this discourages innovation.

The starting point of the Facebook and Google business models was the provision of free (and relatively unstructured or user-defined) platform services. These were initially loss-making, but attracted funding via advertising and eventually re-use of profile information once it became known that:

- the audiences would grow through positive feedback (positive network effect);
- people would gradually reveal more and more personal information either through learning to trust their 'friends' in the case of Facebook or through inadvertent expression of interests via search topics in the case of Google; and
- these platforms would gradually become 'essential' to their users, who would then – in effect – be willing to put up with greater intrusion in exchange for more efficient services (faster and better search) or a richer social experience.

In both cases the monetisation of attention constituted a risky business model in which 'personal information' was created or shaped by participation in the platform itself and where user attitudes changed as their experience increased.

Therefore, when considering the impacts of e.g. the prohibition of anonymised profiling, it is useful to consider whether this may lead to or prevent the emergence of wholly new ways for data subjects, controllers and processors to interact to create and capture value.

This Chapter discusses the lessons arising from the survey, interview and literature reviews – first in overall terms and then in the form of an explicit comparison of the three policy options introduced in Section 1.4:

- Option 0 is the proposed Regulation;
- Option 1 consists of the proposed Regulation with the following modifications

- Article 20 is recast to clarify that the legal and significant effects required for exemption from automated data processing and decisions apply to identifiable persons (*data subjects* rather than *natural persons*);
- Article 28 is modified to limit required documentation to data protection policies and implementation and monitoring measures, and to permit trust hierarchies to permit data controllers to certify data processors or vice versa depending on the size, resources and relative discretion of the parties; and
- Article 44(1)(h) is modified to remove the reference to 'massive or frequent' data transfers. In addition, the legitimate interests of data controllers include transfers necessary for efficient data management and explicitly agreed in service level or privacy level agreements. The justification for this change is that international data transfers are fundamental to cloud computing.

- Option 2 involves enhanced self and/or co-regulation involving European and non-European DPAs and industry stakeholders; this option is discussed in Section 4.5.3 but not formally considered, because its scope and complexity go beyond the scope of this briefing.

This Chapter is organised as follows. Section 4.2 considers the lessons arising from the case study perspectives, first in terms of the specific measures proposed for profiling, documentation and data transfers and then more generally in terms of overarching principles such as trust, consent, decision-making power, national and sector specificity and neutrality. Sections 4.3 and 4.4 develop the implications of the regulation for competitiveness of participants in the European data processing value network and for innovations that might affect or be driven by privacy protections. Finally, Section 4.5 recapitulates the analysis as a concise impact assessment, building on the problem statement, objectives and options developed in Chapter 1 and the evidence and analysis in Chapters 2 and 3 in order to compare the options and select a preferred alternative.

4.2. Conclusions from the cases

Table 10 summarises the impacts of the profiling, data controller responsibility and data migration provisions on competitiveness and innovation – compared to the *status quo ante* - from the perspective of the four nascent lines of business considered in Chapter 3. The conclusions are discussed in more detail in the sections that follow. In Table 10:

- The first column indicates the overall impact; subsequent columns indicate impacts of specific provisions;
- The impacts are colour-coded: Red (negative), green (positive), blue (ambiguous) and white (insignificant) - the intensity of colour indicates the strength of the impact.

Table 10: Summary of impacts

	Art. 20: profiling	Art. 28: responsibilities	Art. 44(1)(h): migration
Competitiveness			
Profiling, Behavioural Advertising, Cookies and Social Media	Bad for EU B2B vs. US B2C	Onerous for small data processors and controllers	Reciprocity, level playing field
Big Data	As with profiling; May favour larger firms	Uncertainty due to unclear data processing and controlling roles	Can limit efficiency-enhancing migration Can reassure users
Cloud Computing	Seems to require *logged-in* model	Difficult for cloud-hosted services; may ease DPA work	No significant impact[112]
Privacy friendly technologies	Trust frameworks, better data sharing	Good if standardised	No significant impact
Innovation			
Profiling, Behavioural Advertising, Cookies and Social Media	Bad for EU innovations based on PBD; not neutral	No significant impact	May inhibit app development for global markets
Big Data	Inhibits BD development; may encourage compliant BD by big firms	Potential *effective anonymisation* tools	Can limit size of data sets: ambiguous
Cloud Computing	Rules out freemium models	Potential chains of responsibility	No significant impact
Privacy friendly technologies	Digital identities; but some uncertainty	No significant impact (logging techniques)	No significant impact

4.2.1. Impacts related to the specific provisions of the options

The proposed options are linked to the three areas of regulation (profiling, responsibilities and transfers) considered in this briefing. The adverse impacts identified for Article 20 of the proposed Regulation are largely due to the adverse construction it places on all forms of profiling; Option 1 would replace this by an alternative based on the provisions in Directive 95/46/EC that restores the requirement that automated processing and decision

[112] Data migration is central to the development of the cloud. The proposed Regulation limits the scope of existing protections to "frequent or massive" data transfers and thus does not substantially change the protections and restrictions applying to cloud computing *per se*.

not be applied to identified people or have the effect of identifying them. The adverse impacts identified for Article 28 of the proposed Regulation are largely due to the magnitude and fixed allocation of the documentation burden; they are largely addressed by a more flexible requirement in Option 1 that would allow hierarchies of trust. The adverse competition and innovation impacts of Article 44(1)(h) are traceable to the asymmetric treatment of data transfers by size and frequency – which artificially tilts the playing field but does not correspond to current and evolving market behaviour – and to the 'legitimate interest' exemption, which could benefit from clearer definition, especially in relation to cloud computing. Option 1 addresses these by removing the asymmetry and by linking the legitimate interest of data controllers to contractual agreements with data subjects.

Profiling

Article 20 presents the greatest potential for adverse impacts. It is likely to:

- Harm competitiveness by undercutting existing business models since profiling is increasingly important for back-office efficiency, new service discovery and customer quality of service delivery e.g. targeting to mutual benefit;
- Foreclose an existing trajectory of innovation where Europe is in the lead – and where the innovation and associated line of business can be said to have originated with Directive 95/46/EC; and
- Prove more burdensome to small firms than large ones due to e.g. the ease with which the latter can get high degrees of consent from their installed base.

Data controller and data processor responsibilities

Article 28 will raise both fixed and variable costs for many European stakeholders, and may have a modest effect on data processing markets:

- It will create administrative burdens for certain data controllers and data processors – and possibly for regulators forced to handle the flood of new information; and
- It may distort business and service models and market relationships away from the forms dictated by technological and market forces, especially in emerging areas such as cloud and big data.

Data transfer

Article 44(1)(h), due in particular to the limitations regarding data transfer size and frequency, is expected to have fairly modest effects. However, it:

- Is likely to affect small and innovative companies more than large incumbents; and
- May pose significant obstacles in relation to cloud and big data, where a vast proportion of data transfers are large-scale and frequently international – though this can be compensated to some extent by the growth of capacity that reduces the need for such transfers.

4.2.2. More general impacts arising in the value network

Other market impacts will arise from the overall effect of the provisions on the competitive landscape, rather than the effects of specific provisions on particular stakeholders.

Trusting users

As a general rule, those interviewed agreed that – taking into account the fact that data subjects may need to rely on data controllers of processers to make certain decisions on their behalf - regulation should seek to augment user control through targeted PET innovation rather than prohibition. The latter could signal a dangerous move for EU innovation in a global economy that is increasingly based on the collection and use of data.

The trouble with consent

Europe's B2B data processing industry will have a hard time achieving the consent rates that the US based B2C companies (operating in the EU) are likely to obtain. Early indications are that consent rates in the B2B industry range from 1-10%[113], effectively killing 90% of the business (and corresponding innovation).

Sector-specificity

In contrast to Option 0, US regulations are highly sector-specific. Implementation and impacts under the current Directive – and by extension under Option 1 – are also highly variable (see Section 2.3.1). This comes about mainly as a result of stakeholder decisions in response to common provisions which have led them towards business model, service, or technological innovation, or to modified or reduced use of personal data.

- Advantages of Option 1: a better fit between the constraints and burdens posed by the provisions on one side and the advantages of data protection on the other. For instance, Article 20 rules out many types of profiling, but the advantages and disadvantages are very different for e.g. retail advertising and financial fraud detection where even data subjects' interests may be served by unconsented profiling.
- Disadvantages of Option 1 include complexity, limits to competition and inhibition of the development and deployment of effective horizontal privacy- or compliance-enhancing services. Sectoral variations may also fail to serve data subject interests or to be future proof.

