Ghent University

Master of Advanced Studies in European Law

LL.M. Paper

E-commerce and Privacy in the EU and the USA

Author: Agne Kalinauskaite
Supervisor: Prof. Dr. Ignace Claeys

Ghent, 2012
# Table of Contents

Introduction .................................................................................................................................................. 3
1. Concepts of e-commerce and privacy ........................................................................................................... 5
   1.1 Concept of e-commerce .......................................................................................................................... 5
   1.2 Concept of privacy .................................................................................................................................. 6
   1.2.1 Concept of privacy in international law ............................................................................................. 6
   1.2.2 Concepts of privacy in the EU and the USA ....................................................................................... 7
   1.2.3 Privacy and data protection ............................................................................................................... 8
2. Privacy regulation in the context of e-commerce in the EU ............................................................................. 10
3. Privacy regulation in the context of e-commerce in the USA and the self-regulatory approach................. 15
4. Trans-border data flows .................................................................................................................................. 19
   4.1 Safe Harbor Agreement ......................................................................................................................... 19
   4.2 Anti-Counterfeiting Trade Agreement .................................................................................................... 21
4.2 SWIFT case .............................................................................................................................................. 27
5. Certain aspects of e-commerce and privacy in the EU and the USA ............................................................. 32
   5.1 RFID and the Internet of Things .......................................................................................................... 32
   5.2 Cookies .................................................................................................................................................. 36
Conclusions ...................................................................................................................................................... 39
Bibliography ...................................................................................................................................................... 41
Introduction

Both academics and legislators are trying to catch up with the rapidly advancing age of information technology. Harnessing the potential of electronic communications to conduct trade in goods and services is estimated to potentially save customers in the European Union (hereinafter – the EU) internal market €204 billion per year. At the same time, the internet economy is capable of creating 2.6 jobs for each ‘off-line’ job lost. One of the main reasons of relatively low level of online purchasing is the lack of trust in electronic communications for conducting transactions. Increasing consumers’ trust in electronic transactions would foster the development of e-commerce and at the same time – the development of the EU internal market.

This research is a comparative study of privacy and e-commerce in two major world markets that enjoy the world’s largest bilateral trade relationship - the EU and the USA. The comparative manner was chosen due to the fact that e-commerce is a global phenomenon, as it removes the barriers of distance. The different markets tend to merge ever-more on the level of e-commerce. Consequently, it is of extreme importance to look for common standards in the field of e-commerce regulation. The aim of this paper is to reveal the main differences, similarities and tendencies of legal regulation and case-law in the relevant field in the EU and the USA. Possible solutions for future development will be proposed in the end of this research with the view that the ultimate goal of any regulation of electronic communications is substantive technological neutrality – ‘consumers or businesses ought not to prefer one medium over another for transacting on the basis of fearing its increased risks and inadequate remedies.’

To achieve this aim, firstly, the concepts of e-commerce and privacy in the two different jurisdictions will be analyzed. Secondly, the main legislative acts, as well as case-law will be analyzed, focusing on the main principles of privacy in e-commerce. Thirdly, the relevant international agreements between the EU and the USA will be analyzed, paying a special attention to the Anti-Counterfeiting Trade Agreement (hereinafter – ACTA), which was recently signed and is yet to be ratified in the EU, as well as the SWIFT agreement. Fourthly, selected aspects of e-commerce that are particularly important in terms of privacy will be analyzed in a comparative manner (RFID and the internet of things, cookies). The conclusions of the research will highlight the main problematic aspects, tendencies and propose possible future developments of e-commerce and privacy in the EU and the USA.

Due to the limited extent of the paper, some other relevant issues, such as the digital press, social networks, adolescence safety, exposure on-line, smart cards and cloud computing will not be separately analyzed.

The main method used in the research is the comparative method by which legislation and case-law will be analyzed in the respective jurisdictions. Particular statutory provisions will be analyzed in a teleological manner, e.g., relevant EU directives will be analyzed in the light of their legislative aim of privacy protection. Often an effects-based approach will be taken in order to assess the consequences of particular provisions’ implementation in practice, e.g. the SWIFT and the ACTA agreements will be critically analyzed with the view to consider the impact they have on the right to privacy and the balance that they ensure in relation to other rights.

---

2 European Commission, Europe’s Digital Competitiveness Report 2010, 68
4 D. Rowland, U. Kohl, A. Charlesworth, Information Technology Law (Routledge, 2012), 233
The research will be based on a vast variety of sources, including legislative acts and proposals, case-law, working papers of EU institutions, as well as doctrinal resources – articles, books and on-line journals on information technology law.
1. Concepts of e-commerce and privacy

1.1 Concept of e-commerce

The concept of e-commerce varies in different legal documents. However, it could be agreed that not only an increasing number of people use electronic communications as a way to conclude contracts, but also the scope of e-commerce grows in the sense that new kinds of transactions are concluded on-line via different media. Therefore e-commerce is a dynamic concept. The European Initiative in Electronic Commerce\(^5\) describes e-commerce as

   many diverse activities including electronic trading of goods and services, on-line delivery of digital content, electronic fund transfers, electronic share trading, electronic bills of lading, commercial auctions, collaborative design and engineering, on-line sourcing, public procurement, direct consumer marketing and after-sales service.

One of the main documents regulating e-commerce in the EU is Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.\(^6\) This document, however, does not provide a definition of e-commerce. This may be due to the fact that the concept of e-commerce is dynamic by nature, constantly evolving as a result of development of new technologies. Nonetheless, e-commerce could be broadly defined as ‘conducting business by electronic means’.\(^7\) This definition encompasses both B2B (business-to-business) and B2C (business-to-consumer) commercial relationships. In this paper, the focus will be given to the latter – B2C relationship, because issues of privacy protection usually arise with regard to private individuals.

