DOI: 10.1007/s10272-013-0470-y

EU Data Protection Reform: Opportunities and Concerns

Last year, the European Commission proposed a comprehensive reform of the EU's data protection rules. The proposed regulation has been surrounded by fierce controversy and has been the subject of frenzied lobbying by global corporations, industry groups, research centres and privacy campaigners on both sides of the Atlantic. This Forum applies cool economic reasoning to this heated issue. What are the potential economic benefits of EU harmonisation? Will the proposed regulation negatively impact the competitiveness and innovation of European firms in the global marketplace? Or could it jeopardise attempts to protect privacy as a fundamental right in civil societies?

Alexander Dix

The Commission's Data Protection Reform After Snowden's Summer

When the European Commission published its proposals for a General Data Protection Directive for the public and private sectors and a special Directive for police and justice matters in January 2012, it initiated a long overdue discussion among European legislators on the protection of privacy in the 21st century. This discussion will have long-lasting repercussions on questions of worldwide competition in the information age. At the same time, this discussion has been taking place under considerable time pressure from the start. Since the European Parliament faces new elections in May 2014, time to reach an agreement on this very important legal framework that will be in force for the next 20 years is extremely short. However, there are examples which indicate that European legislators can act swiftly to adopt secondary legislation where political consensus exists, with the Data Retention Directive 2006/24/EC of 15 March 2006 being the obvious example (which took just two years from the first Council Declaration on Combating Terrorism of 25 March 2004 to the adoption of the Directive).

In the case of the General Data Protection Regulation, which is to replace the Data Protection Directive 95/46/EC, this consensus is much less obvious, to say the least. Almost 4000 amendments have been tabled in the European Parliament, and Member States have not yet reached political agreement in the European Council. The window of opportunity to pass this legislation before the next European Parliament election is closing swiftly, but hope remains that recent developments may contribute to a political consensus just in time.

Why is European harmonisation in the field of data protection economically important? The answer is obvious: if market participants (European and non-European) have to deal with 28 separate legal frameworks, they will encounter considerable problems. The European Union has already achieved a certain degree of harmonisation through the adoption of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. But 18 years after adopting and implementing the Directive, the degree of harmonisation is still insufficient, and Europe therefore remains at a disadvantage in the global competition with other countries and regions such as the US, Southeast Asia and in particular China. Therefore, the Commission has proposed a draft Regulation to cover the private and most of the public sector with a directly applicable legal instrument which will supersede most (not all) of the national legislation on data protection and thus provide for a level playing field.

In addition, the draft Regulation clarifies a crucial point: which law should be applied to a non-European company offering services in the European market? Large Internet companies such as Google and Facebook have for some time taken the view that they should be able to do business according to US law, since they have their

headquarters in the United States. This position has put users in Europe at a disadvantage if they have a need to seek judicial redress against these non-European service providers. It would also seem to contradict the jurisprudence of the US Supreme Court, which has ruled that any foreign company wanting to do business in the US market should comply with US law. Therefore, it would appear to be overdue that the Draft Regulation makes it crystal clear that this principle will in the future also apply to any non-European provider offering services to European citizens. It is, however, fair to say that many US providers have since accepted this self-evident rule.

At the same time, coherent supervision of the new Regulation will be key. A uniform framework is of little value and may still distort competition if it is applied differently by authorities in separate Member States. Therefore, the Commission proposes even closer cooperation among European supervisory authorities, including a "consistency mechanism" to avoid "forum shopping" by non-European data controllers. Both proposals – the directly applicable Regulation and the consistent supervision by national authorities – will increase the attractiveness and competitiveness of the European Union as a marketplace.

In this context, it should be realised that so far data protection very often has been perceived as a barrier to competition. However, this perception is false. One has to remember that the World Trade Organization already made it clear in 1995 that data protection rules are not to be considered as illegitimate trade barriers. The General Agreement on Trade in Services (GATS) explicitly states that its provisions should not be construed to prevent the adoption and enforcement "of laws and measures for the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts" as long as these laws and measures are applied in a non-discriminatory fashion and not as a disguised restriction on trade in services.

Thus, the European Union is in a rather comfortable position in the current negotiations with the US government on a Transatlantic Trade and Investment Partnership (TTIP): there is neither need nor justification to give way to any demands from the US side to decrease the level of data protection in Europe. On the contrary, as the Data Protection Commissioners in Germany and in Europe have rightly suggested, the TTIP negotiations should be used by the EU Commission to convince the US government of the need to introduce federal legislation for the better protection of personal data in the private sector. This could lead to a harmonised and level playing field in a future transatlantic free trade area.

Harmonisation should, however, not be an end in itself. The question is what level of protection is necessary and to what extent this level will influence competitiveness.

This may best be exemplified by the case of cloud computing. Even before Edward Snowden started to reveal the excessive surveillance activities by the US National Security Agency (NSA) and the British General Communications Headquarters (GCHQ), it was evident that there was a considerable gap between Europe and the United States in terms of privacy protection in the private sector. There are stricter requirements for the processing of personal data on servers located outside the European Union than on servers in the Union. This resulted in such a competitive disadvantage for US companies offering cloud services (Google, Amazon, Microsoft, etc.) in comparison to their European counterparts that major US companies openly urged Congress to pass privacy legislation for the private sector.[1] The European Commission has adopted a strategy for European cloud computing, and companies such as the Deutsche Telekom are already offering reliable cloud services.

Furthermore, the Directive 95/46/EC and likewise the Draft General Regulation require an adequate level of data protection in any recipient country outside the European Union. Some have criticised this as the undue

1 See https://www.microsoft.com/en-us/news/press/2005/nov05/11-03dataprivacypr.aspx.

Alexander Dix, Berlin Commissioner for Data Protection and Freedom of Information, Berlin, Germany.

Gregor Thüsing, University of Bonn, Germany.

Johannes Traut, University of Bonn, Germany.

Laurits Christensen, Analysis Group, Inc., Denver, USA.

Federico Etro, Ca' Foscari University of Venice, Italy.

Susan Ariel Aaronson, George Washington University, Washington DC, USA.

Rob Maxim, George Washington University, Washington DC, USA.

extraterritorial application of European law. There are numerous examples in US law (e.g. the Sarbanes-Oxley Act) which show that there are situations where states or supra-national institutions impose legal obligations on entities such as data controllers which engage in transactions abroad or which want to do business in any given jurisdiction. Therefore, the European Union has decided that data on European citizens should be afforded an adequate level of protection should they be exported to third, non-European countries. With regard to the European Union and the United States, this adequate level of protection should have been achieved by the "Safe Harbor Agreement" of 2000. Furthermore, when exporting personal data to the United States or to other "third countries", data controllers can rely on several sets of standard contractual clauses approved by the European Commission in 2001, 2004 and 2010. Whereas the Safe Harbor Agreement rests on a scheme of self-certification by US companies supervised mainly by the Federal Trade Commission, standard contractual clauses govern the bilateral relationships between data exporter and data importer.

With Edward Snowden's revelations, the situation has changed. There had been hints in the past that US intelligence agencies were monitoring global communications to some extent, made possible by the fact that most global communications today are routed through the United States, which has thus become a kind of "global switchboard". But the information published by the *Guardian* and other newspapers shows a picture which is not only different in terms of quantity but of substance – phrases used by the intelligence community such as "Mastering the Internet" and "full take" indicate the totality of surveillance being undertaken. The information made public by Snowden has basically been confirmed by US security agencies as well as by the government (in part because it has not been refuted). One should not forget that the US government is asking for Snowden's extradition for breach of confidence, not slander.

The disproportionate monitoring of global communications (metadata as well as content) by the US NSA and the British GCHQ has resulted in a massive loss of confidence in the reliability of US companies providing cloud services. It is estimated that US companies will lose around $35 billion in the next three years due to the NSA revelations.[2] It is small comfort that some companies seem to fare better than others in the US market because they have at least tried (albeit unsuccessfully) to contest the legality of NSA actions before the Foreign Intelligence Surveillance Court. Thus, Yahoo has recently surpassed Google in terms of the number of visits to its website (though not in usage of its search engine). The fact that Yahoo went to the Foreign Intelligence Surveillance Court, while Google did not, may have contributed to this.

There can be little doubt that Europe now has the chance to take advantage of this situation. European Internet companies can benefit, as evidenced by the recent sharp rise in the number of users who have opened e-mail accounts with German providers (though one wonders what effect this will have if the GCHQ's "TEMPORA" programme continues to collect basically all data going through the UK's transatlantic submarine cables, which includes many telephone calls or mail exchanges made in continental Europe). More importantly, European legislators should now agree without delay on a framework for data protection in the private sector – the Draft General Regulation – which stresses the need for high-security IT and which would strengthen the European IT industry. It is obvious that the demand for secure communications is constantly rising in order to restore some of the confidence lost through the disclosure of the systematic monitoring of communications. This increases the possibility that products and services offering secure encryption will be more successful in sales than they have been in the past, when US products and services became bestsellers because of their convenient features.

To avoid any misunderstanding: of course there is a need to fight terrorism online as well as offline. But this should be done under effective judicial and parliamentary control. Indiscriminate and random surveillance is neither necessary nor tolerable in a democratic society. Spying on United Nations communications or European Union embassies cannot be justified as anti-terrorism measures. Although industrial espionage is part of the official remit of intelligence services in some countries, a sovereign state has the duty to protect its economy against such measures by foreign intelligence services.