Locus of decision

The perspectives considered in Chapter 3 varied in terms of where the power and responsibility are placed by law or by stakeholders. An example of legal variation is provided by the right to be forgotten; in the EU, this like the exemption from automated processing or the placement of cookies, is granted to (or imposed on) end-users. In contrast, US laws such as the Fair Credit Reporting Act place the responsibility on data controllers obliging them to demonstrate erasure of data after a certain time.

- Advantages of placing responsibility on firms: greater – and easier to monitor - compliance and minimised possibility (especially important for data involving children, health records and financial data) that informed consent may not be practicable or meaningful.
- Disadvantages include the possibility that genuine differences in user preferences may not be reflected in data retention or processing decisions (e.g. a *right to be remembered* as secured in SOX[114]). Another disadvantage is the possible tension between the data

[113] Data from UK Information Commissioners' Office discussed at: http://www.cbsoutdoor.co.uk/About-Us/Market-Digest/June-2012/Users-giving-implicit-consent-on-cookies/.

[114] Section 2.3.3

privacy and data integrity aspects of personal data rights. On the other hand, obliging firms to provide their subscribers with privacy controls has yet to demonstrate its effectiveness. While social network platforms like Facebook have responded to legal and consumer pressure by offering a range of privacy policy settings, recent evidence[115] shows that seemingly-trivial implementation details have a powerful influence over whether users' privacy settings align with their privacy preferences.

National differences

Differences in the implementation of privacy provisions within the EU[116] or between the EU and the US can affect the ability of small and innovative firms to enter and survive in the market, whether for data processing services or for services whose production and delivery obliges the firm to process personal data. This effect can be negative; in order to attain multi-country critical mass, an expanding firm may need to adapt its services to a host of different requirements. On the positive side, diversity may serve as a test bed for the development and implementation of innovative solutions matching the differentiated needs of data subjects and others involved in controlling, processing and using personal data. This can create an innovation threshold; a minimal level of diversity below which new and better solutions to existing problems and new problems associated with changes in technologies, and attitudes and business models are unlikely to emerge. Without such diversity, only a narrow range of approaches may be legally permissible and realistic comparisons by users or effective competition are both impossible. In particular, a suitably large number and wide range of national settings may be needed to permit firms to pursue innovations that provide valued protections (which may be more effective or more feasible under different regulatory regimes). For instance, if the legal regime in one country allows more discretion to e.g. cloud computing providers, this may result in a solution that solves a sector-specific problem. That same discretion may allow authorities in that country to observe new violations of privacy, which might lead to a strengthening of the law. However, without a standard of comparison, it would be difficult to identify and to assess such innovations; if they are effectively prohibited there will be no opportunity to explore them under real market conditions. This is not limited to what firms actually do, but extends to *transparency* whether firms can convincingly demonstrate compliance and effective protection, and thus reap market rewards when their innovations align with data subjects' needs. Both innovation and the availability of transparent and credible performance information are necessary for the growth of privacy-friendly cultures in business. They are also necessary to resolve the *paradox of privacy* (that data subjects value privacy in surveys but are unwilling to pay for it or to change their behaviour in order to protect it). If a wider range of options and better information become available, consumer preferences can be refined in light of experience and choice can better reflect actual preferences. From the competitiveness perspective, above the innovation threshold step-change (CAPEX) innovations can emerge, which reduce entry costs to the innovator but do not increase end-user prices. Under suitable conditions, the resulting services or solutions[117] may be supplied at low or zero marginal cost to other firms, improving privacy while reducing prices – but this may require regulatory intervention, because possession of such solutions is a barrier to rivals' entry and a source of market power.

[115] Leon et. al. (2012).

[116] See e.g. Korff (2002), Olavsrud (2012) and Robinson et. al. (2009).

[117] E.g. public-key encryption applications that can be 'bolted on' to data transfer services.

Technological and service neutrality

The example of anonymous profiling shows that constructive ambiguity or technological neutrality in drafting can stimulate useful innovation. In this case, it is regarded as having protected consumers' legitimate privacy interests while making available to them levels of personalised service previously available only through intrusive identified profiling. On this basis, the technique has spread to US markets, constituting a genuine competitive advantage for the European developers. Moreover, anonymisation eliminates the costs of obtaining consent, which are in some circumstances sufficient to prevent deployment and which in other circumstances militate strongly in favour of large US-based providers with enormous installed user bases. In the view of those interviewed, the proscriptions in Article 20 of the proposed Regulation will invalidate this innovation. The broader lesson is not to judge a service or technology by its first or most visible application, but to adopt a rule of reason or incentive-based approach.

Public-private cost- and responsibility sharing

The perspectives developed in Chapter 3 have concentrated on competition and innovation in the private sector; a related area not explicitly covered is shared responsibility - industry and regulators (DPAs) working together for a common good (compliance and protection of fundamental human right). In this domain, the data protection value network is so complex that society expects (through the prism of legislation and regulation) industry to do all the innovating whilst the regulators limit themselves to checking over these binding corporate rules (BCRs), Service Level Agreements (SLAs) and onward agreements with pen and paper. This provides an interesting counterpoint to the perceived risks of regulatory capture that motivates the current emphasis on DPAs independence. In relation to this, the proposed Regulation provides for the establishment of a European supervisory body[118], which is expected to have a stronger position to support harmonisation in the interpretation of data protection legislation across Member States.

The law of unintended consequences

There are some potential adverse consequences to the success of the new Regulation. Behaviour may be brought into line and remain there due to a lack of innovation; to the extent that European firms lose global competitiveness, this may be compensated by dominance in the EU market behind the shelter of the Regulation. But most of the cases revolve around scale, automation and the pervasive use of ICTs (processing power, storage and ubiquitous resilient connectivity). The Regulation creates a demand for a wide range of monitoring and compliance data, which will increase with the range and intensity of covered activity. The rapid expansion of personal data flows, and the expected increases (coming from eHealth, financial services and the migration of end-user personal data to the cloud), are likely to produce a glut of data for DPAs to analyse; they may not have the capacity or the tools to do so.

[118] Chapter VI of the Regulation Proposal introduces the European Data Protection Board.

4.3. Lessons regarding competitiveness

To summarise the implications of the options for competitiveness, it is useful to translate the privacy principles into a set of stylised facts.

- Overall, the EU framework and provisions take an overarching approach to privacy that is centred on data subjects and pays relatively less attention to specific sectors and types of data, compared to the US.
- As a rule, the protections offered under the existing and proposed EU frameworks are stronger than their US counterparts (where such exist) and compliance is in general more costly.
- Provisions in the EU are therefore more likely to shape market developments than to respond to them in the short run; this may lead to greater homogeneity of practice and greater interoperability of firms handling private information.
- EU privacy provisions are based[119] on a range of requirements, which include transparency[120], legitimate purpose[121] and proportionality; these may interfere with profitable (or even mutually beneficial) processing of personal data, but this depends on specific legal procedures. Overall, they emphasise data subject information and consent if mandatory prohibitions are to be lifted.
- The costs of compliance with privacy provisions may be fixed or variable[122] and different for: large and small firms; European or foreign-based firms; data processors and data controllers; and (at least under Directive 95/46/EC) different across Member States. The same provision may impose fixed costs in one sector or stage of market development and variable costs in another (e.g. if provided 'as a service').
- The benefits to firms of compliance range from lawful access to markets and to business transaction and interoperation possibilities to improved reputation and trust on the part of customers.
- The benefits to customers of privacy protection range from freedom from harms associated with invasion of privacy to new opportunities to obtain better services (from more efficient searches to personalised products) and to control the use of information in order e.g. to exchange it for other things of value.
- Costs to customers of privacy protection arise when they are unable efficiently to obtain and process necessary information or to give meaningful consent, or when the costs of exercising their rights exceed the benefits of doing so.

It is also worth noting that competitiveness can be understood in terms of *relative productivity* of European (as compared to non-European) operators; this in turn gives them better access to and survival in foreign and domestic markets. Cost advantages are only part of the picture; the privacy provisions (as reflected in firm practices, business models and culture) directly affect market access and sustainability. Finally, privacy rules that are well-aligned with customers' actual privacy preferences will contribute to competitiveness by ensuring that compliant firms are better able to capture and defend market share.