Considering this broad definition of e-commerce, it is important to bear in mind the fact that its origins are relatively old. It is noted in literature that ‘e-commerce began soon after Samuel Morse sent his first telegraph message in 1844, and it expanded across the sea when another message, containing share price information from the New York stock market, linked Europe and North America in 1858’.\(^8\) This almost immediate use of electronic communications for transatlantic information sharing reflects the main feature of e-commerce, i.e. its international nature due to the fact that it disregards distances and borders of the states. Being the main advantage of electronic communications, the rapid sharing of information with anyone around the globe, creates a number of problematic legal aspects. One such difficulty is the protection of privacy when conducting e-commerce. The possibility to share information so fast has, in many ways, changed the face of commerce as such. This is both with regard to international contracting and individualized advertising. Whereas traditional, non-electronic business usually targets masses of consumers, e-commerce is able to use individualized advertising in order to make the business process more effective. Therefore information about users of electronic communications, which is often private information, became a marketable good with the introduction of e-commerce. This leads to the discussion about the second very important concept in the context of e-commerce, namely, privacy.

---


\(^6\) [2000] OJ L 178/1


1.2 Concept of privacy

1.2.1 Concept of privacy in international law

Despite the wide-spread consensus on the importance of privacy, its definition in scholarship is far from uniform. Furthermore, even though privacy is usually described as a fundamental human right, there are a number of constitutions around the world where privacy is not mentioned, including the constitution of the USA. However, in such cases, ‘the courts of many countries have recognized implicit constitutional rights to privacy, such as Canada, France, Germany, Japan and India’.9

Art. 12 of the Universal Declaration of Human Rights states that ‘no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.’

Privacy is also enshrined in Art. 8(1) of the European Convention on Human Rights – ‘everyone has the right to respect for his private and family life, his home and his correspondence’. Art. 8 (2) also states that

> there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The two provisions are very similar in their wording. However, the European Convention on Human Rights is enforceable through the European Court of Human Rights, whereas the Universal Declaration of Human Rights does not have this mechanism. Therefore, the latter can be seen as ‘idealistic ideal’ and the former – as ‘realistic ideal’.10

The exception of state interference for the interests of ‘the economic well-being’ provided in the Art. 8(2) of the European Convention on Human Rights can be considered as the basis for state regulation of restricting the right to privacy when taking part in e-commerce. However, the main question in such a case is what scope of restriction is necessary in democratic society. The answer to this question might depend on how the privacy itself is perceived in a particular society.

The European Court of Human Rights has decided several times on the application of this article in the context of electronic communications. E.g., in case *Malone v. United Kingdom*11 the Court explained that ‘Article 8 covers not only telephone conversations but also traffic information such as a telephone number generated by a telephone conversation.’12 This decision could be of importance when deciding on relevant issues in the context of internet, by analogy, not only the information explicitly provided by a user, but also an IP address of a computer could be regarded as covered by Art. 8 of the Convention.

---

11 App no 8691/79 (ECHR, 2 August 1984)
Another relevant judgment of the European Court of Human Rights was *K.U. v. Finland*, where a violation of Art. 8 was found due to the fact that no effective remedy existed under Finnish law to reveal the identity of the person who had posted an ad about another person on an internet dating site. This case clearly shows that complete anonymity on the internet is not desired and the exceptions provided for in Art. 8(2) are not only allowed for the states, but sometimes also required.

An important document with regard to privacy in the context of e-commerce is the Council of Europe Convention on data protection. The Convention is ‘the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the transfrontier flow of personal data.’ Signed by 44 countries, the Convention gives important guidance to national legislatures and enshrines such basic data protection rights as fair and lawful processing, adequacy, relevance and necessity of data processing. In this Convention privacy is understood as a fundamental human right. The Convention was followed by an explanatory report which *inter alia* highlights the need for an international agreement with regard to international data traffic. This is of importance to the below analyzed problematic of trans-border data flows between the EU and the USA.

### 1.2.2 Concepts of privacy in the EU and the USA

In the relevant jurisdictions – the EU and the USA, privacy is understood differently. As mentioned above, privacy is understood as a human right in Europe and is protected by most of the European Constitutions, as well as by the Charter of Fundamental Rights of the European Union, whereas in the USA there is no constitutional protection of privacy. Scholars do not agree whether the difference of privacy protection in the respective jurisdictions is substantial or merely formal. According to Professor James Whitman, ‘American privacy law is a body caught in the gravitational orbit of liberty values, while European law is caught in the orbit of dignity.’ However, D. J. Solove notes that ‘the basic framework for the European Union Data Protection Directive emerges from an American privacy report written for the Department of Health, Education, and Welfare in 1973 as a part of the effort that led to passage of the federal Privacy act of 1974.’ The report has influenced many laws in the USA and also helped to shape the OECD Privacy guidelines of 1980, which form the basis of privacy laws in countries around the world.

---

13 App no 2872/02 (ECHR, 2 December 2008)
15 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (28 January 1981), CETS 108
18 Art. 1 of the Convention
22 Ibidem
According to C. Bennett, ‘while the nomenclature and codification may vary from country to country, the substance and purpose of these principles are basically the same.’

Scholars often note that the different approaches to privacy lie in different historical circumstances of the respective societies: ‘<…>dictatorships such as the Nazis (who used census data for the holocaust) and repressive regimes in East Europe have sensitized Europeans to the importance of data protection. The absence of such experiences, combined with a long tradition of distrust against government, led to a preference for markets and self-regulation <…>.’ As a consequence, where the market is the main actor to regulate privacy issues, i.e. in the USA, privacy is seen as a commodity that is tradable, and the legal system treats it as though it was private property. In the European Union, as evidenced by the text of Directive 95/46/EC (hereinafter – Data Protection Directive), privacy is regarded as a fundamental human right that should be protected by states.