In view of these developments, the European Commission has announced that it will evaluate the Safe Harbor Agreement. There are strong indications that the level of data protection in the United States is no longer adequate as required by the Directive 95/46/EC as a prerequisite for transferring the data of European citizens to the US This concept of requiring an adequate level of protection in a third country where personal data are to be exported to is not unique. The Asia-Pacific Economic Community (APEC) is working on a similar concept. In its 2000 Safe Harbor Decision, the European Commission expressly empowered the European supervisory authorities to

2 U. Clauß: Dürfen deutsche Schüler in der Datenwolke arbeiten?, in: Die Welt, 21.8.2013, http://www.welt.de/print/die_welt/politik/article119222264/Duerfen-deutsche-Schueler-in-der-Datenwolke-arbeiten.html.

suspend data flows if there was a substantial likelihood that the Safe Harbor Principles were being violated. The Principles may be limited only to the extent necessary to meet national security. The Commission made a similar decision with regard to limitations on data protection under standard contractual clauses. These limitations may not go beyond what is necessary in a democratic society. These words are taken from Article 8(2) of the European Convention on Human Rights, which describes exceptional limitations of the right to privacy.

There can be no doubt, at least from a European perspective, that the systematic collection of metadata on Internet use exceeds what is necessary in a democratic society and what is necessary for national security. Therefore, the German Data Protection Authorities have written to the German Federal Chancellor informing her that transatlantic data flows may have to be suspended and new licences to export data from Europe to the US may not be granted as long as the intelligence services are continuing to monitor the entire Internet traffic indiscriminately and to store all traffic data for a certain period of time. The German government has proposed adding a new protocol to the International Covenant on Civil and Political Rights stressing that the guarantee of private life also covers privacy in cyberspace. Whether this proposal will be supported by other governments remains to be seen. The main challenge will be to convince the US government that the National Security Agency once again needs better oversight and should refrain from certain activities altogether. President Obama has announced that more transparency will be provided for, but whether this will lead to a curtailing of US intelligence services' power despite the lingering trauma of 9/11 is an open question. A transatlantic free trade area is hardly conceivable in a climate of mistrust.

Gregor Thüsing and Johannes Traut

The Reform of European Data Protection Law: Harmonisation at Last?

One of the Commission's major selling points for the proposed data protection regulation[1] is that through it the harmonisation of data protection rules will be achieved at last.[2] The hope of a truly harmonised data protection framework has in particular led business groups, on the whole, to speak out in favour of the reform. Taking into account the considerable political influence wielded by the various lobbying groups representing business interests, the goal of harmonisation may thus be the Commission's strongest argument for the reform as a whole. This makes looking at its validity in more detail worthwhile.

The status quo

The need for more harmonisation is clear: presently 28 different national data protection laws exist, which, though quite fully harmonised as far as substantive law is concerned, differ considerably in terms of procedure and the structure of the national supervisory authorities. Furthermore, structural weaknesses of the law enforcement authorities in some member states, as well as the general lack of harmonised administrative practices,[3] contribute to the disparate application of the harmonised substantive law throughout the member states. Both the differences in procedural law as well as the differences in application have led to competitive gaps among member states.

Of course, this was not the intention of European lawmakers when they created the data protection directive in 1995. The data protection directive 95/46/EC erects a European framework for data protection, setting a European uniform standard from which member states may not derogate – neither in the direction of stricter rules nor by relaxing them.[4] Assuming proper implementation of the directive into national law, the substantial law standards are the same in all member states.

1 European Commission: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final.

2 European Commission: How will the EU data protection reform strengthen the internal market, available at http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/4_en.pdf; European Commission: Why do we need an EU data protection reform?, available at http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf.

3 See European Commission: The Proposed General Data Protection Regulation: The Consistency Mechanism Explained, available at http://ec.europa.eu/justice/newsroom/data-protection/news/130206_en.htm, in which the Commission rightly points to the Google Street View case, which was handled very differently in various member states.

4 ECJ Case No. C-101/01 – European Court Reports 2003, I-12971, paragraph 96 (Lindqvist).

But even though the standard of substantive law might be the same, the administrative practices of the national supervisory authorities responsible for its application have so far not been effectively harmonised. This is a serious flaw, as their administrative practices significantly determine the practical application of the substantive data protection rules, since the field data protection is particularly dependent upon efficient enforcement by state agencies.[5] The existence of independent supervisory authorities is an essential component of the protection of individuals with regard to the processing of personal data.[6] The current consultation process within the framework of the Art. 29 Working Party (WP) – while helpful in producing input and guidelines – cannot set mandatory standards and enforce them. It is even less capable of overruling individual decisions by national supervisory authorities. The general lack of cohesion is aggravated by the structural weaknesses of some supervisory authorities who lack the financial and personnel resources to properly discharge their mission.

Therefore the true challenge of harmonisation lies in the field of application. Ensuring the uniform application of the harmonised rules through harmonised administrative practice is far more difficult than harmonising the substantive law. This is where the current framework is insufficient. Most likely, the proposed regulation will improve the situation.

At least the Commission has recognised that harmonising the work of the national supervisory authorities is the key to practical harmonisation of the law. The increased emphasis of the proposed regulation on practical implementation and enforcement is apparent on many levels, for instance in the space devoted to the enforcement authorities. Whereas today these are regulated in a scant article of the current data protection directive, the proposed regulation contains an entire chapter (Chapter VI) dealing with the enforcement authorities. Moreover, it devotes another chapter (Chapter VII) to their cooperation (Section 1) and the consistency mechanism (Section 2).

The consistency mechanism

The latter is certainly one of the most noteworthy novelties in the reform package. The consistency mechanism aims at effectively harmonising the administrative practices of the national supervisory authorities, at least as far as data subjects in several member states are concerned (Art. 57).[7] The Commission's approach for reaching consistency can be characterised as carrot and stick. On the one hand, the Art. 29 WP is transformed into the European Data Protection Board (EDPB). The Board is composed of the head of each national supervisory authority and the European Data Protection Supervisor (Art. 64 (2)). The national supervisory authorities can democratically vote on and adopt with majority (Art. 68 (1)) resolutions. These can be non-binding resolutions containing mere guidelines, along the same lines as the decisions of the Art. 29 WP.

In regard to the consistency mechanism, however, its powers are somewhat broader. Within this framework, the EDPB is endowed with the power to adopt an opinion on concrete draft measures produced by national supervisory authorities (Art. 58 (7)). The consistency mechanism covers, broadly speaking, all cases which concern more than one member state (Art. 58 (2)(a)) and all those which may substantially affect the freedom of movement of personal data in the union (Art. 58 (2)(b)).[8] The supervisory authorities to whom the opinion is addressed have to take the EDPB's opinion "into account" and inform the EDPB and the Commission whether it maintained its draft measure or amended it according to the EDPB's opinion.

This contrasts sharply to the impact of an opinion adopted by the Commission. Art. 59 (1) enables the Commission, within ten weeks after a matter has been raised under Art. 58, to adopt an opinion in relation to the matter raised, in order to ensure correct and consistent application of this regulation. This opinion by the Commission is not per se binding; however, the supervisory authority has to take "utmost" account of the Commission's opinion (Art. 59 (2)), which will in practice mean that the authority usually will have to follow the Commission's opinion. In case it should not, however, the Commission can still ensure that its position prevails. Where the supervisory authority concerned intends not to follow the opinion of the Commission, Art. 59 (4) provides that it shall inform the Commission and the EDPB thereof within the period referred to in paragraph 1 and provide a justification. In this case, the draft measure shall not be adopted for one further month.

Why, however, delay another month? This gives the Commission time to suspend the proposed measure for up to 12 months, in accordance with Art. 60. Within that timeframe, the Commission can then adopt an implementing act determining the correct implementation of the regula-

5 See German Federal Supreme Court, Reports of the Federals Supreme Court (BVerfGE), Vol. 65, p. 1, 46.
6 ECJ Case No. C-614/10 (Commission v Austria), not yet published in the Court Reports, paragraph 37.
7 European Commission: Proposal for a Regulation …, op. cit, p. 13.
8 Ibid.

tion in the case referred to the consistency mechanism (Art. 62 (1)(a)). In the end, therefore, the Commission can push through its opinion on an individual case. This is the stick aspect of the consistency mechanism.

Furthermore, this power is not limited to those cases referred to the consistency mechanism by national supervisory authorities. The Commission will be able to involve itself into practically any important decision, since Art. 58 (4) provides that the Commission may, in order to ensure correct and consistent application of this regulation, request that any matter be dealt with in the consistency mechanism. Consequently, it may involve itself in any matter of the implementation it pleases, even purely national cases.

The total picture, though pieced together from various provisions, is a clear one: in contrast to the EDPB, the Commission will be able to enforce its position, even though the Commission is not per se responsible for implementing and enforcing the regulation. However, it is given a decisive role in the consistency mechanism, which aims at harmonising the application of the regulation throughout Europe. This is a novel approach, as thus far in the context of European law, either the Commission or national authorities have been responsible for the application and enforcement of the law, but not both. Certainly the Commission's power within the consistency mechanism – if the regulation becomes law as proposed – will play a great role in practice, even though this is downplayed by the Commission in the current debate.[9]

The Commission has good reason to do so, as its role in the proposed consistency mechanism is one of the most sensitive areas of the reform. Here the Commission even faces opposition from the data protection supervisory authorities, which on the whole are quite supportive of the reform.[10] It likewise is heavily criticised by member states,[11] and the Rapporteur in the European Parliament, Jan Albrecht, has proposed significant changes to the consistency mechanism.[12] His model gives the EDPB the power to adopt a binding opinion with a two-thirds majority. The Commission would be relegated to challenging the opinion before the European courts.[13] Its role, therefore, would be reduced from determining the appropriateness of the application of the regulation to simply ensuring the legality of the supervisory practice. This, of course, leaves a wide and non-harmonised margin of discretion for the national supervisory authorities.