---

[119] The EU-US Safe Harbour Agreement uses a modified statement of principles: Notice; Choice; Onward Transfer; Security; Data Integrity; Access; and Enforcement.

[120] This includes notification and a default presumption against processing in the absence of consent or specified sufficient conditions identifying circumstances when processing is necessary.

[121] This requires legitimate purpose and prohibits further processing that contravenes the original purpose.

[122] Fixed compliance costs arise for instance when an entire line of business – like anonymous profiling - must be dropped; variable costs of compliance scale with the records held or the volume of business done (e.g. the reporting requirements under Article 28 of the proposed Regulation.

Starting from this basis, we can identify several ways in which the options affect market outcomes.

4.3.1. Implications arising from compliance costs

- Provisions that create fixed costs of compliance (e.g. those associated with Article 20) create barriers to entry that tend to favour the incumbency of existing firms, protecting profits and inhibiting innovations unless they provide effective compliance at lower cost. Such costs are typically not passed on directly to consumers. Fixed costs are generally spread over a firm's operating volume; the average reduction in operating surplus is therefore likely to be smaller for larger firms than for SMEs.
- Provisions that increase marginal or variable compliance costs (e.g. those associated with Article 28) do not create barriers to entry, but subject compliant firms to competitive disadvantage if they must compete with non-competitive firms. Where the costs fall on all firms, there is no distortion to market entry and exit, but compliance costs are passed on to consumers.
- Where compliance provides greater privacy protection or reliable proof of privacy protection, the costs may be offset by increased demand from consumers to the extent that they value such protection.
- The level of costs for a given firm reflects other aspects of its operational and business models; therefore, European firms may face lower costs of compliance with EU provisions than their American counterparts, because they are acclimated to the European privacy culture and framework. Conversely, EU firms may face a disadvantage in US markets if the higher levels of protection they provide are not valued by US consumers or if their commercial partners in the US are not set up to interoperate in handling personal data according to EU provisions.
- Differential compliance costs or EU and US firms operating in EU and the US markets may therefore affect the relative competitiveness of EU firms in different ways; if EU companies are able to comply with US provisions at lower cost[123] than US consumers' extra willingness to pay for higher levels of protection, they may enjoy a competitive advantage[124]. Similarly, EU firms may enjoy a competitive advantage at home if their compliance costs are lower and/or the levels of protection they are able to offer (and certify) and sufficiently high compared to foreign competitors – even when the latter satisfy the conditions of laid down in EU law.
- The positive-feedback evolutionary dynamics noted in Section 4.1 can work to the benefit of other services with a stronger commitment to privacy along European lines. User social networks can be involved in co-creation of privacy solutions aligned to European law and their preferences; if this 'crowd' is trans-European in size and scope, it can catalyse the export of the underlying networking service abroad; the users helping to increase awareness and appreciation of privacy-friendly approaches, particularly in markets where the dominant incumbents have been seen to have failed to provide adequate privacy provisions[125].

[123] This cannot be taken for granted, despite the higher levels of protection of personal data from private sector intrusion; US laws contain their own requirements regarding access and integrity and do not offer the same protections from government access to personal data. See 2.3.3

[124] The effectiveness of EU principles and pressure from EU firms adhering to these principles in inducing privacy policy changes outside Europe is demonstrated in Langheinrich (2001).

[125] At least as consumers see them; see Leon et. al. (2012).

4.3.2. Implications arising from innovation

- The static effects of privacy protection (competitiveness) must be set alongside the dynamic effects (innovation[126]). Strong privacy protections can induce firms to innovate in order to find more cost-effective ways to comply.
- More specifically, protections that force firms to obtain user consent to profiling and other forms of data processing may lead to innovations designed to facilitate notification and consent or to compensate users for providing consent. The latter amount to *gain-sharing* for data reuse between data subjects and data controllers and can lead the former to provide more and more useful data.

4.3.3. Implications arising from regulatory and market uncertainty

One strand of argument arising from the case studies concerns the impacts of regulatory uncertainty. Such uncertainties arise with respect to both the Directive (due to differences in implementation across the Member States) and the Regulation (due to as yet-unresolved definitional and implementation issues). Some foresee adverse impacts of the privacy provisions coming jointly from restrictions in the provisions themselves and uncertainty as to differences in implementation across MS (which can happen even with the Regulation, which merely makes the provisions uniform and creates a potential point of harmonisation via central oversight), combined with uncertainty as to what the provisions say. There is also uncertainty as to how much people will care about privacy and take action to protect it[127] and how much those processing or reusing private information will be willing to pay for the privilege. In the case of reuse for targeted advertising (see 3.3) this depends on the differential effectiveness of such ads[128] . This applies as well to recommender systems – if people want the same things as their friends do, those friends' behaviour potentially infringes privacy?

A deeper issue concerns the nature of regulation in evolving market contexts. The literature and those interviewed displayed an unresolved tension between:

- a 'suck it and see' approach in which basic protections and regulatory forbearance are used to facilitate natural experiments to see which approaches to (legal, technological or commercial) privacy protection are acceptable and efficient; and
- a precautionary principle approach that seeks to combine high levels of protection for fundamental rights and legal certainty to create a low-risk (if high-cost) environment within which users and firms are willing to experiment.

Those holding the former view believe that countries that pursue a precautionary principle in applying privacy provisions to innovations are less likely to explore new services and business models in order to ensure that privacy is protected once the potential threats are known. This was the thinking behind the often-repeated assertion that Facebook or Google would not have started in Germany (discussed in Section 4.1);

This has a further implication in relation to the effectiveness or legal soundness of putting responsibilities on firms, data subjects, data controllers, etc. The main argument on this side is that acting in advance of market outcomes risks two kinds of errors (excluding uses of personal information that are justified in the view of all parties and encouraging

[126] Which determines future competitiveness.

[127] The literature [Asay (2012) and Westin (2003)] indicates that preferences evolve in response to experience and information, which are in turn influenced by laws and regulations.

[128] And thus on personal attitudes combined with the relevance and specificity of the targeting permitted by the available information.

protections/precautions that are not justified compared to the (counterfactual) case if they were allowed to develop.

On the other hand, the protections offered by a strong and pre-emptive law include protection from competition arising outside EU data privacy protections; such competition could, if successful, undermine the principles as well as the practices of EU data protection in subtle ways. This approach is viewed by many of the SMEs and EU-based firms as offering a stable legislative framework, which gives certainty to industry and defines rules and levels playing field; such countries are more likely to explore privacy friendly services and business models.

The evidence is mixed, though it seems reasonable to suggest that the former approach leads to innovations that can enhance privacy as a by-product of commercial innovation while the latter approach reinforces innovations aimed primarily at privacy. It may also follow that the latter setting is more congenial to the development of an identifiable data privacy protection subsector of the data processing industry.

Privacy protections must work together with market forces

The extent to which market behaviour can effectively protect privacy – whether or not consumers have powers of consent- is uncertain. Consumer choice on its own is unlikely to suffice. Privacy protection involves certifiable or visible processes and facilities, but also monitoring and a privacy-respecting business culture. Levels of protection are hard for end-users to observe directly and enforce through switching behaviour and the profitability of privacy-invasive and non-transparent practices poses a constant danger that market forces have not managed adequately to control.

Individuals have different preferences as well – a one-size-fits-all policy by providers is unlikely to meet their needs, let alone to respond as those needs develop. If privacy policies were transparent and switching was easy, market discipline could produce an efficient matching of user preferences and service provider policies – but policies are rarely understandable and switching is rare. An alternative is to give users greater control over their data, but the effectiveness of end-user controls has thus far been shown to depend on very small differences in provision[129].

Implications arising from regulatory variation

The Regulation replaces national implementation of the requirements of Directive 95/46/EC with a single set of provisions and a single point of oversight and control. This uniformity, it is argued, will diminish compliance costs. This likely to be true of companies operating mainly in countries with very different regimes and especially those doing business primarily in the currently 'gold-plated' countries. Firms currently working across borders may already have Europe-wide policies based on the most restrictive regime in which they operate.