1.2.3. Privacy and data protection

Privacy is often understood as encompassing different notions. For example, D. J. Solove distinguishes between such different conceptions of privacy – the right to be let alone, limited access to the self, secrecy, control over personal information, personhood, and intimacy. R. Gavison states that privacy has three components: secrecy, anonymity and solitude. When analyzing these perceptions of privacy, it becomes clear that privacy is not only about information, but also relates to physical privacy, what D. J. Solove calls ‘the right to be let alone’ or R. Gavison refers to as ‘solitude’. Therefore the aspect of privacy relevant to this paper can be called ‘informational privacy’.

In the author’s view, not all data gathering should be considered as intrusion of privacy in the context of e-commerce. It is only personally identifiable information that should be seen as restricting or intruding privacy. Such personally identifiable information can be defined as ‘information which can be used to distinguish or trace an individual’s identity either alone or when combined with other public information that is linkable to a specific individual’.

---

23 C. J. Bennett, Regulating privacy – data protection and public policy in Europe and the United States (Cornell University Press, 1992) 96
25 Ibidem
26 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 [1995] OJ L 281. High level of protection of privacy as a fundamental right is mentioned as an objective of the directive in point 10 of the preamble and Art 1(1)
29 The term ‘informational privacy’ is mentioned in the works of several authors, e.g. Herman T. Tavani ‘Informational privacy, data mining, and the Internet’ [1999] Ethics and Information Technology 1(137–145) Kluwer Academic Publishers
30 Secretary of State for the Home Department, Cmnd 7341
assessed not separately, but together with other data that can be accessed by that same data controller.

In the Data Protection Directive (Art. 2(a)) personal data is understood as ‘any information relating to an identified or identifiable natural person <…>; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity’.

Despite the widely divergent understanding of privacy in different societies, concerns about privacy are voiced louder and louder, especially in the context of ever-increasing use of information technologies. ‘Countless commentators have declared that privacy is “under siege” and “attack”; that it is in “peril,” “distress,” or “danger”; that it is “eroding,” “evaporating,” “dying,” “shrinking”, “slipping away,” “diminishing” or vanishing; and that it is “lost” or “dead”.32

It is the author’s view that privacy is in fact in danger, however, not yet dead. Recent worldwide protests against the ACTA agreement (discussed below) is evidence that people in different societies do want to protect the degree of privacy that they still enjoy.

---

2. Privacy regulation in the context of e-commerce in the EU

The right to privacy is mentioned both in the text of the Lisbon Treaty33 and in the Charter of Fundamental Rights of the European Union. Art. 16(1) of the Treaty on the Functioning of the European Union (hereinafter – TFEU) states that ‘everyone has the right to the protection of personal data concerning them’. A more precise description of the right to protection of personal data is enshrined in Art. 8 of the Charter of Fundamental Rights of the EU as follows:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

In one of his speeches, Peter Hustinx, European Data Protection Supervisor, has compared data protection to other rights given under the EU Treaties, like the right of free movement of persons. He also stressed that persons can invoke the right directly before the national courts. Although EU legislation may foresee some limitations of the right, they ‘can not render impossible the exercise of the core elements of the right to data protection, mentioned in the Charter.’34

The main secondary document regulating data protection in the EU is Directive 95/46/EC.35 It establishes data protection principles such as fair and lawful processing, specified, explicit and legitimate purposes of data collection, adequacy, accurateness and necessity of data collection, consent of the data subject (Art. 6(1), 7). Provisions of the directive have been the subject of dispute before the Court of Justice of the European Union in case C-465/00 Rechnungshof v Österreichischer Rundfunk and Others.36 One of the main issues in question in this case was the direct applicability of Articles 6(1)(c) and 7(c) and (e) of the directive. The Court concluded that the ‘provisions are sufficiently precise to be relied on by individuals and applied by the national courts <…> to oust the application of rules of national law which are contrary to those provisions.’37 It is noted in the scholarship that due to the similar wording, other parts of Articles 6 and 7 could also be considered to have direct effect before the national courts.38 This judgment is very important with regard to the different implementation of the directive in national laws. It indicates that in cases when the directive is incorrectly implemented, individuals can still claim their rights directly before the national courts. This is especially important having in mind the importance of privacy as a fundamental right and that its assurance comes from the legislature of the EU in this case. At the same time it limits the discretion of national legislatures and increases the powers of national courts with the view of protecting the fundamental human right to privacy.

The part of the directive that is especially relevant for the analyzed topic is Chapter IV ‘Transfer of Personal Data to Third Countries’. It establishes the ‘adequate level of protection’

---

36 [2003] ECR I-04989
37 Par. 100, 101 of the judgment
standard for data that is transferred from a Member State to a third country. The adequacy is
decided upon taking into account various factors, such as ‘the nature of the data, the purpose and
duration of the proposed processing operation or operations’,<...> the rules of law, both general and
sectoral, in force in the third country in question and the professional rules and security measures
which are complied with in that country.’^39 If the Commission finds that the level of protection in
the third country is not adequate, ‘Member States shall take the measures necessary to prevent any
transfer of data of the same type to the third country in question.’^40 Therefore the mechanism that is
constructed in this article is by its nature setting up a global scheme of data protection, where the
EU data protection standards are the minimum standards. Even though the provisions themselves
have no direct effect on any of the third country data protection laws, it does affect them indirectly,
having in mind the economic loss that third countries would incur not being able to transfer the data
relating to EU citizens to their territory (especially considering the continuously and rapidly
growing e-commerce which would be hindered by blocking the data flows).^41