The main reason for the critical attitude towards the Commission's role is the perceived threat to the independence of the national supervisory authorities.[14] Closer inspection of this argument, however, shows that the independence of national supervisory authorities is not legally necessary at all. The existence of independent supervisory authorities is mandated by Art. 8 (3) of the Charter of Fundamental Rights of the EU. It is nevertheless a misconception that these have to be national supervisory authorities. The current structure of supervisory authorities is the result of the current data protection framework, which is based on a directive and thus implemented by the individual member states. The change to a regulation could just as well be accompanied by the creation of one supervisory authority at the European level. Thus, national supervisory authorities have no legally protected status as such.

Moreover, it is obvious that the goal of harmonising the application of data protection rules throughout the internal market cannot be reached while retaining the absolute independence of national supervisory authorities. Even under a uniform legal regime, the application of the provision may differ significantly in practice, as law grants the supervisory authorities some discretion in the application of the law which is not scrutinised by the court. This might include, for instance, how the supervisory authority discharges its duty to monitor and ensure the application of the regulation (Art. 52 (1)(a)) or where it issues an authorisation according to Art. 34.

The EDPB is likewise ill-suited to achieve complete harmonisation in the application of the regulation. This has already been demonstrated for the Art. 29 WP in the past,

9 European Commission: The Proposed General Data … , op. cit.

10 Article 29 Data Protection Working Party: Opinion 01/2012 on the data protection reform proposals (WP 191), p. 20, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf; European Data Protection Supervisor: Opinion of the European Data Protection Supervisor paragraph 268, available at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf.

11 Limiting the role of the Commission in the consistency mechanism and preserving the "independence" of supervisory authorities is for instance included in the mandate for negotiations given by the German Bundestag to the Federal Government; see Deutscher Bundestag, Drucksache 17/11325, No. 14.

12 See Committee on Civil Liberties, Justice and Home Affairs, Rapporteur Albrecht: Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.

13 See Committee on Civil Liberties, Justice and Home Affairs, Rapporteur Albrecht, op. cit., Amendment 280 ff., pp. 169 ff.

14 See Deutscher Bundestag, op. cit.; Article 29 Data Protection Working Party, op. cit.; European Data Protection Supervisor, op. cit.

and the same will apply to the EDPB. Both are democratically organised bodies that decide by majority. Where no majority can be achieved, they are paralysed into inaction, and the referring supervisory authority is free to do as it pleases. Particularly in the case of difficult questions, this leaves plenty of room for indecision, which gives supervisory authorities a license to act as they please. The Rapporteur's proposal to allow the EDPB to adopt binding opinions, but only with a two-thirds majority, will be plagued even more so by indecisiveness.

Hence, a strong supervisory authority at the European level is indeed necessary if the central goal of the reform – the harmonisation not only of data protection rules but also their application across Europe – is to work in practice. That supervisory authority must be able to ensure not only the legality but also the appropriateness of national supervisory authorities' actions. Such a supervisory authority could be set up at the European level and operate as an independent authority pursuant to Art. 8 (3) of the Charter and Art. 16 (2) TFEU.

However, it is less clear whether the Commission should assume that role, as is proposed in the current regulation. Whereas the Commission, as guardian of the treaties (Art. 17 (1) TEU), is in principle an independent organisation (Art. 17 (3) TEU and Art. 245 TFEU), its mission is very broad and it is subject to political influence. The Commission is committed to advancing and protecting many other interests, some of them contrary to the protection of privacy and the protection of personal data. Therefore, the Commission cannot concentrate on solely promoting the protection of personal data and might even be forced to compromise data protection for the benefit of other interests covered by its mission. In this regard, the Commission is quite comparable to the national executive branch, which was deemed to be insufficiently independent to act as a supervisory authority according to Art. 8 (3) of the Charter and Art. 16 (2) TFEU.

The Commission's current role within the proposed regulation could thus be seen as violating Art. 8 (3) of the Charter and Art. 16 (2) TFEU, which mandate the establishment of independent supervisory authorities. If the legal provisions are interpreted to require single-minded authorities focused solely on data protection, the European Commission certainly does not qualify. That would of course be a very narrow interpretation of the relevant provisions, arguably one that is too narrow. A distinction should be made between the quasi-legislative functions of the Commission when exercising the power to adopt delegated acts and the supervision of the application of the provision as such. The quasi-legislative functions certainly cannot – for reasons of democratic legitimacy alone – be exercised in full independence. As far as the supervision as such is concerned, the work of the Commission within the Framework itself is scrutinised by the European Data Protection Supervisor (EDPS), who is an independent supervisory authority. This should be sufficient to meet the requirements of Art. 8 (3) of the Charter and Art. 16 (2) TFEU.

In any case, simply maintaining the status quo or assigning all responsibility to the EDPB is no serious alternative. One sensible option could be, as mentioned above, setting up a supervisory authority at the European level with a comprehensive right of direction vis-à-vis national supervisory authorities. In the course of the drafting process, this option was considered but rejected because of the expected cost. The recently established European Union Agency for Fundamental Rights would appear to be a reasonable alternative at first glance, as its mission is solely focused on the protection of fundamental rights, but it is not authorised to hear individual complaints or exercise regulatory power and thus would be of little value.

Regulating the status of the supervisory authorities

The second reason for the unequal enforcement of the current law is the strained state of some supervisory authorities who are currently not fully able to fulfil their mission. This of course does not apply to large and powerful institutions like the French CNIL or the German *Bundesdatenschutzbeauftragter*. However, it has thus far proved difficult in some countries, particularly some of the smaller ones which have more recently joined the EU,[15] to establish effective supervisory authorities and especially to provide them with sufficient resources and financial independence.[16] The proposed regulation explicitly addresses this problem; its detailed rules on the supervisory authority will provide them with far greater clout to demand adequate resources in national budgetary discussions, particularly since these provisions are directly applicable in every member state:

Each member state shall ensure that its supervisory authority is provided with the adequate human, technical and financial resources; premises; and infrastructure

15 See the evidence given by the Commission in a hearing by the British House of Commons Justice Committee: The Committee's opinion on the European Union Data Protection framework proposals, paragraph 39, available at http://www.publications.parliament.uk/pa/cm201213/cmselect/cmjust/572/572.pdf.

16 The Art. 29 WP therefore endorses this particular aspect of the reform quite strongly; see Article 29 Working Party, op. cit, p. 17; similarly, European Data Protection Supervisor, op. cit., paragraph 235.

necessary for the effective performance of its duties and powers (Art. 47 (5));

Art. 47 (6) further clarifies that every supervisory authority shall have its own staff, which shall be subject (only) to the direction of the head of the supervisory authority;

Art. 47 (7) aims at ensuring their financial independence by stipulating that each supervisory authority shall have its own budget.

The importance of these provisions is highlighted by the fact that the Art. 29 WP advocates even more detailed regulations, going so far as to stipulate a formula by which the actual budget can be calculated according to the respective member states' populations.[17] This clearly goes too far, as the national parliaments' budgetary powers would be undermined. Nevertheless, the very request shows the great importance an adequate provision of resources has for the effective functioning of supervisory authorities. In this respect, the proposed regulation will greatly improve the practical application of data protection law.

Administrative sanctions: over the top?

An increase in the formal powers of the supervisory authority complements these improvements in legal status. Foremost in the political discussion is the question of the newly introduced power to impose administrative sanctions. However, that the proposed regulation provides for administrative sanctions as such is only questioned by the most ardent lobbyists. The power to impose fines has commonly been part of the implementation of the directive so far and is nothing new.[18]

Nevertheless, the potentially enormous scale of the fines is very controversial,[19] as they can reach as high as two per cent of an enterprise's annual turnover (Art. 79 (6)). This goes far beyond the current framework, which only requires member states to provide supervisory authorities with "effective powers of intervention" (Art. 20 (3) of Directive 95/46/EG), and also beyond the scale of fines currently possible under national law.[20] However, the currently proposed scale of the sanctions is no cause for alarm but rather the right approach.

These sanctions and their potentially large scale mark the extreme boundaries of what is possible. They will not be applied on a regular basis, if at all. Fears that they will be are mainly voiced by lobbyists, for obvious reasons. Their alarmism at times loses all proportion. For instance, stating that the provisions "appear to be very prescriptive, leaving little flexibility for supervisory authority"[21] simply ignores the actual wording of the draft. A closer look at the actual provisions shows that exactly the opposite is the case. Art. 79 (2) mandates that the administrative sanction shall be effective, proportionate and dissuasive in each individual case. This establishes the important principle of proportionality. The sanction has to be determined for every individual case and in regard to that case. This not only gives the supervisory authority ample leeway to tailor the fines to the individual case but actually requires them to do just that.[22] Art. 79 (2) goes on to further specify this principle of proportionality:

> The amount of the administrative fine shall be fixed with due regard to the nature, gravity and duration of the breach, the intentional or negligent character of the infringement, the degree of responsibility of the natural or legal person and of previous breaches by this person, the technical and organisational measures and procedures implemented pursuant to Article 23 and the degree of co-operation with the supervisory authority in order to remedy the breach.[23]

These determining factors were obviously chosen with great care. They are inspired by the Commission's practice in competition law.[24] Their purpose is, therefore, not only to punish infringements but to punish them in such a way as to act as effective market regulation. They are designed to give an economic incentive to follow the rules of the proposed regulation. Because of its competition regulating function, there can be no alternative to a flexible threshold that is based on an enterprise's turnover. The principle of proportionality not only limits the amount of a fine vertically, it also requires that fines are fair horizontally in regard to the perpetrator's competitors who committed comparable violations. It must grant authorities the power to hit one competitor as hard as the other, regardless of the size of their respective enterprises.