However, differences in national approaches – in an ideal world – reflect differences in national circumstances including other laws, market conditions and citizen preferences. A greatest common multiple uniform approach would not be only efficient unless the (commercial and technical) costs of complying with stricter standards outweigh the costs and complexities of using multiple standards – including restrictions on the ability to interoperate across countries within the firm and to modularise data processing functions.

[129] Leon et. al. (2012).

Such considerations apply in particular to foreign firms contemplating entry into EU markets; the need to comply with a multitude of rules makes entry more expensive unless it complies with the strictest standard or unless the entrant is able to 'divide and conquer' specific countries[130]. Adopting a uniform standard makes such entry easier[131]; but it also makes mutual recognition systems (along Safe Harbour lines) easier to negotiate and implement.

As one of the experts consulted for the study observed:

> *"As an economist, I would be inclined to see this as a particularly strong reason to favour uniformity, but I can hear an infant-industry argument suggesting that this will limit the growth and development potential of new EU-based players if they are exposed to the big cost and reputation advantages of overseas competitors before they have managed to turn privacy-respecting business and service models to their competitive advantage."*

4.4. Lessons regarding innovation

Many of the implications for innovation have been developed above in terms of their competitiveness implications. However, a few merit further specific discussion.

Adoption of a single standard legal framework will make it easier to set up a business or to develop a product. This may in turn encourage the development of compliance or certification services as a separate line of business activity, and will certainly lower the costs and increase the rewards of creating innovation-friendly products and services (see 3.6.3).

From another perspective, the uniform framework may make it easier for businesses within the EU to achieve an EU-wide user base, which can make strengthen their position and perhaps make it easier for them to develop new products and services (by *crowdsourcing* innovation-friendly solutions from their trans-European installed base of customers and suppliers) and to export products/services outside the EU. This may lead to an increase in trust.

4.5. Comparing the options

This section analyses the effectiveness, efficiency and coherence of the options within the limited focus of this briefing (the impacts on competitiveness and innovation of the provisions regarding profiling, documentation responsibilities and data transfer).

4.5.1. Option 0

As indicated by the case studies, measures under Option 0 would provide effective harmonisation of rules within the European Union.

However, the measures specified are likely to lead to differential impacts on firms of different sizes, firms based inside and outside the European Union, firms in different market segments in the global data processing value network and firms fulfilling different roles (e.g. data controller/data processor) within the data processing industry per se.

[130] This has been seen in other contexts e.g. International call termination. [Courtade (2006)].

[131] But they may face greater competition as previously-isolated markets become more trans-European.

These cost differentials may favour large and established firms, and especially incumbent network service providers. Smaller firms and firms operating more in the service layers of the information economy are less linked to existing – and geographically localised – infrastructures and are therefore more likely to seek to compete in global and foreign markets. Their domestic cost disadvantages may weaken their ability to create and sustain market penetration; at the same time, the economies of scale that encourage them to use business models compliant with the provisions foreseen in Option 0 may make them uncompetitive with foreign firms on cost grounds. On the positive side, the same economies of scale (using a single, privacy-friendly model) may allow such firms to deliver higher levels of privacy protection more cheaply and effectively than foreign rivals, allowing them to attract a loyal customer base among overseas and global customers who value privacy.

In contrast, the burdens of compliance (and thus the costs of access to European partner firms and consumers) are likely to be higher for foreign firms seeking to enter European markets. This may provide a degree of protection to the European data processing industry. On the other hand, given the current dominance of large overseas-based providers in key market segments (including social networking and many aspects of e-Commerce), the effective enforcement of stronger privacy protections may restrict the access of European Internet users to (non-privacy orientated) innovations.

More worryingly, the close linkage of current provisions to current technologies and their potential hazards (especially with regard to profiling) may undercut privacy friendly innovations such as anonymous profiling. This may increase the effective cost to European customers of obtaining the enhanced level of service provided by such innovations, while at the same time preventing European firms from consolidating the market advantage provided by the uptake of these innovations overseas.

Therefore Option 0 is likely to lead to harmonisation but not to the associated neutral competitive environment.

Enforcement is likely to be consistent across the European Union, but may be inconsistent across market sectors and firm characteristics to the extent that larger firms are more easily able to innovate and adopt cost-effective compliance procedures, while smaller firms may be driven out of business. In respect of the documentation requirements laid down in Article 28, evidence suggests that the burden will be greater on data processors than on data controllers and that the resulting large volumes of information may prove difficult to monitor or use in an effective and cost-effective compliance regime. This creates a risk that effective enforcement will be greater in the core than in the long tails of the industry.

The foregoing arguments also suggest that the burdens of compliance will not be minimised, and that they may distort innovation effort. In particular, larger firms may be better able to meet their obligations through fixed cost investments, while smaller firms and firms who find it necessary to purchase privacy compliance as a service may therefore face entry as well as cost hurdles.

Individual control of personal data as laid down in the proposed Regulation is reasonably secure, but technical difficulties with defining, implementing and monitoring consent requirements[132] may limit their effectiveness. In addition, user control may allow some firms to enjoy differential levels of responsibility if they are better able to secure consent.

Protection when data are processed abroad should remain effective, especially as regards incentives for foreign-based data controllers to adopt compliant policies in order to retain

[132] See e.g. Sections 3.3.2 3.4.2 and 3.5.2

access to business opportunities based on processing of EU-based data. However, with the growing prevalence of location-independent data processing and demands for ubiquity of access, data subjects may not be able to control or verify whether transfers of their data are massive or frequent. Thus, they may not be able to opt out of small, infrequent but potentially damaging transfers or to opt into transfers that align with their preferences.

Accountability in the formal sense will be strong, but the disproportionate burden of documentation requirements on small players and the retention in the language of the Regulation of legacy roles and business models may limit the benefits of formal accountability in terms of accountability to data subjects and others making legitimate use of personal data. In addition, if large incumbent firms are better able to secure consent or are able to provide privacy policies that are difficult for users to understand[133], accountability may be weakened.

4.5.2. Option 1

Option 1 shares with Option 0 a harmonised stance regarding the implementation (Objective 1.1) and enforcement (Objective 1.2) of the privacy provisions. It also clarifies the rules, by restoring explicit links to natural persons and removing the potentially confusing exemption for data transfers that are not 'frequent or massive.' By limiting the freedom from automated processing to identifiable subjects, it permits innovation in the direction of privacy-friendly profiling and targeting applications and business models, and thus offers a more neutral and open competitive environment without compromising essential privacy protections. These advantages arise both in terms of competitiveness (through exploitation of existing *privacy by design* innovations) and innovation (by permitting the development and initial deployment of compliant alternatives that may be adopted). The need for flexibility arises because the trade-offs between privacy and other benefits may not be obvious until end-users have gained experience with a new service or business model. Option 1 permits such natural experiments to be conducted while the expected level of individual protection is maintained.

The burden of red tape is also reduced; Option 1 limits documentation to the level necessary to determine whether firms are offering meaningful choice to their clients and thus allows market discipline to supplement formal regulation. The use of trust hierarchies allows burdens to be allocated to those stakeholders best able to bear them and to take effective action to minimise compliance burdens by minimising risks to privacy.

4.5.3. Option 2

Self- and co-regulation, almost by definition, do not guarantee harmonised rules. Different self-constituted bodies are able to choose the codes, rules and standards they adopt, and the mechanism by which compliance is monitored and enforced. This variation is not likely to run along national lines, however, Option 2 should also help to reduce the Single Market barriers resulting from current national differences in implementation[134]. The co-regulatory option (e.g. Safe Harbour) whereby public authorities support self-regulatory decisions that comply with specified public policy principles (in this case, those laid down e.g. in Directive 95/46/EC) does provide some harmonisation, but there is no guarantee of its effectiveness and some risk that different rules will be used to restrain competition. On the other hand, the possibility of adopting different privacy codes and the ability of service providers and their clients to choose between them does enhance the scope for competition and

[133] Leon et. al. (2012).
[134] See Section 2.3.1.

innovation. In particular, the ability of consumers to choose between different certification schemes helps to clarify and 'price' their evolving willingness to pay for privacy protections and to eliminate unduly restrictive precautions.

Option 2 allows greater sector specificity though this may be exploited for the benefits of data controllers and processors rather than data subjects. In particular, as seen with privacy policies on social networking sites, industry-provided privacy policies and controls may not allow data subjects consistently to protect their interests.