An important case decided by the Court of Justice of the European Union on the issue
of trans-border data flows was case C-101/01 Bodil Lindqvist.^42 Here one of the main questions at
stake was the meaning of ‘transferring data to a third country’. The reference for a preliminary
ruling was made by a Swedish court in criminal proceedings where Mrs. Lindqvist ‘was charged
with breach of the Swedish legislation on the protection of personal data for publishing on her
internet site personal data on a number of people working with her <...>.’^43 As the internet site was
in fact accessible to users from third countries, the question here was whether publishing data on an
internet site amounted to transferring data to third countries. The Court took a teleological approach
here and drew its attention to the state of development of the internet in times when the directive
was enacted, as well as to the absence of criteria applicable to the use of internet in Chapter IV of
the directive. Moreover, the Court also took an effects-based approach by noting that, were the
provisions interpreted as meaning that there is a transfer to a third country each time when data is
uploaded on an internet page and ‘if the Commission found <...> that even one third country did
not ensure adequate protection, the Member States would be obliged to prevent any personal data
being placed on the internet.’^45 Consequently, it was concluded that there was no transfer of data to
third countries in the meaning of Chapter IV of the directive when personal data was uploaded to an
internet page. ^46

This case illustrates that being a 17 year old document enacted in times when only 1%
of Europeans were using the internet^47 the directive is in need of change. Even though the basic
principles enshrined in the directive remain valid and relevant, in the background of fast new
technologies development (e.g. social networking sites, cloud computing, smart cards), the
regulatory framework is not accommodated well enough to face these new challenges. ^48 The
European Commission has recently proposed a reform package of the current regulatory framework
which includes a regulation setting out general data protection rules and a directive ‘on protecting

---

^39 Article 25(2)
^40 Article 25(4)
^41 The problematic of adequateness of the protection that is provided in the USA is analyzed in subchapters 4.1 and 4.3
(Safe Harbor Agreement and SWIFT case)
^42 [2003] ECR - 12971
^43 Par. 2
^44 Par. 68
^45 Par. 69
^46 Ibidem
^47 European Commission, Press Release, ‘Commission proposes a comprehensive reform of data protection rules to
increase users’ control of their data and to cut costs for businesses’ (Europa, Press Releases RAPID, 25 January 2012)
personal data processed for the purposes of prevention, detection, investigation or prosecution of
criminal offences and related judicial activities.”

The main proposed changes are the following: a ‘right to be forgotten’, explicit consent for data processing, easier access to one’s own data, reduction of administrative burden for companies and organizations, national data protection authorities would gain enforcement powers. Another very important feature of the proposed changes is that the legislative document regulating general data protection would take a form of a regulation, therefore removing the existing differences in the implementation of the current directive in Member States.

The proposed changes are important for better protection of personal data of EU citizens and for fostering development of e-services (e.g. the proposed freedom to transfer personal data from one service provider to another would increase competition between e-service providers, because users would be able to easily move between different service providers). However, it remains to be seen how the changes will be implemented in practice. E.g., the requirement of acquiring an explicit consent for data processing may be technically complicated issue and it also may be time consuming for the user to explicitly agree to each data processing and read the conditions of the data processing. Therefore implementation of the regulation depends highly on the technical solutions that can be found in order to properly and efficiently embody the legal requirements. That requires co-operation between the e-service providers and data protection authorities, e.g. in implementing privacy by design. Furthermore, the proposals are still being discussed and criticized by some experts in the field and may possibly undergo changes until they are adopted.

Other very important directives currently regulating private data protection in the context of e-commerce are the following: Directive 2002/58/EC on privacy and electronic communications, Directive 2006/24/EC on data retention and Directive 2009/136/EC amending Directive 2002/22/EC. The final directive has brought a certain amount of confusion in the legal situation concerning cookies. The issue will be discussed below in the subchapter 5.2 Cookies.

Directive 2006/24/EC on data retention obliges Member States to adopt measures in order to ensure that particular categories of telecommunications data would be retained for a period...


50 Ibidem

51 Ibidem


53 The problematic of user’s consent in the context of cookies is discussed below in subchapter 5.2

54 E.g. the proposal for the regulation is criticised by Article 29 Data Protection Working Party as granting too much powers for the European Commission in the process of adopting delegated and implementing acts in order to apply certain provisions of the regulation in practice. Nikolaj Nielsen, ‘Commission data protection reforms under fire’ (EUObserver, 3 May 2012) <http://euobserver.com/22/116129> accessed 7 May 2012


of 6 to 24 months. The provisions of the directive have been criticised by scholars as non-compliant with the proportionality principle. Even though the directive aims at assisting criminal investigations, it has a direct effect on the over-all development of telecommunications use and e-commerce as well, considering that restriction of on-line privacy by public authorities may as well discourage users from participating in e-commerce.

The directive came under scrutiny of the Court of Justice of the European Union, when Ireland challenged the legal basis on which the directive was adopted. The action was dismissed in that case. However, the Court of Justice has not yet analyzed the directive in the light of protection of privacy as a fundamental human right.

Another directive that is of relevance to privacy in e-commerce is directive 2004/48/EC on the enforcement of intellectual property rights. Art. 8 of the directive establishes cases when the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided. There are two important safeguards enshrined in this provision. Firstly, the information on the infringing goods and services may only be obtained according to an order of competent judicial authority. Secondly, the information may be obtained only in cases when the infringement is ‘on a commercial scale’, this criterion being decisive.

This provision is of relevance to some debatable aspects of the below discussed Anti-Counterfeiting Trade Agreement as it may serve as an example to demonstrate that the proposed regulation of the Anti-Counterfeiting Trade Agreement would in fact diminish the protection of privacy by substantially reducing the existing procedural safeguards with respect to privacy in e-communications.