17 See Article 29 Working Party, op. cit., p. 17.
18 See inter alia § 43 of the German BDSG and Art. 55a of the British Data Protection Act (1998).
19 A matter of concern especially in the United Kingdom; see British House of Commons Justice Committee, op. cit., paragraph 84 ff.
20 § 43 of the German BDSG; Art. 55a of the British Data Protection Act (1998).
21 This opinion was voiced by the British Ministry of Justice in an Explanatory Memorandum to the House of Commons Justice Committee; see British House of Commons Justice Committee, op. cit., paragraph 84.
22 See European Commission: Proposal for a Regulation …, op. cit, p. 92 for the official explanation of the provision.
23 Ibid.
24 See Guidelines on the method of setting fines imposed pursuant to Article 23(2)(a) of Regulation No. 1/2003, in: Official Journal of the European Union 2006/C 210/02, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2006:210:0002:0005:en:PDF.

Since it served as the model for the provision, the Commission's practice in competition law can provide some idea of the extent to which the Commission will exploit the limits for fines given by the regulation. Council Regulation 1/2003 provides for even heavier fines – up to ten per cent of an enterprise's turnover (Art. 23 (2)) – for infringements of EU competition law. So far, however, the fines have not been even close to that threshold. Of the ten highest fines ever imposed, the highest (Pilkington) reached about 6.5 per cent of the enterprise's annual turnover, or 65 per cent of the maximum fine possible, and this was only after an earlier order to dissolve the same cartel was not followed. By contrast, six of the fines were less than three per cent of annual turnover.[25]

Summary

Achieving harmonisation is perhaps the central goal of the ongoing reform of the European Data Protection Framework. Harmonisation requires not only the harmonisation of substantial law but also of administrative practices. This has been recognised by the Commission, which accordingly provided for a consistency mechanism in its proposed regulation. The consistency mechanism, in its current form, follows a carrot and stick approach. The EDPB gives national supervisory authorities a platform for voluntary cooperation. This is, however, backed by powers of the Commission which allow it to effectively intervene even in individual cases and not only to ensure the legality of national supervisory authorities' decisions, but also to determine what measures might be appropriate in an individual case. Though much criticised, such powers are necessary to achieve harmonisation, which must include the harmonisation of administrative practices. These powers can arguably be exercised by the Commission itself without compromising the existence of an independent supervisory authority at the European level, as the Commission is also subject to the scrutiny of the EDPS. Alternatively, the supervisory powers could be vested in the European Data Protection Supervisor or a new independent agency at the European level. The consistency mechanism is rightly flanked by measures to ensure that supervisory authorities have the necessary resources to discharge their duties.

Administrative sanctions are also needed. The scale of the sanctions proposed by the Commission is far less intimidating than many critics wish to portray. The sanctions are governed by the principle of proportionality and are modelled on the fines developed in competition law. Experience there shows that the maximum fine will be rarely, if ever, imposed. Overall, it is likely that the reform will be a big step towards harmonising data protection within the internal market.

25 See the statistics available at http://ec.europa.eu/competition/cartels/statistics/statistics.pdf, section 1.6.

Laurits Christensen and Federico Etro

Big Data, the Cloud and the EU Regulation on Data Protection

The recent increase in the creation and storage of ever larger quantities of data, referred to as "big data", is expected to enhance the productivity of the global economy. Indeed, it is as if a new factor of production had been constructed. Moreover, the use of big data is going to affect the way firms, academic institutions and consumers do business, make discoveries and interact with each other. It is estimated that people around the world generate more than 2 exabytes (i.e. quintillion bytes) of unstructured data (that is, data that lack a predefined model, such as search engine queries, posts on Twitter, "likes" on Facebook and so on) every day, and organisations generate and store even more exabytes of structured data every year. In most cases, people and organisations do not know what to do with all these data; consumers do not know how their own data are processed and protected; organisations need to develop tools to process, store and transmit these data; and institutions must regulate data protection. All of this creates a set of interesting issues: what is the economic importance of big data? What is the appropriate role for cloud computing? What is the proper way to protect data?

From an economic perspective, it is important to understand how the accumulation of data, which represent a sort of new factor of production, can affect growth and generate added value across society. A typical example of the importance of big data is related to consumer behaviour online, whose importance has been rapidly increasing over time and is, in turn, a source of new business and trade online. This and other new possibilities are enhanced by the rapidly declining costs of storing data. Cloud computing has contributed more than any other technology to the diffusion

and use of large-scale datasets and to the spread of the benefits of the newly gained efficiencies across companies and to consumers relying on cloud computing solutions.

The use of cloud services to accumulate data implies that the volume of new data will increase exponentially in the years to come. Cisco forecasts that the annual volume of global IP traffic will exceed a zettabyte (a thousand exabytes) in 2015. The velocity of data collection is similarly increasing. Remarkably, 90 per cent of the volume of global data was generated in the last couple of years, and data creation is expected to be 44 times larger in 2020 relative to ten years earlier. This growth derives from a variety of unstructured data that are being accumulated today. The economy is going to benefit from this, with new businesses to be created based on big data and cloud computing. This is possible thanks to two main factors. The first is technological: novel computing methodologies help firms to understand and use data by means of machine learning and analytical tools. The second is economic: the hardware needed to store and process data has become incredibly inexpensive.

As a general matter, big data is expected to benefit the economy directly through more efficient marketing, more efficient pricing, more targeted product development and the development of new businesses (which is always a source of more competition and efficiency). There has been significant discussion of how big data will allow companies to become more efficient in their marketing efforts.[1] The ever increasing quantities of data are allowing firms to better understand what economists call "customer heterogeneity" (put simply, the fact that customers are not all alike and can differ in ways that are important to companies). The power of big data is increasingly allowing companies to deploy their marketing dollars in ways that increase the return on their advertising investment.

Big data is also allowing companies to price their products in ways that recognise customer heterogeneity. For example, there has been an increasing level of experimentation by companies in varying prices based on the outlet through which the product is sold (think Priceline vs. Expedia), the day of the week, or even the hour of the day. This variation in pricing allows companies and consumers to sort themselves according to their specific preferences. Those who are willing to invest time in searching for the lowest prices will be rewarded for their efforts.

Finally, big data holds the promise of improving product development by allowing companies to know more about consumer preferences without having to undertake survey research. The explosion of data allows them to gain this knowledge through careful analysis of consumer choices around real products and pricing. As firms learn more about consumer preferences within existing product lines, they can better target their future offerings in ways that cater to consumers' revealed preferences. This is likely to be particularly true in the service sector where new product development time can be considerably shorter than in other sectors (e.g. automobiles).

These factors are likely to contribute to increased measures of productivity in traditional economic assessments. However, the full economic value of big data is hard to measure because it creates indirect benefits. The point can be explained with an example. The use of personal data for diagnostic purposes and to avoid duplicative testing in the healthcare sector clearly produces a real economic benefit. But because the value created does not involve explicit market transactions, attributing this benefit directly to data involves some inspired approximation. More than just a hypothetical, recent research from Microsoft Research Labs and Stanford and Columbia Universities has found that by analysing large volumes of data, they could identify previously unknown adverse pharmaceutical drug interactions. This research may be just the tip of the iceberg for improvements in health treatments. As the amount of data available to analyse health outcomes increases (either formally through drug studies or informally through big data), it will be possible to improve treatment regimens and make the healthcare sector more efficient, benefitting individuals and society more broadly. Of course, this example also points to complex issues concerning data privacy and data protection, which present new problems for regulation.

While the economic benefits from big data and cloud technologies are potentially large, privacy groups and consumer advocates have raised alarms over how personal data are collected and processed. They worry as well about the potential to learn details about people that they may wish to keep private. A recent analysis of Facebook data by a research team in Cambridge revealed that researchers could predict sexual orientation with a high degree of accuracy based on seemingly generic information revealed through Facebook pages. Bio-ethicists similarly worry that it will become possible to learn about individuals' current (and probable future) health status by virtue of information revealed through the myriad interactions that create big data.

In response to these and other similar concerns about data privacy and protection, the EU has proposed a new Data Protection Regulation, with the aim of protecting individuals with regard to the processing of personal data. The new regulation seeks to create a single set of rules across the EU and introduces a number of new requirements for busi-

1 See e.g. A. Ignatius (ed.): Spotlight on the Future of Advertising, in: Harvard Business Review, Vol. 91, No. 3, 2013, pp. 59-89.

nesses. As the privacy debate continues, an important distinction will arise as to whether one should prevent the collection and analysis of data (the current approach favoured by the EU) or allow it and instead focus regulation on ensuring that the results are not used in an illegal or unethical manner. For example, should there be a prohibition on the collection of data that could, if analysed in particular ways, allow one to predict with reasonable accuracy which people are likely to develop cancer? Such a prohibition would preserve the privacy of the individuals and ensure that companies could not use that information inappropriately, but it would also prevent these individuals from knowing that they were at risk, which would allow them to take appropriate health precautions.