It is likely that industry stakeholders will play more prominent roles in self-regulatory arrangements than data subjects and that larger firms and more central market segments will hold the balance of power. This may produce competitive distortions, but it may also militate in favour of placing the locus of decision on those best able to take action. This may be especially important as regards data transfers, since stakeholder bodies may be able to internalise the legal liabilities of their members and implement mutual recognition arrangements similar to the essentially co-regulatory Safe Harbour agreement. This can be reinforced by co-regulation, to the extent that government bodies are willing to impose effective and demonstrable location-independent data protection practices as a condition for recognition.

Self-regulatory arrangements also offer different rules compared to formal regulation[135]. The rules adopted may be stricter than those enshrined in public law, especially in cases where the industry reputation effect is stronger than the actual threat to the public interest, or where a sector-specific body (e.g. in finance or health) is able to adopt much stricter measures than would be appropriate for general regulation. Levels of compliance may also be different; rules created by industry stakeholders may be easier to comply with because they will factor in the full costs of compliance and balance them against the (market and other) consequences of non-compliance. Where reputational effects for the sector as a whole are stronger than those for individual firms and where individual non-compliance is difficult to verify and assess unless detected by (self-) regulatory scrutiny, there is a risk that having the rules is regarded as sufficient and enforcement is a costly – or even damaging (because it reveals non-compliance to the world) addition.

4.5.4. Summary Table

The following Table briefly compares the options in terms of effectiveness, efficiency and coherence based on the analysis in Section 4.2.

[135] See Cave et. al. (2008).

Table 11: Summary table

Option	Option 0	Option 1	Option 2
Effectiveness linked to objective 1: internal market dimension of data protection			
1.1 Harmonising and clarifying rules to provide neutral competitive environment	+/- Harmonisation reduces national asymmetries, but some competitive distortion	+/+ Harmonised, clarified rules; scope limited to direct risks, competition balances protection, value of Personal Identifiable information (PII)	-/+ Variation by self-regulatory body; *choice of rules* levels playing field, adaptation
1.2 Consistent enforcement across jurisdictions, sectors and firms	+/- Consistent across jurisdictions, some variation by sector and firm size/type	+/+ Retains single Regulation, clarified enforcement	+/-- Consistent across jurisdictions, but likely to vary across sectors; possibly weak enforcement
1.3 Cutting red tape	+ Some reduction through unified requirement; additional burdens for processors	+++ Burdens minimised and used as incentives	++ Lowest burden, but not necessarily aligned with data subject interests
Effectiveness linked to objective 2: fundamental right to data protection			
2.1 Individual control of data and trust in digital environment	+ Provides personal control, but may not be effectively exercised due to consent problems	++ Limits complexity of data subject choices; consent may still be problematic for e.g. cloud, big data	++ May allow more understandable PLA[136], but potential for confusing choice.
2.2 Protection when data are processed abroad	++ Enhanced incentive for offshore compliance; protection depends on size and frequency of transfers; may inhibit mutual recognition	+++ Size and frequency asymmetries removed; incentive for providers to make contractual protections explicit	+ Indirect control possible through *Safe Harbour* types of arrangements, conditional co-regulation.
2.3 Accountability and responsibility	++ New obligations on data controllers and processors	+++ Accountability obligations aligned with data subject interests; increased role for PLAs	- Limited by market forces.

[136] Privacy Level Agreement – see Section 3.5.1.

Option	Option 0	Option 1	Option 2
Efficiency			
Minimising costs and other burdens	++ Decreased localisation costs, but undercuts existing business models (esp. profiling) and imposes data handling burdens on processors and regulator; costs may be lower for large, incumbent firms.	+++ Decreased localisation costs, enhanced revenues from profiling, cloud, big data and sales of PETs, lower documentation costs, wider geographic market scope for small and innovative firms	+ Costs minimised by industry input to rulemaking; costs lower for firms with significant market power unless competition rules applied to self-regulatory bodies.

4.5.5. Preferred option

Option 1 is the preferred option because it retains the harmonisation, transparency and effectiveness benefits of the proposed Regulation, while sustaining privacy-friendly business models developed under Directive 95/46/EC and enabling innovations in light of continuing technological, market and societal evolution. The ability to rebalance and reallocate transparency requirements should strengthen partnerships between data controllers and processers without compromising data subject interests. This focusing of data flows should also simplify the monitoring and enforcement requirements on Data Protection Authorities and facilitate oversight by the European Regulator. This option also removes time-bound asymmetries as regards the potentially beneficial uses of profiling and removes existing obstacles to the development of cloud computing and big data analytics. However, because it maintains the data protection principles underlying the existing framework, it provides an additional impetus to the development of privacy-friendly technologies orientated towards European data protection expectations.

This offers three additional advantages to European citizens and firms. First, it ensures that the foreign firms that currently occupy prominent positions in delivering data-intensive services to European citizens can continue to make these services available because necessary modifications to their technological or business practices to conform to the new Regulation are defined in functional terms and compatible with the best of current European practice. This in turn may encourage them to license compliant services from European firms or to purchase them as add-ons to their current services. European firms would be strongly competitive in an emergent domestic *privacy as a service* market.

A second additional advantage is that the development of a more dynamic and competitive privacy layer in the European data processing industry would provide an enhanced base for European firms seeking to compete in world markets. As the example of anonymous profiling demonstrates, the relatively fragmented and ineffective privacy protections available to citizens of the US (for example) does not represent a fundamental difference in privacy provisions or an inability of US providers to implement privacy-respecting technical and business models; rather, it is a form of lock-in – customers do not demand what they have not been offered, and firms do not provide what is not demanded. Of course, there may be a price to pay for this dissemination of European standards of privacy protection. Once global rivals have risen to the challenge, the domestic competitiveness of European firms may be undercut – but this will work to the advantage of European citizens. All users, however, may face an increase in the cost of services currently supported by service

provider revenues arising from reuse of personal data. However, Option 1 makes it possible to negotiate mutually beneficial alternatives in which data subjects participate in the economic gains from reuse of their data without risk to their fundamental data rights. In other words, subject control is potentially enhanced by extending to the market for personal data.

The third potential advantage is more long-term and derives from the legal certainty, uniformity and innovation friendliness of the preferred option. The co-evolution of the demand for and supply of data protection is likely to provide a growth engine capable of offering sustained benefits as new applications (exemplified here by profiling, cloud computing and big data) continue to develop. This can be seen as a 'win-win' response to the current economic crisis; if the only route to economic recovery is increased global trade and competition, it will be necessary for Europe to find a recovery strategy that builds on a unique and valued understanding of the value of privacy. Otherwise, there may be a stark choice between an increasing loss of control in exchange for the benefits of participation in an increasingly globalised Internet economy that runs on personal data, and loss of access to the most dynamic markets and advanced services.

REFERENCES

- Acquisti A. and Grossklags, J. (2004) "Privacy Attitudes and Privacy Behaviour: Losses, Gains, and Hyperbolic Discounting" in J. Camp and R. Lewis (eds.) The Economics of Information Security, Kluwer.
- Acquisti A., Friedman, A. and R. Telang (2006) "Is there a cost to privacy breaches? An Event study" pre-proceeding draft 27th International conference on Information Systems Milwaukee 2006 and Workshop on the economics of Information Security 2006 available at: http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf [visited 12/11/2012].
- Acquisti, A. L. John and G. Loewenstein; (2010) "What is Privacy Worth?" Leading paper, 2010 Future of Privacy Forum's Best "Privacy Papers for Policy Makers" Competition.
- Act, F. (2009) "Fair Credit Reporting Act" Flood Disaster Protection Act and Financial Institute.
- Akhigbe, A. and Whyte, A. (2004) "The Gramm-Leach-Bliley Act of 1999: Risk implications for the financial services industry" *Journal of Financial Research* 27(3): 435–446.
- Asay, C. (2012) "The Impact of EU Privacy Regulation in the US" *JURIST – Forum* (Nov. 9, 2012) at: http://jurist.org/forum/2012/11/clark-asay-eu-privacy.php.
- Birnhack, M. D. (2008). "The EU Data Protection Directive: An engine of a global regime." Computer Law & Security Review 24(6): 508-520.
- Bodogh, Z. (2011). "Privacy Issues of the Internet Search Engines-In the Light of EU Data Protection Legislation." Masaryk UJL & Tech. 5: 163, pp. 174-175.
- Bollier, D. (2010) "The Promise and Peril of Big Data" The Aspen Institute.
- Bradshaw, D., Folco, G. Cattaneo, G. and Kolding, M. (2011) "Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Uptake. SMART 2011/0045 D4 Final Report". IDC.
- Brynjolfsson, E, L. M. Hitt and H. H. Kim (2011) "Strength in Numbers: How Does Data-Driven Decisionmaking Affect Firm Performance?" available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1819486.
- Burnside, R. (1987) "Electronic Communications Privacy Act of 1986: The Challenge of Applying Ambiguous Statutory Language to Intricate Telecommunication Technologies" *Rutgers Computer & Tech. LJ* 13: 451.
- Camden, B. (1989) "Fair Credit Reporting Act: What You Don't Know May Hurt You" 57 *U. Cinn. L. Rev*. 267.
- CapGemini (2012) "The Deciding Factor: Big Data & Decision Making" Report.
- Cave, J., Marsden, C. and S. Simmons (2008) "Options for and Effectiveness of Internet Self- and Co-Regulation" Report for European Commission. Available at SSRN: http://ssrn.com/abstract=1274571.
- Cave, J., Robinson, N., Kobzar, S. and Schindler, R. (2012) "Regulating the Cloud: More, Less or Different Regulation and Competing Agendas." TPRC.