Equally important in terms of privacy protection in the context of e-commerce is Directive 2009/140/EC which adds a new paragraph (3a) to the Directive 2002/21/EC. The new paragraph establishes that any of these measures regarding end-users’ access to, or use of, services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and with general principles of Community law, including effective judicial

60 Case C-301/06 Ireland v European Parliament and Council [2009] ECR I-00593
63 Chapter 4.2
This provision in principle *expressis verbis* reiterates that restrictions of privacy in the context of e-communications should take place in accordance with the basic standards of human rights protection (appropriateness, proportionality and necessity within a democratic society, effective judicial protection and due process). It clearly reflects the historically enrooted European approach to privacy as a fundamental human right and is an important reminder both in the process of EU legislative developments and when concluding any relevant international agreements that may unduly restrict the right to privacy.

---

66 Emphasis added.
3. Privacy regulation in the context of e-commerce in the USA and the self-regulatory approach

In contrast to the EU regulatory framework, there is no general data protection law on the federal level in the USA. The basic approach, embodied in the Clinton/Gore 1997 Framework for Global Electronic Commerce, is that governance of the internet and e-commerce should be led by the private sector.67 Existing laws are sectoral, regulating particular privacy aspects, such as healthcare data (Health Information and Portability Accountability Act68), financial data (Gramm-Leach-Bliley Act69), children’s privacy protection (Children’s Online Privacy Protection Act70),71 as well as privacy in relation to video rentals (Video Privacy Protection Act72) and credit reporting (Fair Credit Reporting Act73), etc.74

Several legislative initiatives related to privacy in the context of e-commerce have recently been tabled before the legislators of the USA. The most controversial ones are the Stop Online Piracy Act (hereinafter - SOPA75) and Protect IP Act (hereinafter - PIPA76).77

SOPA has been introduced to the U.S. House of Representatives in October 2011 with the aim of strengthening enforcement of intellectual property rights online. One of the most controversial aspects of the proposal in terms of privacy is section 102 which states that a service provider is obliged to block a website that is infringing intellectual property rights. This provision in practice ‘could require Internet providers to monitor customers’ traffic and block the addresses of Web sites suspected of copyright infringement.’78 A similar provision is also present in PIPA, which has been introduced before the U.S. Senate in May 2011.

Both of the proposals have been halted due to the wide-spread protests and petitions signed by millions against them.79 However, it is important to bear in mind the basic tendency of limiting privacy on-line by laws designed for intellectual property rights’ enforcement when analyzing the recent international developments in the area (namely, the ACTA).

Getting back to the general data protection regulatory framework that currently exists in the USA, as mentioned above, the area is left to industry self-regulation. However, it is important to note that the self-regulation itself is perceived differently in the EU and in the USA. Whereas in the EU self-regulation usually means ‘close cooperation between industry and government in the

---

68 1996, H.R. 3103
69 1999, S. 900
70 1998, H.R. 4328
72 1988, S. 2361
73 1970, S. 1114
75 2011, H.R. 3261
76 2011, S. 968
77 One of the subsequent legislative initiatives, controversial in terms of privacy, is the Cyber Intelligence Sharing and Protection Act (CISPA) (H.R. 3523), proposed in November 2011. However, the privacy protection limitations contained therein relate to public security issues, therefore the proposal will not be analyzed in this paper.
The pursuit of a jointly defined policy goal, in the USA it is understood as a phenomenon where ‘companies get to make decisions about the rules that regulate markets and that government stays out entirely.’ Therefore when one speaks about self-regulation in the USA, it means that the rules are created by the private entities themselves, without the need of any government verification.

More precisely, in the context of e-commerce, commercial websites or online service providers in the USA are not only free to decide on the content of their privacy policy, but they are also not required to maintain privacy policies. However, if they do maintain a privacy policy, they are potentially subject to litigation by the Federal Trade Commission if they do not adhere to their stated privacy practices. It will be considered an unfair and deceptive trade practice for a website or online service provider to violate its own privacy policy. This self-regulatory approach might be debatable, as some websites, in order to avoid litigation, might not maintain any privacy policies, or, alternatively, under the link to their privacy policy statement they may provide the terms of its privacy policy that are in fact not privacy-friendly, or are too complex for an average consumer to understand.

Although in the literature it is argued that, as a result of such self-regulatory approach, ‘users in the U.S. protect themselves by being very selective in the kinds of information they want to reveal and to which websites they reveal the information,’ this also can be debated. Firstly, it is hardly realistic that users read privacy statements of each of the commercial websites that they visit. Secondly, even if users would, privacy statements are often too complex for specialists to understand, let alone for average users. This can be exemplified by a recent change of Google’s privacy policy. Whereas it was presented by Google as ‘simplifying its privacy rules’ and ‘consolidating 60 privacy policies into one’, the changes have raised ‘strong doubts about the lawfulness and fairness of such processing and its compliance with European data protection legislation’ to both national and EU data protection authorities. Furthermore, the French data protection authority noted that ‘Google’s explanation of how it will use the data was too vague and difficult to understand “even for trained privacy professionals.”’ Considering the position of Google in the e-market, it is difficult to believe that users would stop using its services because of the new privacy policy that is expressed in vague terms. At the same time, by enacting a vague privacy policy that intrudes on the privacy of users, the entity that has a strong position in the market, can gain even more profit by selling the private data of the users and reinvesting the money in strengthening its position in the market. Consequently, it becomes even more difficult for users to effectively oppose the privacy rules of a stronger undertaking in the market that is disproportionately intruding their privacy. As a result, the companies that choose not to mistreat private data may find themselves at a competitive disadvantage as they do not reap extra profit from selling unfairly gained data. This and similar situations clearly illustrate the main disadvantages of the self-regulatory approach in the area of privacy and e-commerce.