In the face of this debate regarding how to strike an appropriate balance between maintaining privacy and realising the economic benefits from these new areas of research, economic quantification of the potential benefits and costs can help inform the discussion. Recent research on the benefits from cloud computing and the costs of complying with the proposed regulations offers insights into how the benefits of new technology can be curtailed or eliminated through regulation. In prior research on the benefits of cloud computing, it has been shown that this new technology could generate benefits in terms of increased employment and economic growth.[2] This research showed the clear promise of the decreasing costs of computing and storage. But it is also in response to the growth of cloud computing and big data that the EU has proposed new data privacy regulations.

In related research with Greg Rafert and Andrea Colciago, we have shown that the cost of complying with the new data privacy requirements in the proposed data protection regulation is expected to have adverse effects on growth and employment, in particular among small and medium-sized enterprises (SMEs).[3] This research analyses the compliance costs associated with the direct application of the new regulation as well as the indirect effects on job growth and business creation. Compliance with the proposed regulation poses a number of challenges for firms. The first challenge concerns the design of systems and procedures for data protection. In particular, under the proposed regulation, firms must develop data management systems that allow for greater flexibility, such as the right to data portability (i.e. the right to transfer data from one electronic processing system to another) as well as the right of data subjects (identified natural persons) to obtain their personal data in a structured, commonly used electronic format. Additionally, data protection impact assessments must be incorporated into IT project management so that firms can identify and mitigate specific risks associated with the processing of personal data.

Another major challenge is the designation of a data protection officer (DPO). This obligation will apply to all public sector bodies and enterprises with 250 or more employees, as well as to firms whose core activity involves the monitoring of data subjects. The controller (the entity that determines the purposes, conditions and means of the processing of personal data) and the processor (the entity that actually processes personal data on behalf of the controller) will be subject to different obligations and possibly also to different supervisory authorities (which could create useless duplication costs).[4] The controller and the processor will also have to ensure that the DPO is involved in all issues that relate to the protection of personal data and maintain detailed documentation on all processing operations. The compulsory notification of any data breach to the supervisory authority within 24 hours and to the data subjects without undue delay – which is extremely demanding, especially for non-serious data breaches – will lead to substantial compliance costs for firms. Several additional articles in the regulation will also result in additional costs, depending on the type and amount of information processed.

However, it should be noted that some of the proposed articles within the legislation will reduce costs for firms. For example, the "one-stop-shop" principle reduces some compliance costs by ensuring that data controllers and data processors that operate across countries are typically regulated by a single supervisory authority, though this is not the case for companies that happen to be both data controllers and data processors in different countries (for instance, cloud computing providers). Moreover, binding corporate rules will potentially reduce legal ambiguity surrounding data transfers, and joint operations on the part of supervisory authorities will reduce bureaucratic burdens. The ongoing effort to promote secure data transfers is important, as this is crucial for the development and the diffusion of cloud computing; however, more needs to be done, such as supporting and standardising the stronger and more transparent protection of data that are transferred outside the EU for cloud computing services. Both the costs and the benefits

2 F. Etro: The Economic Impact of Cloud Computing on Business Creation, Employment and Output in the E.U., in: Review of Business and Economics, Vol. 54, No. 2, 2009, pp. 179-208.

3 For technical details, see L. Christensen, A. Colciago, F. Etro, G. Rafert: The Impact of the Data Protection Regulation in the E.U., Intertic Policy Paper, 2013.

4 Problems of duplication are reduced in many cases with this new regulation, but not for entities that happen to be both controllers and processors. A clearer distinction between the status of controller and the status of processor would be useful to identify which supervisory authority has jurisdiction. The controller should be the entity that determines the reason why data are processed and the processor the entity that determines how the data are actually processed.

Table 1
Summary of expected fixed and variable costs from the data protection regulation by article

	Fixed annual cost (euros)				Variable annual cost (euros)			
Article	Wholesale and retail trade	Hotels and restaurants	Transport, storage and communication	Real estate, renting and business activities	Wholesale and retail trade	Hotels and restaurants	Transport, storage and communication	Real estate, renting and business activities
23, 33					1,462	688	1,056	2,236
28, 35, 36, 37	0	0	539	2,763	0	0	56	254
31, 32	100	100	100	100	1,005	446	442	1,094
12, 17, 18	97	46	41	105	185	52	103	207
7	418	627	173	212				
11	219	103	92	237				
5, 19, 20					1,366	2,049	565	694
43					-1,128	-531	-471	-1,218
8	124	0	43	30				
22	0	0	0	0	0	0	0	0
24, 25	151	71	63	164				
34					156	73	65	168
55, 56, 57, 58, 76					-100	-47	-42	-108
77					303	143	127	327
79	0	0	0	0	0	0	0	0
Total	1,109	947	1,051	3,611	3,249	2,873	1,901	3,654
% of IT budget	6	5	6	20	18	16	11	20

Note: No firms related to manufacturing are thought to be impacted and all costs for this sector will be zero.

Source: Authors' elaboration.

of the proposed regulation have been taken into consideration in our analysis. Finally, it is important to note that we did not take into consideration the expected costs associated with the administrative sanctions, whose homogenous application to all companies (without distinction between intentional and unintentional harm) may create an unfair and disproportionate burden on SMEs that fail to comply with the regulation for reasons other than repeated negligence.

We have simulated the impact of the new regulation on the process of business and job creation, estimating first the likely costs and benefits created by the proposed regulation and then using a dynamic stochastic general equilibrium model. Our estimates of the average expected costs and benefits of compliance for SMEs are summarised in Table 1 (divided by macrosectors and expressed in terms of average net cost per firm). Our results suggest that the net costs are large – indeed, larger than what could be expected, for instance, from the evaluation of the Impact Assessment prepared by the European Commission. The percentage of firms impacted as well as the average expected costs and benefits were estimated for each of the 15 article groups deemed important in the EU Data Protection Regulation. We calculated an average annual IT budget of €18,000 and then used this value to calculate total costs as a per cent of IT budget; these estimates are also provided in Table 1.

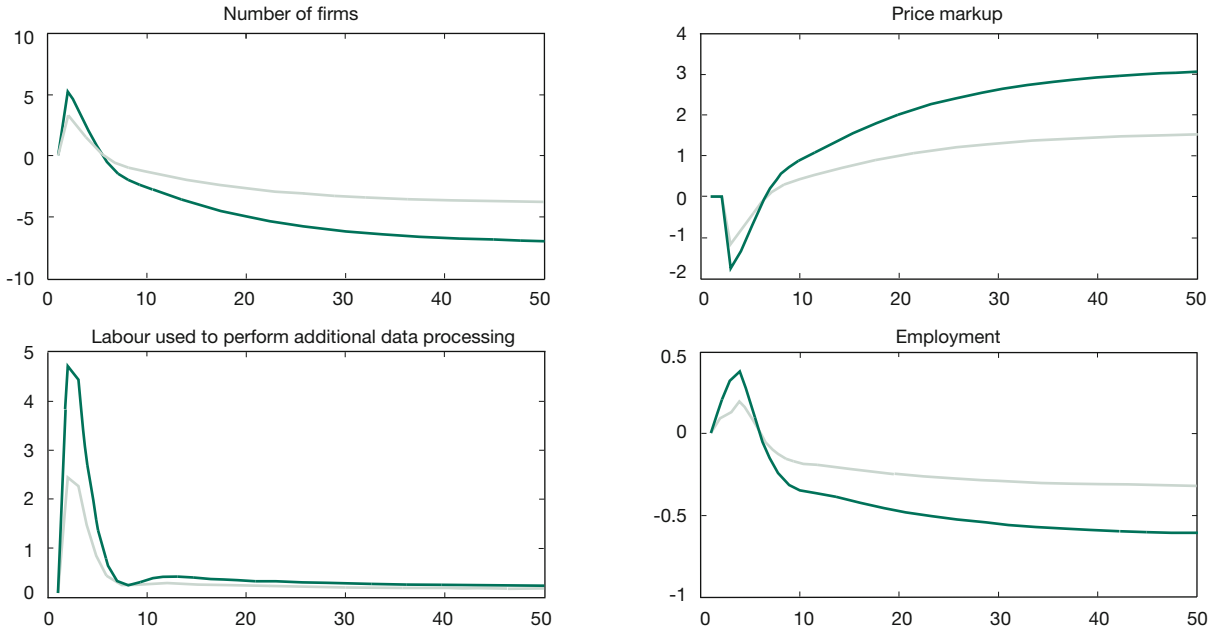
On the basis of the above estimates, we then simulated the impact in a macroeconomic model whose production structure is based on Etro and Colciago,[5] augmented with a description of the labour market with search frictions and endogenous unemployment. The economy features four types of firms: the producers of intermediate goods, the final good producer, the producers of IT material and the providers of data management services. The intermediate goods industry features many sectors where the dynamics of the number of market competitors is endogenous. In this industry, firms face a sunk cost of entry into the market, which they decide to incur if sufficiently compensated by the expectation of future profits. Goods are produced using labour and IT, which can be interpreted as hardware but also as the stock of data stored at each firm. The industry

5 F. Etro, A. Colciago: Endogenous Market Structure and the Business Cycle, in: The Economic Journal, Vol. 120, No. 549, 2010, pp. 1201-33.

Figure 1

Simulated impact of the legislation on data protection in the EU 27: real estate, renting and business activities sector

Percentage deviation



Note: dark green line: baseline impact; light green line: low impact scenario.