- Cave, J., Robinson, N., Schindler, R., Bodea, G., Kool, L. and M. van Lieshout (2011) "Does it help or hinder? Promotion of innovation on the internet and citizens' right to privacy" A study for the European Parliament Committee on Industry, Research and Energy reference. IPOL-ITRE_ET(2011)464462 available at: http://www.europarl.europa.eu/committees/fr/studiesdownload.html?languageDocument=EN&file=65871.
- Cavoukian, A and Khaled E. (2011) "Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy" Information and Privacy Commissioner Office of Ontario Available at http://www.ipc.on.ca/images/Resources/anonymization.pdf
- Cavoukian, A. (2008) "Privacy in the clouds" *Identity in the Information Society* 1(1): 89-108.
- CEBR (2012): "Data equity: Unlocking the value of big data", Report for SAS, April 2012.
- Cohen, J. E. (2013) "What is Privacy for?" *Harvard Law Review* (forthcoming) available at: http://www.harvardlawreview.org/symposium/papers2012/cohen.pdf [visited 12/11/2012].
- Costa, L. and Y. Poullet (2012) "Privacy and theRegulation of 2012" *Computer Law & Security Review* 28(3): 254-262, p. 259.
- Council of the European Union (2010) "Council Decision on the conclusion of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program" 24 June 2010. See www.statewatch.org/news/2010/jun/eu-usa-draft-swift-agreement-com-final-3.pdf.
- Courtade, T. (2006) "A Strategic Guide on Two-Sided Markets Applied to the ISP Market" *Communications & Strategies* No. 61. Available at SSRN: http://ssrn.com/abstract=976591.
- Cukier, K. (2010) Data, data everywhere, *The Economist*, February 2011 Available at: http://www.economist.com/node/15557443.
- Danezis, G. and S. Gurses, (2010) "A critical review of 10 years of Privacy Technology" in "Proceedings of Surveillance Cultures: A Global Surveillance Society?" Berlin: Springer.
- Dwyer III, S., Weaver, A. and K. Hughes (2004) "Health Insurance Portability and Accountability Act" in "Security Issues in the Digital Medical Enterprise" Society for Computer Applications in Radiology, second ed., April 2004.
- EC Court of Justice (2006) "Joined Cases C-317/04 and C-318/04: Judgement of the Court (Grand Chamber) of 30 May 2006 — European Parliament v Council of the European Union (Protection of individuals with regard to the processing of personal data — Air transport — Decision 2004/496/EC — Agreement between the European Community and the United States of America — Passenger Name Records of air passengers transferred to the United States Bureau of Customs and Border Protection — Directive 95/46/EC — Article 25 — Third countries — Decision 2004/535/EC — Adequate level of protection)" document C2006/178/02 at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:178:0001:0002:EN:PDF.

- European Commission (2007) "Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing"
- European Commission (2010a) "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: A Digital Agenda for Europe" COM(2010) 245 final/2
- European Commission (2010b) "COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Delivering an area of freedom, security and justice for Europe's citizens Action Plan Implementing the Stockholm Programme" COM(2010) 171 final
- European Commission (2012a) "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)" Brussels, 25.1.2012, COM(2012) 11 final, 2012/0011 (COD).
- European Commission (2012b) "Impact Assessment Accompanying the document 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) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data" COMMISSION STAFF WORKING PAPER SEC(2012) 72 final at: http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2012/sec_2012_0072_en.pdf.
- European Commission (2012c) "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses" Press release accompanying European Commission 2012a, Reference: IP/12/46, available at: http://europa.eu/rapid/press-release_IP-12-46_en.htm.
- Federal Trade Commission (1998). Privacy online: a report to Congress Federal Trade Commission, June 1998 at: www.ftc.gov/reports/privacy3/toc.htm.
- Feldman, B. (2012) "Big Data in Healthcare" DrBonnie360 Report Available at: http://rockhealth.com/2012/10/rock-report-big-data-healthcare/.
- Gatzlaff, K. M. and McCullough, K. A. (2010) "The Effect of Data Breaches on Shareholder Wealth" *Risk Management and Insurance Review* 13: 61–83.
- Hildebrandt, M. and Koops, B-J (2010) "The Challenges of Ambient Law and Legal Protection in the Profiling Era" *The Modern Law Review* 73: 428-460.
- Hon, K., Millard, C. and Walden I. (2011) "The Problem of 'Personal Data' in Cloud Computing – What Information is Regulated? The Cloud of Unknowing, part 1". Queen Mary, University of London.

- http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0171:FIN:EN:PDF.
- http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF.
- IBM Global Reputational Risk and IT study (2012) available at http://www-935.ibm.com/services/us/gbs/bus/html/risk_study-2012-infographic.html [visited 12/11/2012].
- IDC (2012) "IDC Releases First Worldwide Big Data Technology and Services Market Forecast, Shows Big Data as the Next Essential Capability and a Foundation for the Intelligent Economy" Press release 7/3/2012 Available at: http://www.idc.com/getdoc.jsp?containerId=prUS23355112.
- JRC (2012) *Smart Grid projects in Europe: lessons learned and current developments*, JRC Reference Report, Joint Research Center, 2012 Available at: http://ses.jrc.ec.europa.eu/sites/ses/files/documents/smart_grid_projects_in_europe_lessons_learned_and_current_developments.pdf.
- Katz, M. and C. Shapiro (1994) "Systems Competition and Network Effects" *J. Econ. Perspectives* 8: 93–116.
- Korff, D (2002) "EC Study on Implementation of Data Protection Directive 95/46/EC" at: http://ssrn.com/abstract=1287667.
- Langheinrich, M. (2001) "Privacy by design—principles of privacy-aware ubiquitous systems." "Ubicomp 2001: Ubiquitous Computing". Springer Berlin/Heidelberg.
- Leon, P. Ur, B., Shay, R., Wang, Y., Balebako, R. and L. Cranor (2012) "Why Johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising" 40th TPRC, Arlington, Va.
- Lundgren, I. (2012) Mobile Industry Wants To Turn Its Mobile Data Into A Big Data Business, Launches Dynamic Insights Unit, *TechCrunch* 8/10/2012 Available at: http://techcrunch.com/2012/10/08/Mobile Industry-wants-to-turn-its-mobile-data-into-a-big-data-business-launches-dynamic-insights-unit/.
- Massey, A., Otto, N., Hayward, L. and A. Antón (2010) "Evaluating existing security and privacy requirements for legal compliance" *Requirements Engineering* 15:119–137.
- McAfee, A. and E. Brynjolfsson (2012) "Big Data: The Management Revolution" *Harvard Business Review Online*, October 2012.
- McCarthy, M. (2002) "USA Patriot Act," *Harv. J. on Legis.* 39: 435.
- McKinsey (2012) "Big data: The next frontier for innovation, competition, and productivity" Report.
- McNamara, R. (1973) "The Fair Credit Reporting Act: A Legislative Overview" 22 *J. Pub. L.* 67
- Mell, P. and Grance, T. (2009) "The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology". NIST Special Publication 800-145
- Ohm, P. (2010) "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" *UCLA Law Review* 57: 1701.