The self-regulatory approach in the USA is being justified by several arguments, such as the ‘free flow of information <...>, promotion of commerce and wealth and “a healthy distrust for

---

81 Ibidem
83 Ibidem
84 Ibidem
government solutions.” Nevertheless, according to a report of Federal Trade Commission, already in 2000, 92% of respondents did not trust privacy policies posted on-line and 82% suggested government legislation to protect their privacy. During the 10 following years the situation has not changed significantly. Even though the Safe Harbor Principles came into being, they are still based on the same system of self-regulation. In its report of 2010, the Federal Trade Commission highlighted the deficiencies of the existing self-regulatory model, such as the failure “to recognize a wider range of privacy-related concerns, including reputational harm or the fear of being monitored” as well as the overall harm-based approach (meaning that the infringement of privacy policy is usually only detected if a user sues the website controller for non-compliance with the privacy policy; whereas usually by that time a lot of private data would be mistreated by the website controller). In the same report, the Federal Trade Commission has proposed a new framework for consumer privacy protection. It is interesting to note that the EU Data protection directive was taken into account while preparing this framework. The proposed framework establishes such principles like data security, reasonable collection limits, data accuracy, etc. Another legislation project was proposed by senators Kerry and McCain, including rights of internet users such as the right to security and accountability, the right to notice, consent, access and correction of information. However, the bill would prevent private rights of action. Although this project has had the support of the industry, it has been criticized by privacy advocates as providing insufficient protection.

There have been more legislative proposals introduced on the same issue, representing diverse approaches to privacy protection in e-commerce. So far it is not clear which of the proposals is prevailing and will eventually be enacted. Nevertheless, the overall tendency of revising the privacy protection standards with the view to strengthening them and, possibly, aligning them with the standards of privacy protection in the EU, is very positive. One of the aspects that foster the enactment of a federal law concerning data protection in e-commerce is the fact that the EU is planning to enact legislation in the form of regulation. Such a regulation may be perceived as a more serious restriction to the American companies conducting business in the EU in comparison to the current situation, where the issue is regulated by a directive. The variable implementation of the directive in different Member States makes the overall data protection standards less enforceable in the sense that the foreign undertakings can choose to act in a Member State where those standards are either not implemented or loosely implemented. Therefore, it may be predicted that the overall tendency of revising the privacy protection standards will be strengthened and the successful implementation will foster a more harmonized approach to privacy protection in e-commerce. So far it is not clear which of the proposals is prevailing and will eventually be enacted. Nevertheless, the overall tendency of revising the privacy protection standards with the view to strengthening them and, possibly, aligning them with the standards of privacy protection in the EU, is very positive. One of the aspects that foster the enactment of a federal law concerning data protection in e-commerce is the fact that the EU is planning to enact legislation in the form of regulation. Such a regulation may be perceived as a more serious restriction to the American companies conducting business in the EU in comparison to the current situation, where the issue is regulated by a directive. The variable implementation of the directive in different Member States makes the overall data protection standards less enforceable in the sense that the foreign undertakings can choose to act in a Member State where those standards are either not implemented or loosely implemented. Therefore, it may be predicted that the overall tendency of revising the privacy protection standards will be strengthened and the successful implementation will foster a more harmonized approach to privacy protection in e-commerce.

89 Discussion below in subchapter 4.1
90 Federal Trade Commission, Preliminary FTC Staff Report, Protecting Consumer Privacy in an Era of Rapid Change, A proposed framework for businesses and policy makers (December 2010), iii
91 Ibidem
92 Ibidem, 9
93 Ibidem, 39
94 Ibidem, 44
95 John Kerry, U.S. Senator for Massachusetts, ‘Commercial Privacy Bill of Rights’
96 Cecilia Kang, ‘Senators Introduce Internet Privacy Bill’ (Consumer Watchdog, 4 December 2011)
97 Ibidem
eventual enactment of a federal law in the USA will, to large extent, also depend on the regulatory changes concerning data protection in the EU. The aspiration of closer interaction of the both legal systems has also been confirmed in a very recent EU-U.S. joint statement on data protection, where it was noted that ‘... as expressed in the Obama Administration’s privacy blueprint, the United States is committed to engaging with the European Union and other international partners to increase interoperability in privacy laws and regulations, and to enhance enforcement cooperation.’

The integration of privacy regulation is dictated by the very nature of e-market. It is very positive that the issue has been acknowledged on the political level. It is also important to foresee that in the process of forthcoming legislative change, strong lobbying by the entities having major commercial interest in free data flows will be present in both jurisdictions. It is the author’s view that in order to find the proper balance between privacy protection and commercial interests, it is essential to take the views of civil society representatives and academics into account, the point of departure being that privacy is a fundamental human right. Another important factor to be considered is the basic consumer welfare: in order to foster development of e-commerce, one should be able to buy goods and services via electronic means by retaining the same level of privacy protection as if one would be taking part in the off-line market.