Source: L. Christensen, A. Colciago, F. Etro, G. Rafert: The Impact of the Data Protection Regulation in the E.U., Intertic Policy Paper, 2013.

producing IT adopts physical capital as the only input, while in the industry providing data management services, the input is labour. The labour market is characterised by the frictions related to job search and matching. In the intermediate goods industry, both new firms and incumbent firms need to hire workers from the pool of unemployed agents who are looking for a job. They also need to set up a stock of IT before starting production. Similarly, the industry providing data management services faces labour market frictions.

The model counterpart of the introduction of the EU Data Protection Regulation can be illustrated as follows. In order to mimic the need to install a DPO, we have assumed that the intermediate goods producers will incur a period fixed cost. The designation of a DPO can be regarded as a fixed cost, since it does not scale with the size of the firm nor with the number of data records. On the other hand, the development of a data management system is a variable cost for the firm which depends on the amount of data processed or more generally on the number of projects currently being developed at a firm. For this reason, the model counterpart of this requirement is an increase in the units of data management services necessary to deal with each unit of information involved in the production process. Since the introduction of the EU Data Protection Regulation represents a permanent shock to the cost function of firms, we computed a transition from the pre-reform steady state to the post-reform steady state of the economy we have just described.

The simulation under two scenarios shows a substantial negative impact of the introduction of the EU Data Protection Regulation on business creation and employment under both scenarios. Among the industrial macrosectors that we considered, the one most severely affected by the regulation is the real estate, renting and business activities sector (see Figure 1), which displays a long-run reduction in employment ranging from 0.2 to 0.6 per cent, together with a reduction in the number of market competitors ranging from three to five per cent. The reduction in employment and the number of operating firms is particularly severe in those sectors where compliance with the EU Data Protection Regulation will imply higher fixed operating costs for firms. For example, the effect is stronger in sectors in which a large fraction of firms will be required to designate a DPO.

These results suggest that much or all of the potential benefit from big data and cloud computing could be undone via regulation. If countries wish to benefit from the big data and cloud computing revolution, finding ways to balance privacy concerns against the expected economic benefits from both will be paramount.

Susan Ariel Aaronson and Rob Maxim*

Data Protection and Digital Trade in the Wake of the NSA Revelations

In July 2013, American computer whiz Edward Snowden leaked details regarding various National Security Agency programs. Snowden did not aim to undermine U.S.-EU free trade talks; he wanted to engage the public in a debate about NSA spying. However, Snowden's revelations that America was monitoring phone calls and Internet communications of foreign citizens, as well as using the Internet to spy on allied governments, drove a wedge between the two trade giants. Within days, German Chancellor Angela Merkel expressed her support for tougher privacy rules.[1] President Hendryk Ilves of Estonia argued that the EU should create a secure "European cloud" with high data protection standards.[2] The European Parliament called on the European Commission to determine whether data passed on to the NSA by private U.S. companies was in violation of EU data protection regulations.[3] Privacy and the EU's attempts to modernize EU-wide data protection rules became one of many issues bedeviling negotiations for a U.S.-EU free trade agreement, the Transatlantic Trade and Investment Partnership (TTIP).[4]

Concerns about U.S. failure to protect privacy in the cloud are not new. Under Mutual Legal Assistance Treaties, law enforcement agencies in one nation can review private data of citizens in the cloud if investigative authorities believe such information may be relevant to national security.[5] U.S. legislators expanded these powers in the Patriot Act (2001) and the Foreign Surveillance Intelligence Act (2008).[6] Consequently, if they fall under U.S. jurisdiction, cloud servers anywhere in the world have to comply with data requests from U.S. authorities. Overseas critics of these policies note that U.S. citizens can challenge violations of their privacy, but non-citizens have no such rights.[7]

Global concerns about NSA spying reached a fever pitch in September 2013. The New York Times reported that the NSA had circumvented or cracked much of the encryption that guards global commerce and banking systems, protects sensitive data like trade secrets and medical records, and secures online communications. Moreover, the NSA deliberately weakened a 2006 standard adopted by the National Institute of Standards and Technology (NIST), which was later adopted by the 163 states belonging to the International Organization for Standardization.[8] Some security experts said that these strategies "undermine the fabric of the Internet," because they made encryption, the main tool to protect privacy online, useless.[9] To put it differently, U.S. strategies to maintain Internet security had undermined the trust necessary for the free flow of information.

In this article, we examine the trade and national security spillovers of U.S. and EU approaches to data protection. Both governments want to protect the privacy of citizens moving information through the cloud, ensure that information flows smoothly across the Atlantic and enable government officials to protect their citizens from harm by monitoring such information flows when necessary. We argue that neither the EU nor the U.S. has developed a consistent stance. The U.S. wants to ensure that trade rules include language facilitating the free flow of information as a default position and wants to maintain aspirational and voluntary language on privacy.[10] But the NSA revelations have threatened U.S. leadership of the Internet, as well as American market share; hence, the U.S. must take steps to protect privacy and build

* The MacArthur and Ford Foundations provided funds for this research.

1 I. Traynor: NSA spying row: bugging friends is unacceptable, warn Germans, in: The Guardian, 1 July 2013, http://www.theguardian.com/world/2013/jul/01/nsa-spying-allegations-germany-us-france; and A. Travis: European commission backs Merkel's call for tougher data protection laws, in: The Guardian, 15 July 2013, http://www.theguardian.com/world/2013/jul/15/european-commission-angela-merkel-data-protection.

2 Reaching for the Clouds, in: The Economist, 20 July 2013; and M. Ermert: Nations Begin to Take Action Against United States for NSA Spying, Intellectual Property Watch, 12 July 2013.

3 European Parliament Calls For 'Full Review' Of Data Transfer Agreement, Inside U.S. Trade, 11 July 2013, insidetrade.com/Inside-US-Trade/Inside-U.S.-Trade-07/12/2013/european-parliament-calls-for-full-review-of-data-transfer-agreement/menu-id-172.html.

4 M. Price: Turn back the limousines: EU-U.S. trade pact faces rocky road, BBC News, 1 July 2013, http://www.bbc.co.uk/news/world-europe-23126238.

5 W. Maxwell, C. Wolf: A Global Reality: Governmental Access to Data in the Cloud, Hogan Lovells White Paper, 23 May 2012, p. 2.

6 Ibid, p. 4.

7 Z. Whittaker: Patriot Act can 'obtain' data in Europe, researchers say, CNET, 6 December 2012, http://news.cnet.com/8301-13578_3-57557569-38/patriot-act-can-obtain-data-in-europe-researchers-say/.

8 N. Perlroth, J. Larson, S. Shane: N.S.A. Able to Foil Basic Safeguards of Privacy on Web, in: New York Times, 5 September 2013, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all.

9 R. Gallagher: Latest Snowden Leak Reveals NSA War on Encryption, but It's Not Yet Dead, Slate, 6 September 2013, http://www.slate.com/blogs/future_tense/2013/09/05/nsa_surveillance_snowden_leak_reveals_nsa_war_on_encryption.html; and N. Perlroth: Government Announces Steps to Restore Confidence on Encryption Standards, BITS, 10 September 2013, http://bits.blogs.nytimes.com/2013/09/10/government-announces-steps-to-restore-confidence-on-encryption-standards/?_r=1.

10 S.A. Aaronson, M.D. Townes: Can Trade Policy Set Information Free? Trade Agreements, Internet Governance, and Internet Freedom, December 2012, http://www.gwu.edu/~iiep/governance/taig/CanTradePolicySetInformationFreeFINAL.pdf.

trust. Meanwhile, some European officials want EU firms to tout their respect for privacy to gain cloud market share. Yet like the U.S., several EU member states monitor private communications of their citizens and non-citizens and, in so doing, devalue the privacy rights they supposedly prize.[11]

We argue that U.S. and EU policy makers must find common ground on privacy. Given the important roles of the U.S. and EU in the Internet economy, the standards they agree on could be the building blocks for internationally accepted standards. The U.S. and the EU should use the opportunity presented by the TTIP negotiations to find common ground on their two very different approaches to privacy.

How did trade policy become a tool to regulate the Internet?

As the Internet belongs to all people in all states, no single government, company or individual controls its rules, processes and mechanisms. But policy makers and netizens early on recognized the Internet would need a shared system of norms and rules to ensure that information could flow as freely as possible across borders. They began by devising voluntary principles. The Organisation for Economic Co-operation and Development (OECD) has spearheaded many of these efforts, including principles on privacy.[12] Building on these efforts, in April 2012, the U.S. and the EU signed a set of non-binding trade-related principles for information and communication technology (ICT) services, which address issues such as transparency and cross-border information flows.[13] However, these principles are neither universal nor binding.

Trade agreements and policies have become an important source of rules governing cross-border information flows for several reasons. First, when information, including personal data, travels across borders in the cloud, it is essentially traded.[14] Second, some 65 percent of the world's population is not yet online, so it is not surprising that these governments see a huge potential for growth in cross-border e-commerce.[15] Third, U.S. and EU policy makers want to both protect their firms' competitiveness and increase market share; hence, they want shared global rules. Finally, these officials recognize that they must develop global regulations with international legitimacy and force. The World Trade Organization (WTO) is an obvious venue to develop these rules. Since its beginning in 1948, members have developed a system of rules as well as exceptions to those rules. These exceptions allow policy makers to limit trade in the interest of protecting national security, ensuring public health or protecting public morals.[16] Today the WTO has 159 members.