- Olavsrud, T. (2012) "EU data protection regulation and cookie law - Are you ready?" *Computerworld UK* 24 May 2012 at: http://www.computerworlduk.com/in-depth/security/3359574/eu-data-protection-regulation-and-cookie-law--are-you-ready/.
- Parsons, P. and R. Frieden (1998) "The cable and satellite television industries" Allyn & Bacon, 1998.
- Robinson, N., Graux, H., Botterman, M. and L. Valeri (2009) "Review of the European Data Protection Directive" Report to the UK Information Commissioner's Office at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.pdf.
- Schaffer, G. (2002) "Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance through Mutual Recognition and Safe Harbor Agreements." 9 Columbia Journal of European Law 29-77 (Fall 2002).
- Schwartz, P. (2000) "Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices" 2000 Wis. L. Rev. 743.
- Serwin, A. (2010) "The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices. (Version 2.0)." December 31, 2010. Available at SSRN: http://ssrn.com/abstract=1733217 or http://dx.doi.org/10.2139/ssrn.1733217.
- Taylor, P. (2012) "Crunch Time for Big Data" *Financial Times*, 19/06/2012.
- Tene, O. and Polonetsky, J, (2012) "Privacy in the Age of Big Data - A Time for Big Decisions" *Stanford Law Review Online* 64(63) 02/02/2012.
- Terry, N. (2012) "Protecting Patient Privacy in an Age of Big Data" Available at http://ssrn.com/abtract=2153269.
- United Kingdom Cabinet Office (2012) "Open Data White Paper: Unleashing the Potential" at: http://www.cabinetoffice.gov.uk/sites/default/files/resources/CM8353_acc.pdf.
- United Nations (2012) "Big Data for Development: Challenges & Opportunities" UN Global Pulse Report, May 2012.
- United States Government (2012) "Consumer Data Privacy in a Networked World: A framework for protecting privacy and promoting innovation in the global digital economy" Washington: White House, February 2012.
- Weitzner, D., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J. and G. Sussman (2008) "Information accountability" *Commun. ACM* 51(6): 82-87.
- Westin, A. (2003) "Social and Political Dimensions of Privacy" *Journal of Social Issues* 59(2): 431—453.

ANNEX 1. INTERVIEW PROTOCOL

INTRODUCTION: POLICY AND STUDY CONTEXT

A previous study commissioned by the ITRE Committee ("Does it help or hinder? Promotion of innovation on the internet and citizens' right to privacy")[137] established that data processing industries in the US and the EU have taken slightly different turns because of the very different level of data protection at federal US level compared with EU standards, and the associated comprehensive data protection framework at the EU level.

There does not, however, appear to be a comprehensive and reliable assessment of the real effects of the 95/46/EC Data Protection Directive on innovation and competitiveness in EU industries, any resulting differences as compared to their US counterparts and the extent to which the proposed data protection Regulation (COM 2012/0011) is likely to change this situation.

Some differences in data protection obligations and in data processing developments are evident even to the casual observer. For instance, the EU obliges the processor and controller to ensure that the data subject enjoys the benefits of data protection even if the personal data is processed outside of the Union. Possibly as a result, EU data processing industries appear to be active more in the business-to-business layer of data processing services than their US counterparts, which tend to focus on the business-to-consumer end.

The purpose of the interview is to garner greater insight into stakeholder understandings of the current and proposed EU data protection provisions, the mechanisms by which these provisions affect innovation and the implications for EU competitiveness.

Scope: As much as possible, opinions/arguments are to: be validated by/based on existing case law, offer concrete figures and statistics (and provide sources) and/or be supported by concrete illustrative examples. Where specific evidence is not ready to hand, subjects should be asked to identify potential sources of which they are aware.

Interview time: 30-45 mins.

CONFIDENTIALITY

Q A1: Would you like to conduct this interview under Chatham House Rule? [Y/N]

As a default option, interviews will be held under the Chatham House Rule. It allows the study team to use the information received, providing neither the identity nor the affiliation of the interviewee(s) are revealed. However, at the beginning of the interview, interviewees will be informed about their rights and offered the opportunity to answer publicly, with the possibility that they may be called to the European Parliament to present their position in person.

[137] http://www.europarl.europa.eu/committees/fr/studiesdownload.html?languageDocument=EN&file=65871

PROFILING

Q B1: Which sector do you represent?

Public sector:

- Government or public service delivery
- local, regional, national
- Europe, USA
- Other

Private sector:

- Data processing, user of data processing, other
- Company size
  - Micro (1-9 persons employed)
  - Small (10-49 persons employed)
  - Medium (50-249 persons employed)
  - Large (250 or more persons employed)
- % of business activity:
  - How many of your company's employees are based % in Europe?
- % of innovative activity in Europe:
  - Approximately how much does your company invest in innovation (R&D, new product, service or business model development)?
- What proportion of your workforce is actively involved in this innovative activity?
- How many of these are based in Europe?

Citizens/Consumers/Academia:

- local, regional, national, NA
- Europe, USA, NA
- Other

Q B2: Are you aware of the current Data Protection Directive in relation to your business activities?

Q B3: Are you familiar with the proposed new Data Protection Regulation?

- Familiar
- Partially familiar
- Not familiar

Q B4: Have you noticed any concrete impacts of the legislation implementing the current EU Data Protection Directive on your (business) activities? [baseline – all that apply]

- Yes, promoting/preventing specific activities (encouraging or preventing us from offering customer services, creating or changing internal business process requirements, facilitating or inhibiting further processing of data);
- Yes, favouring/restricting the scope and/or geographic spread of services, activities and business processes due to regulatory constraints;
- Yes, a need to invest in Data Protection measures such as installing a privacy officer or initiating an audit procedure;
- Some effects, but nothing concrete or significant;
- No, no impact whatsoever on (business) activities.

IMPACT OF NEW DATA PROTECTION LEGISLATION ON EU COMPETITIVENESS AND INNOVATION

Article 15 of Directive 95/46/EC grants the right ***to every data subject to not be subject to automatic processing ('automated individual decisions')*** producing legal effects or significantly affecting the data subject. This right is further developed in Article 20 ('measures based on profiling') of the proposed Regulation.

The major changes proposed imply that measures concerning natural persons, based on profiling activities, are essentially prohibited when they have a legal or significant effect on the individual. In particular, it no longer matters whether the 'natural person' is a data subject (i.e. an identified or identifiable individual) or not; the prohibition could apply even to profiling that does not identify the individuals involved. Moreover, 'measures' is a broader category than 'decisions' as used in the 1995 Directive; it also covers, for instance, advertising activities. Therefore, for example, it may be (the interpretation is not yet clear) that directing (by email or web content) advertisements to people based on their search behaviour alone (i.e. without any identification) is prohibited.

Q C1.1: Do you think that the existing provision (Article 15) has had an impact (e.g. financial, organisational, business process oriented or technical) on the direction of data processing innovation – in Europe and abroad? If Yes, say how and whether this applies more to specific types of business than others.

Q C1.2: In light of the proposed Regulation, in particular (Article 20), how, if at all, will it (continue to) affect data processing innovation – in Europe and abroad?

Q C1.3: Which impacts do you expect to result from the greater breadth requirements in the proposed Data Protection Regulation as compared with Directive 95/46/EC - in Europe and abroad?

***

Article 17(2)-17(4) of Directive 95/46/EC obliges the data controller to ensure that a data processor is able to fulfil the ***protection requirements of the Directive with regard to the data subject***. This obligation is further developed in Article 28 of the proposed Regulation. The data controller is obliged to have detailed documentation of all processing activities and responsibilities and the contact details of responsible persons. ***The aim of this provision is to require businesses to demonstrate compliance with the Regulation***.

Q C2.1: Do you think the existing control requirements have given rise to any particular new business models or other developments (changes in contacts or services) – for data controllers or data processors side? If Yes, please describe these developments, or at least indicate whether they relate to developments within businesses, among businesses (e.g. business-to-business interactions such as cooperation and mutual agreements), between businesses and (data protection) authorities and/or business-to-consumer interactions?

Q C2.2: This obligation is further developed in Article 28 of the proposed Regulation. What business model, contractual or service effects do you foresee (for private sector interviewees: in your own operations or those of other firms with whom you do business) as a result of the rephrased Article 28? If Yes, please describe either the reasons why current practices have to change or the developments you foresee.