---

4. Trans-border data flows

4.1 Safe Harbor Agreement

After the adoption of EU Data Protection Directive, there was a risk of hindrance to data flows between the EU and the USA. Namely, Art. 25(1) of the Directive states that transfer of personal data to third countries may take place only if the third country in question ensures an adequate level of protection. As mentioned above, this provision of the EU Data protection directive can be seen as an incentive for other countries to raise their data protection standards. ‘By 1999, the EU was negotiating with the USA, Japan, Australia, and New Zealand. One year later, Canada, Australia, Taiwan, Norway, Iceland, Hong Kong, Poland, Hungary, and Switzerland all had either implemented privacy legislation or were in the process of doing so.’ 99 As J. R. Reidenberg noted, ‘countries elsewhere are looking at the European Directive as the basic model for information privacy’, 100 and, after adoption of the Directive, there were ‘significant legislative movements toward European-style data protection in Canada, South America and Eastern Europe’. 101 However, due to the significantly divergent understanding and regulation of privacy in the EU and the USA, a separate agreement was negotiated. It was named ‘the Safe Harbor Agreement.’

In essence, this agreement provides for a set of principles, which can be voluntarily adhered to by organizations of the US. 102 Furthermore, the system is based on self-certification, i.e. a participating organization has to publicly declare that it adheres to the U.S.-EU Safe Harbor Framework’s requirements and recertify itself annually with the Department of Commerce (in the USA) in writing. 103 There are seven Safe Harbor privacy principles which include elements such as notice, choice, access, and enforcement. 104 The principles mainly reflect the same standards that the EU Data protection directive is based on. However, the issue of enforcement is regulated differently, because here it rests mainly in the hands of private individuals. As it is noted in the agreement itself ‘enforcement <...> will be carried out primarily by the private sector. Private sector self-regulation and enforcement will be backed up as needed by government enforcement of the federal and state unfair and deceptive statutes.’ 105 This particular aspect has received criticism in literature. It is noted that

European Commission expressly relied on representations made by U.S. Department of Commerce concerning available damages in American law. The memorandum, however, made misleading statements of U.S. law. For example, the memorandum provides a lengthy discussion of the privacy torts and indicates that the torts would be available. The memorandum failed to note that the applicability of these tort actions to data processing and information privacy has never been established by U.S. courts and is, at present, purely theoretical. <...> all three of the state courts that have addressed this tort in the context of data privacy have rejected it. 106

---

101 Ibidem
103 Ibidem
104 Ibidem
105 Ibidem
106 Joel R. Reidenberg. E-commerce and transatlantic privacy. Houston Law Review (38) 717, 745
Furthermore, the legal authority of Federal Trade Commission (the body that is responsible for enforcement of the Safe Harbor Agreement in the USA) to enforce this agreement is also questioned in literature. It is noted that even though it has jurisdiction to acts or practices ‘in or affecting commerce’, however, at no time the FTC was given the competence to protect foreign consumers, which the Safe Harbor agreement is in fact designed for.

The legal status of the agreement in the EU is also debatable. Even though the agreement took place in form of exchange of letters, procedurally it was not an international treaty, but only an approval by the European Commission, certifying that the standards of Safe Harbor are adequate to the European standards. However, the Safe Harbor principles were not yet applied in the USA when they were approved by the European Commission. Furthermore, in order to enter into negotiations for the adequacy of the data protection provided in a third country, the European Commission first had to find that the protection provided in the USA was inadequate. However, in this case the Commission made no such finding, and that is considered to be a significant administrative law defect in literature.

When comparing the standards that are established in the Safe Harbor Agreement with those protected by EU law, it is obvious that the voluntary self-certification system is in fact not of the same level as the system in Europe, where these standards are obligatory to all data controllers. Therefore, it is debatable whether the Safe Harbor agreement is in fact an agreement on some adequate standards, or rather an agreement to disagree – whereas in form it looks adequate to the European standards, in practice the enforcement of the agreement in the USA remains doubtful.

Even though the terms of the agreement can be justified by the need to quickly find a solution for the problems arising from divergent data protection regimes in the EU and the USA, the Safe Harbor principles can only serve as an interim solution. Therefore, it should be agreed with the view that an international agreement should be concluded, which would assure that private data of the European citizens will be granted the same protection under the USA law as under the EU law. Considering the current legislative debates in the USA on a new law that would establish higher standards of privacy protection in the context of e-commerce, a respective international agreement between the two countries could be feasible. Furthermore, even a more positive solution would be a multilateral treaty, possibly in the framework of the WTO, establishing standards of privacy protection that would resemble those of the EU.

---

107 Ibidem
108 Ibidem
109 Ibidem, 742
111 Ibidem
4.2 Anti-Counterfeiting Trade Agreement

Undoubtedly the most debatable recent initiative in the field of international e-commerce and privacy is the Anti-Counterfeiting Trade Agreement (hereinafter – ACTA). It has attracted not only the attention of experts in the field, but also of the general public. Worldwide protests took place against the agreement in the beginning of 2012. Criticism and concerns were expressed by representatives of governmental and non-governmental organisations, and academics. The criticism mainly focused on the secrecy of the negotiations and the substance of the agreement. E.g. Amnesty International, the EU Economic and Social Committee, the European Data Protection Supervisor, and worldwide coalition of NGOs and businesses have strongly criticised the agreement as violating fundamental human rights, including the right to privacy.

ACTA’s secret negotiation process is one of the worrying aspects constantly referred to by critics. Until the final text of the agreement was announced, negotiations were conducted secretly and the public could only discuss some parts of the agreement that were ‘leaked’. A particularly striking issue is that the European Parliament was not constantly informed about the negotiation process, whereas the American industry representatives took part in the negotiations after signing non-disclosure agreements.