The WTO regulates trade in the goods and services that comprise e-commerce.[17] Since 1998, the members of the WTO have agreed not to place tariffs on data flows.[18] Alas, the member states have not found common ground on how to reduce new trade barriers to information flows or whether privacy rules constitute such a barrier.[19] In 2011, several nations nixed a U.S. and EU proposal in which members would have agreed not to block Internet service providers or impede the free flow of information online.[20] Because members have made little progress in trade talks at the WTO, the U.S., EU and other countries have begun to use bilateral and regional free trade agreements (FTAs) to address these issues.

Trade agreements: free flow of information and privacy

In 2011, U.S. Internet companies called on the U.S. Trade Representative (who negotiates trade for the U.S. government) to develop provisions in trade agreements promoting the free flow of information. Companies such as Google also argued that government restrictions on data flows and server location requirements might be data protectionism.[21] Manu-

11 W. Maxwell, C. Wolf: A Sober Look at National Security Access to Data in the Cloud, Hogan Lovells White Paper, 22 May 2013, footnotes 5, 6, p. 1.

12 OECD: Communiqué on Principles on Internet Policymaking, OECD High Level Meeting on The Internet Economy, 28-29 June 2011, http://www.oecd.org/Internet/innovation/48289796.pdf.

13 European Union-United States Trade Principles for Information and Communication Technology Service, 4 April 2012, http://www.ustr.gov/webfm_send/2780.

14 Internet World Stats, http://www.Internetworldstats.com/stats.htm.

15 OECD: The Future of the Internet Economy, OECD Policy Brief, June 2008, http://www.oecd.org/dataoecd/20/41/40789235.pdf; Internet World Stats, op. cit.

16 K. Coppock, C. Maclay: Regional Electronic Commerce Initiatives: Findings from three case studies on the development of regional electronic commerce initiatives, Information Technologies Group, Harvard University, July 2002, http://cyber.law.harvard.edu/itg/libpubs/andes%20pubs/Regional_Ecommerce.pdf

17 S. Wunsch-Vincent: WTO, E-Commerce and Information Technologies, From the Uruguay Round through the Doha Development Agenda, A Report for the UN IDT Task Force, Markle Foundation, 2005, http://www.iie.com/publications/papers/wunsch1104.pdf.

18 The Geneva Ministerial Declaration on Global Electronic Commerce, WT/MIN (98)/DEC/2, 25 May 1998. The WTO had an Internet tax moratorium from 1999 to approximately 2001, see http://www.tax-news.com/news/WTO_Ministers_Extend_Internet_Tax_Ban_For_2_Years____183.html.

19 Discussions on free flow may be revived as part of a plurilateral agreement on the liberalization of services. See WTO Members Seek Services Accord as Doha Stalls, U.S. Says, Bloomberg News, 2 March 2012; and U.S. steps up push for WTO services trade talks, Reuters, 2 March 2012. Also see European Commission: Negotiations for a Plurilateral Deal on Services, Memo, 15 February 2013, http://europa.eu/rapid/press-release_MEMO-13-107_en.htm.

20 General Agreement on Trade in Services (1994) 33 ILM, 1167, Article XIV, n. 5. On U.S. and EU proposal forbidding blocking, see U.S. Tables Second Part of TPP Data Proposal, But Talks Still Preliminary, Inside U.S. Trade, 11 November 2011.

21 Google: Enabling Trade in the Era of Information Technologies: Breaking down Barriers to the Free Flow of Information, 15 November 2010; and Google letter to Don Eiss, Trade Policy Staff Committee, re. Request for Public Comments to Compile the National Trade Estimate Report on Foreign Trade Barriers, Docket No. USTR-2011-0008.

facturers, banks and retailers also pressed for trade agreements provisions to facilitate the free flow of information.[22] However, because many of these companies had built markets based on manipulating personal data, they did not call for binding language on privacy to protect consumer data flows. Soon thereafter, the U.S. Trade Representative began to develop language for free trade agreements to encourage the free flow of information, as well as policies to thwart data protectionism.

The U.S. and the Republic of Korea were the first states to include specific principles related to Internet openness and Internet stability in the electronic commerce chapter of their FTA.[23] The two nations agreed to accept electronic signatures and protect consumers online.[24] They also agreed that "the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."[25] However, this provision does not forbid the use of such barriers, nor does it define necessary or unnecessary barriers. Hence, the reader does not know if legitimate online exceptions to free flow such as privacy regulations are necessary or not.

As of September 2013, the U.S. has not included binding language on privacy in its free trade agreements. It has agreed to general statements that the parties recognize the importance of protecting consumers online and will cooperate on privacy.[26] But the language does not contain specific mechanisms or policies for enforcing privacy standards.[27] Nor does it include clear exceptions for when and how privacy can be breached in the interest of protecting national security or preventing crime.

Despite its strong legal support for privacy at home, the EU also relies on aspirational language on privacy in its free trade agreements. EU Economic Partnership Agreements with developing countries include aspirational language saying the parties recognize their "common interest in protecting fundamental rights and freedoms of natural persons, and in particular, their right to privacy, with respect to the processing of personal data."[28] In the recent EU-Korea FTA, Chapter 6 of the agreement refers to trade in data, and Article 7.43 of the chapter on services says that each party should reaffirm its commitment to protect fundamental rights and freedom of individuals and adopt adequate safeguards to the protection of privacy.[29] But like the U.S., the EU does not say how partners should protect privacy, nor does it include language on exceptions to privacy in the interest of preventing crime or protecting national security.

In 2011, the U.S. proposed actionable language encouraging the free flow of data in the Trans-Pacific Partnership (TPP), a trade agreement under negotiation by 12 countries bordering the Pacific. The language obligated TPP countries not to block the cross-border transfer of information. The U.S. also proposed that countries be prohibited from requiring that data servers be located in their country as a business condition. Finally, the U.S. wanted to ensure that Internet firms could operate in TPP states via e-commerce platforms, without establishing a commercial presence in the country.[30] However, officials from some of the TPP parties have not responded enthusiastically to these provisions.[31] Australia and New Zealand (among others) are concerned that allowing foreign server locations could undermine their citizens' privacy rights.[32] As of this writing, TPP negotiators have not yet found language that all the countries can accept.[33] The U.S.

22 National Foreign Trade Council: Promoting Cross Border Data Flows: Priorities for the Business Community, 2011, http://www.nftc.org/default/Innovation/PromotingCrossBorderDataFlowsNFTC.pdf.

23 See U.S.-Korea FTA, Chapter 15.2, http://www.ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text.

24 U.S. International Trade Commission: Potential Economy Wide and Selected Sectoral Effects of the U.S.-Korea Free Trade Agreement, Investigation No. TA-2104-24, Publication 3949, September 2007, pp. 4-5. fn. 98, http://www.usitc.gov/publications/pub3949.pdf.

25 U.S.-Korea FTA, Chapter 15, Article 15.8 Electronic Commerce, http://www.ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text.

26 U.S.-Panama FTA, Article 15.5, http://www.ustr.gov/sites/default/files/uploads/agreements/fta/peru/asset_upload_file876_9540.pdf.

27 C.S. Kerry: Trans-Atlantic Solutions for Data Privacy, CFK Keynote Address, Second Annual European Data Protection and Privacy Conference, 6 December 2011, http://www.ntia.doc.gov/speechtestimony/2011/cameron-f-kerry-keynote-address-european-data-protection-and-privacy-conference.

28 Economic Partnership Agreement between the CARIFORUM States, of the one part, and the European Community and its Member States, of the other part, in: Official Journal of the European Union, 30 October 2008, L 289, http://trade.ec.europa.eu/doclib/docs/2008/february/tradoc_137971.pdf. Canada has similar provisions.

29 See Article 7.43, http://trade.ec.europa.eu/doclib/docs/2009/october/tradoc_145166.pdf.

30 TPP Countries to Discuss Australian Alternative to Data-Flow Proposal, Inside U.S. Trade, 6 July 2012, http://insidetrade.com/Inside-US-Trade/Inside-U.S.-Trade-07/06/2012/tpp-countries-to-discuss-australian-alternative-to-data-flow-proposal/menu-id-710.html.

31 Speech by R. Atkinson: Cloud Computing for Business and Society, Brookings Institution, Washington DC, 20 January 2010, http://www.brookings.edu/~/media/events/2010/1/20%20cloud%20computing/20100120_cloud_computing.pdf. See also P. Taylor: Privacy Concerns Slow Cloud Adoption, in: Financial Times, 2 August 2011, http://www.ft.com/intl/cms/s/0/c970e6ee-bc7e-11e0-adac-00144feabdc0.html; and J. Baker: EU upset by Microsoft warning on U.S. access to EU cloud, Computerworld, 5 July 2011, http://www.computerworld.com/s/article/9218167/EU_upset_by_Microsoft_warning_on_US_access_to_EU_cloud/.

32 U.S., Australia Make Little Headway Toward Resolving Differences on Data Flows, Inside U.S. Trade, 12 September 2012, http://insidetrade.com/201209122409796/WTO-Daily-News/Daily-News/us-australia-make-little-headway-toward-resolving-differences-on-data-flows/menu-id-948.html.

33 TPP Negotiators In Malaysia Spending Most Time On Toughest Areas Of Talks, Inside U.S. Trade, 17 July 2013, http://insidetrade.com/Inside-US-Trade/Inside-U.S.-Trade-07/19/2013/tpp-negotiators-in-malaysia-spending-most-time-on-toughest-areas-of-talks/menu-id-172.html.

has also proposed similar provisions in the U.S.-EU FTA, the TTIP, which will be discussed below.