E.g. will the new requirements be handled by standardised business-to-business agreements? Alternatively, will more processing activities remain within one company (in other words, will the roles of data controller and data processor be less likely to be separated)? Can technological and/or organisational measures to ensure and document compliance be part of innovative business models?

Q C2.3: Is it necessary/desirable for the Commission to stimulate privacy friendly business models by specific support measures? If Yes, say which.

Q C2.4: Are such business models likely to lead to improved data protection for European data subjects? Why or why not?

Q C 2.5: To what extent will the impact of such measures taken by the Commission (and the resulting prospects for privacy-friendly business models) be reduced or enhanced by the globalisation of data processing and policy developments in other countries (e.g. US)? a) Considerably enhanced; b) somewhat better; c) mixture of good and bad effects; d) somewhat reduced; e) strongly reduced; f) no difference.

***

Data controllers should ensure that the data subject's right to data protection is not impeded by ***the transfer of data to a third country***. However, Directive 95/46/EC contains an exception from this principle in Recitals 30, 39 and Article 7(f). Compare Recital 38 and Articles 6(1)(f) and 44(1)(h) of the proposed Data Protection Regulation, containing an exception based on controller interest. The restrictions on transfers in Directive 95/46/EC implicitly acknowledge that transfers to non-adequate third countries lead to a reduced level of data protection. Under Directive 95/46/EC, the legitimate business interest of the data controller could not be used to justify transferring data for processing in third countries if those countries did not provide adequate protection. The proposed Regulation does allow such transfers if there is a ***legitimate business interest,*** subject to the documentation requirements described above in relation to Article 28 (namely documentation of data processing and the contact details of responsible parties).

Q C3.1: Do you think that the existing restrictions on data transfers affected the direction of EU innovation in the data processing sector across the EU or within specific Member States? For better or worse? If in your view Directive 95/46/EC affected actual innovation in business models used by EU data controllers, is this effect likely to be magnified or mitigated by the new Regulation?

***

INDUSTRY PERFORMANCE

Existing Data Protection provisions and the proposed Regulation can affect industrial performance in two respects; the indirect costs, benefits and market impacts of the provisions on data controllers and processors who use data in their own business operations; and direct impacts on the data processing industry itself.

Q C4.1: Can you provide us with data on the performance of companies in the data processing industry[138] and the costs and benefits of data processing services to firms who use their services?

Q C4.2: In relation to data processing, do you think that there has been a linkage between innovation and (intra-firm and regional) competitiveness? If so, how can the relationship be measured or analysed?

Q C4.3: Do you think that certain current activities in the field of data processing industries will no longer be possible under the proposed Regulation, or will they require additional measures by businesses (changes in organisation, technology, business process, outsourcing practices, division of responsibilities) to facilitate compliance?

Additional question:

Are you aware of any decisions made by companies to have their main establishment in a specific EU Member State due to a more relaxed approach towards data protection? And, if so, do you think this may change with the introduction of a Regulation, which implies that Member States have no discretionary powers left according to the implementation (in terms of additional requirements or stricter time frames)?

Can the Regulation create a level playing field within the EU and, therewith, possibly promote intra-communitarian competition?

***

[138] The supply side of the data processing industry includes companies whose business involves the provision of data collection, management and processing services; the demand side comprises companies whose business relies on/requires/makes use of data processing.

ANNEX 2. Anonymised List of Interviewees

Name	Organisation / sector
Anonymous	Public sector (DPA)
Anonymous	Advertising Industry
Anonymous	Advertising Industry
Anonymous	Advertising Industry, service provider
Anonymous	Search provider
Anonymous	Privacy academic
Anonymous	EU Telecommunications provider
Anonymous	EU Privacy advocate
Anonymous	EU Privacy lawyer
Anonymous	Data processing industry (supply side)
Maarten Louman	Qiy Foundation (software development)
Peter Lems	Mobihealth
Simon Hania	TomTom
Chiara Giovannini	ANEC
Robert Bond	Speechlys
Michael O'Neil	Baycloud
A. Kupai	BASF

Source: Study Team

ANNEX 3. Comparison of relevant terms of Directive 95/46/EC and proposed Regulation

Table 12: Comparison of provisions relating to profiling

Directive 95/46/EC	Proposed regulation
Article 15: Automated individual decisions	**Article 20: Measures based on Profiling**
1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. 2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision: (a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or (b) is authorised by a law which also lays down measures to safeguard the data subject's legitimate interests.	1. Every natural person shall have the right not to be subject to a measure which produces legal effects concerning this natural person or significantly affects this natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour. 2. Subject to the other provisions of this Regulation, a person may be subjected to a measure of the kind referred to in paragraph 1 only if the processing: (a) is carried out in the course of the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or where suitable measures to safeguard the data subject's legitimate interests have been adduced, such as the right to obtain human intervention; or (b) is expressly authorised by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; or (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards. 3. Automated processing of personal data intended to evaluate certain personal aspects relating to a natural person shall not be based solely on the special categories of personal

Directive 95/46/EC	Proposed regulation
	data referred to in Article 9. 4. In the cases referred to in paragraph 2, the information to be provided by the controller under Article 14 shall include information as to the existence of processing for a measure of the kind referred to in paragraph 1 and the envisaged effects of such processing on the data subject. 5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests referred to in paragraph 2.

Table 13: Comparison of provisions relating to documentation

Directive 95/46/EC	Proposed regulation
Article 17(2)-17(4). Security of processing	**Article 28. Documentation**
2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out, and must ensure compliance with those measures. 3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that: - the processor shall act only on instructions from the controller, - the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor. 4. For the purposes of keeping proof, the parts of the contract or the legal act	1. Each controller and processor and, if any, the controller's representative, shall maintain documentation of all processing operations under its responsibility. 2. The documentation shall contain at least the following information: (a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any; (b) the name and contact details of the data protection officer, if any; (c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1); (d) a description of categories of data subjects and of the categories of personal data relating to them; (e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the

Directive 95/46/EC	Proposed regulation
relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.	legitimate interest pursued by them; (f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards; (g) a general indication of the time limits for erasure of the different categories of data; (h) the description of the mechanisms referred to in Article 22(3). 3. The controller and the processor and, if any, the controller's representative, shall make the documentation available, on request, to the supervisory authority. 4. The obligations referred to in paragraphs 1 and 2 shall not apply to the following controllers and processors: (a) a natural person processing personal data without a commercial interest; or (b) an enterprise or an organisation employing fewer than 250 persons that is processing personal data only as an activity ancillary to its main activities. 5. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the documentation referred to in paragraph 1, to take account of in particular the responsibilities of the controller and the processor and, if any, the controller's representative. 6. The Commission may lay down standard forms for the documentation referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Table 14: Comparison of provisions relating to data transfer

Directive 95/46/EC	Proposed regulation
Data transfer to Third parties. Recital 30,39 and Article 7(f))	**Data transfer to Third countries. Recital 38, Article 6(1)f and 44(1)h)**
R30. Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organisation or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons; R39. Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;	R38. The legitimate interests of a controller may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding. This would need careful assessment in particular where the data subject is a child, given that children deserve specific protection. The data subject should have the right to object the processing, on grounds relating to their particular situation and free of charge. To ensure transparency, the controller should be obliged to explicitly inform the data subject on the legitimate interests pursued and on the right to object, and also be obliged to document these legitimate interests. Given that it is for the legislator to provide by law the legal basis for public authorities to process data, this legal ground should not apply for the processing by public authorities in the performance of their tasks. Lawfulness of processing - Article 6(1)f. 1. Processing of personal data shall be lawful only if and to the extent that at least one of the following applies: (f) Processing is necessary for the purposes of the legitimate interests pursued by a controller, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks. Derogations – Article 44(1)f. In the absence of an adequacy decision pursuant to Article 41 or of appropriate safeguards pursuant to Article 42, a transfer or a set of transfers of personal data to a third country or an international organisation may

Directive 95/46/EC	Proposed regulation
Criteria making data processing legitimate - Article 7(f). Member States shall provide that personal data may be processed only if: (f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)	take place only on condition that: (f) the transfer is necessary in order to protect the vital interests of the data subject or of another person, where the data subject is physically or legally incapable of giving consent;

NOTES