Privacy in the EU and the U.S.

In 2010, Facebook CEO Mark Zuckerberg said that "privacy is dead" because of the Internet.[34] Zuckerberg may be wrong; as netizens become aware of the threats to their information, they are increasingly demanding that governments protect their data online.[35] But the U.S. and the EU have different definitions of privacy and distinct strategies to protect it. The EU uses an extensive system of regulation that has broad effects on other nations' approaches to privacy. The U.S. uses a sectoral approach that relies on a mix of legislation and business self-regulation.[36]

The EU sees privacy as both a human and consumer right.[37] Every EU citizen has the right to personal data protection and firms can only collect that data under specific conditions.[38] All 28 EU member states are required to secure the protection of personal data under human rights law. The EU also requires member states to investigate privacy violations.[39]

In 1998, the European Commission's (EC) Directive on Data Protection went into effect. It prohibits the transfer of personal data to non-EU countries that do not meet the EU "adequacy" standard for privacy protection. The EU requires other countries to create independent government data protection agencies and to register databases with those agencies, and in some instances the EC must grant prior approval before personal data processing may begin.[40]

The Directive has had significant effects on trade because of the importance of cross-border data flows to and from the 28 EU members. Some nations such as India and China are weighing how to make their laws interoperable with EU privacy provisions.[41] Other countries such as the Philippines have adopted EU data protection policies.[42]

In 2011, EC officials decided to update the EU's data protection rules. After obtaining extensive public comment, the Commission released its proposed regulation in January 2012. It includes language granting a right to be forgotten, language requiring individuals to directly give their consent for data processing, and language obligating companies and organizations to notify individuals of serious data breaches without undue delay. The draft regulation also requires that non-European companies apply EU data protection law in full and adopts sanctions to punish companies that do not comply.[43] The directive has received over 3,000 proposed amendments, significantly delaying its passage through the Civil Liberties, Justice and Home Affairs Committee. The committee has postponed voting three times.[44] Many Parliamentarians called for a clause forbidding companies from handing over the personal data of EU citizens to non-EU governments, unless the disclosure was done in accordance with a mutual legal assistance treaty or equivalent agreement.[45]

While the EU has one clear regulation on privacy and is updating it to fit new conditions, Congress has not updated several laws with privacy components, including the Electronic Communications Privacy Act (1986) and the Children's Online Protection Act (1998). Regulators have also issued guidance, including the Federal Trade Commission (FTC) Code of Fair Information Practices Online Report (the FTC investigates and enforces many of these privacy policies). However, these laws and regulations have major gaps; they do not require companies to get informed consent to use personal data, nor do they establish a baseline commercial data privacy framework. Although many members want to update privacy policy, Congress has not been able to find

34 E. Barnett: Facebook's Mark Zuckerberg says privacy is no longer a 'social norm', in: The Telegraph, 11 January 2010, http://www.telegraph.co.uk/technology/facebook/6966628/Facebooks-Mark-Zuckerberg-says-privacy-is-no-longer-a- social-norm.html.

35 M. Geist, M. Homsi: Outsourcing Our Privacy?: Privacy and Security in a Borderless Commercial World, in: University of New Brunswick Law Journal, Vol. 54, 2005.

36 M. Samsun: Internet Library of Law and Court Decisions, http://www.internetlibrary.com/topics/right_privacy.cfm; on Sarbanes-Oxley, see Public Law 107 - 204 - Sarbanes-Oxley Act of 2002, at http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html.

37 S. Bellman, E.J. Johnson, S.J. Kobrin, G. Lohse: International Differences in Information Privacy Concerns: A Global Survey of Consumers, in: Information Society, Vol. 20, No. 5, 2004, pp. 313-324.

38 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, adopted by the Council of Europe in Strasbourg, 28 January 1981, at http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

39 Council of Europe: The protection of privacy and personal data on the Internet and online media, Doc. 12695, 29 July 2011, http://www.assembly.coe.int/ASP/Doc/XrefViewPDF.asp?FileID=13151&Language=EN.

40 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in: Official Journal of the European Union, L 281, 23 November 1995, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

41 Interview with Rosa Barcelo, Policy Coordinator, European Commission, DG CONNECT, 24 July 2012. See also G. Shaffer: Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Data Privacy Standards, in: Yale Journal of International Law, Vol. 25, pp. 1-88, 2000.

42 For the Philippines, see Senate Ratifies Bicam Report on Data Privacy Act, Zambo Times, 6 June 2012, http://www.zambotimes.com/archives/48155-Senate-ratifies-bicam-report-on-Data-Privacy-Act.html.

43 European Commission: Commission Proposes a Comprehensive Reform of Data Protection Rules, 25 January 2012, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.

44 EU Panel Data Protection Regulation Vote Delayed Until Fall by Amendments, PRISM, Bloomberg BNA, http://www.bna.com/eu-panel-data-n17179874844/.

45 Ibid.

common ground on new legislation. In February 2012, the White House announced a set of data privacy guidelines titled the "Consumer Privacy Bill of Rights", and the Department of Commerce convened companies, privacy advocates and other stakeholders to develop and implement enforceable privacy policies based on this proposed bill of rights.[46]

Meanwhile, because Congress has not provided guidance on the privacy implications of global data flows, U.S. officials have tried to accommodate the EU system and avoid mandates on privacy. The Department of Commerce developed the U.S.-EU Safe Harbor Framework, which permits trans-border data flows to the U.S. for commercial purposes. Companies (except financial institutions and telecommunications common carriers) may apply for a safe harbor. Companies that accept the relevant voluntary, enforceable code are certified and safeguarded, so long as their practices do not deviate from the code's approved provisions. Those firms that fail to comply with the code's provisions could be subject to an enforcement action by the FTC or a State Attorney General.[47] U.S. firms want to maintain this voluntary self-regulation; in fact, they lobbied in Europe to water down its new approach.[48]

As noted above, the U.S. has proposed language in TTIP regarding free flow of information, server location requirements and the right to operate without a physical presence. We do not know the exact language, as the negotiations are secret. The EC Trade Commissioner Karel de Gucht said that data protection is outside the scope of TTIP.[49] However, in September the EU Ambassador to the U.S. said the negotiations provide an opportunity to develop regulatory coherence on privacy.[50]

We believe American companies may push the U.S. government to make a deal that builds on the data protection directive, facilitates the free flow of information and provides clear exceptions for national security. First, many U.S. Internet companies fear they could lose business, because the global public does not believe that these firms sufficiently protect their privacy.[51] European Commission Vice President and Justice Commissioner Viviane Reding noted that since the Snowden revelations, "A survey…found that 56% of respondents were hesitant to work with...U.S.-based cloud service providers."[52] Some two weeks after the revelations, Reuters reported that as of September 15, Amazon, Google, Microsoft and Facebook had seen no loss in business.[53] However, Amazon, Google, Microsoft and Yahoo, among others, have gone to court to prod the U.S. government to allow them to disclose more information about the nature of their cooperation with the NSA.[54] Hence, we believe they are still worried that they have lost consumer trust. Secondly, although many U.S. firms want a voluntary approach to privacy, it is expensive to implement different national privacy standards. Thus, we believe these firms will ultimately lobby for one global standard for privacy or some form of interoperability. TTIP could serve as the building block for such a standard.

Conclusion

The Snowden revelations may have a silver lining. Vice President Reding recently noted that they seem to be inspiring U.S. officials to place greater value on privacy rights and to develop ways to make surveillance more transparent.[55] Because both the EU and U.S. want TTIP to succeed, the two trade giants will have to find common ground on regulations to achieve data protection. U.S. Internet firms see ensuring the free flow of information as a priority, but U.S. officials will not be able to achieve that goal without including language on privacy acceptable to the EU. We predict the U.S. will work with their allies across the pond to strengthen privacy protection.

46 http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils- blueprint-privacy-bill-rights.

47 The Department of Commerce Internet Policy Task Force: Commercial Data Privacy and Innovation in the Internet Economy, 2010, pp. 44-45, http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf; and Introduction to the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks, www.export.gov/safeharbor.

48 Tech Groups Urge Administration to Protect "Safe Harbor" in EU Talks, Inside U.S. Trade, 22 August 2013.

49 V. Reding: Data Protection Reform: Restoring Trust and Building the Digital Single Market, speech delivered at the 4th Annual European Data Protection & Privacy Conference Brussels, 17 September 2013, p. 3, http://europa.eu/rapid/press-release_SPEECH-13-720_en.pdf; and M. Schaake, FAQ: Transatlantic Trade and Investment Partnership (TTIP), http://www.marietjeschaake.eu/2013/06/faq-transatlantic-trade-and-investment-partnership-ttip/.

50 Center for European Policy Analysis: Insider View: Head of the EU Delegation to the United States, Ambassador João Vale de Almeida, on TTIP, 10 September 2013, http://www.cepa.org/content/insider-view-head-delegation-eu-united-states-ambassador-jo%C3%A3o-vale-de-almeida.

51 J. Garside: Apple, Google and AT&T meet Obama to discuss NSA surveillance concerns, in: The Guardian, 9 August 2013, http://www.theguardian.com/technology/2013/aug/09/nsa-surveillance-apple-google-obama.

52 V. Reding, op. cit. p. 3.

53 J. Menn: Analysis: Despite Fears, NSA Revelations Helping U.S. Tech Industry, Reuters, 15 September 2013.

54 J. Menn: Internet companies in new effort to disclose more on NSA requests, Reuters, 9 September 2013.

55 V. Reding, op. cit., p. 2.