---


113 Amnesty International: ‘The EU should reject ACTA in its current form – implementing the agreement could open a Pandora’s Box of potential human rights violations’ (<Amnesty International, 10 February 2012)> accessed 23 March 2012

114 ‘According to the Committee, ACTA’s approach is aimed at further strengthening the position of rights holders vis-à-vis the “public”, certain of whose fundamental rights (privacy, freedom of information, secrecy of correspondence, presumption of innocence) are becoming increasingly undermined by laws that are heavily biased in favour of content distributors.’ Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Single Market for Intellectual Property Rights – Boosting creativity and innovation to provide economic growth, high quality jobs and first class products and services in Europe, COM(2011) 287 final (18 January 2012)

115 The European Data Protection Supervisor ‘regrets that he was not consulted by the European Commission on the content of an agreement which raises significant issues as regards individuals’ fundamental rights, and in particular their right to privacy and data protection’, European Data Protection Supervisor Press Release, ‘Anti-Counterfeiting Trade Agreement: EDPS warns about its potential incompatibility with EU data protection regime’ (22 February 2010) <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2010/EDPS-2010-03_ACTA_EN.pdf> accessed 23 March 2012


Over 75 Law Profs Call for Halt of ACTA (Washington College of Law, 28 October 2010) <http://www.wcl.american.edu/pijip/go/blog-post/academic-sign-on-letter-to-obama-on-acta> accessed 23 March 2012
Kader Arif, the ‘rapporteur’ for ACTA in the European Parliament, resigned from this position, criticising the agreement ‘in the strongest possible manner’ for the lack of ‘inclusion of civil society organisations, a lack of transparency from the start of the negotiations’ and ‘exclusion of the EU Parliament’s demands that were expressed on several occasions’, so much so that he refused to ‘take part in this masquerade’. Surprisingly, even some of the officials who signed or supported the agreement, subsequently expressed their public regret for their unquestioning acceptance.

The destiny of the agreement remains unclear. Even though some of the Member States have halted the signing process, the European Commission decided to refer the ACTA agreement to the European Court of Justice. However, the opponents of the agreement encourage the outright rejection of ACTA in the European Parliament as soon as possible, instead of extensively delaying the decision until the ruling of the European Court of Justice. The International Trade Committee of the European Parliament has rejected the possibility to refer ACTA to the European Court of Justice. Therefore it is possible that the European Parliament will vote on the agreement even though it will be referred to the European Court of Justice by the European Commission.

The main provisions of the agreement that raise concerns about privacy are Art. 4, 11 and 27(4).

Art. 11 states that:

Without prejudice to its law governing privilege, the protection of confidentiality of information sources, or the processing of personal data, each Party shall provide that, in civil judicial proceedings concerning the enforcement of intellectual property rights, its judicial authorities have the authority, upon a justified request of the right holder, to order the infringer or, in the alternative, the alleged infringer, to provide to the right holder or to the judicial authorities, at least for the purpose of collecting evidence, relevant information as provided for in its applicable laws and regulations that the infringer or alleged infringer possesses or controls. Such information may include information regarding any person involved in any aspect of the infringement or alleged infringement and regarding the means of production or the

---

121 E.g. The representative of Slovenia Helena Drnovšek Zorko, has expressed her regrets for signing the agreement, ‘Why I signed ACTA’ (31 January 2012) <http://metinalista.si/why-i-signed-acta/> accessed 23 March 2012. The Prime Minister of Poland has also announced that his earlier support for ACTA was a mistake, ‘Poland and Slovenia back away from ACTA’ (18 February 2012) <http://www.scotsman.com/news/poland-and-slovenia-back-away-from-acta-1-2124655#> accessed 23 March 2012
122 ‘The states which decided not to sign the ACTA include Cyprus, Estonia, Germany, the Netherlands and Slovakia while the cabinets of Poland, the Czech Republic, Latvia and Austria decided to put off the ratification of the ACTA.’ (24 February 2012) <http://freepl.info/1785-romania-has-stopped-acta-ratification> accessed 24 March 2012
126 Although there are several other provisions that in one way or the other relate to privacy, e. g. Art. 34 regulates information sharing between Parties to the agreement. Douwe Korff, Ian Brown, ‘Opinion on the compatibility of the Anti-Counterfeiting Trade Agreement (ACTA) with the European Convention on Human Rights & the EU Charter of Fundamental Rights,’ prepared at the request of The Greens / European Free Alliance in the European Parliament <http://en.act-on-acta.eu/images/6/6f/ACTA_and_fundamental_rights.pdf> accessed 12 April 2012
channels of distribution of the infringing or allegedly infringing goods or services, including the identification of third persons alleged to be involved in the production and distribution of such goods or services and of their channels of distribution.  

This article makes the obligation to provide access to the information compulsory for the states, whereas it is voluntary under Art. 47 of TRIPS. Furthermore, the information may be requested both about infringers and alleged infringers whereas under Art. 47 of TRIPS it may be requested only about infringers. Moreover, the proportionality requirement that is enshrined in Art. 47 of TRIPS, is not present in the relevant article of ACTA.

Art. 27(4) reads as follows:

A Party may provide, in accordance with its laws and regulations, its competent authorities with the authority to order an online service provider to disclose expeditiously to a right holder information sufficient to identify a subscriber whose account was allegedly used for infringement, where that right holder has filed a legally sufficient claim of trademark or copyright or related rights infringement, and where such information is being sought for the purpose of protecting or enforcing those rights. These procedures shall be implemented in a manner that avoids the creation of barriers to legitimate activity, including electronic commerce, and, consistent with that Party’s law, preserves fundamental principles such as freedom of expression, fair process, and privacy.

It is to be noted that according to this article, the information identifying a subscriber has to be disclosed by an online service provider also in the cases where the account of a subscriber was only allegedly used for infringement, i.e. the infringement needs not to be proven. This regulation is different from other international treaty provisions, namely TRIPS, where Art. 47 imposes a similar obligation only to an infringer. The expression of ‘legally sufficient claim’ is vague and allows a wide interpretation, possibly to the disadvantage of the internet users. Therefore this provision could be interpreted as requiring the disclosure of information identifying a subscriber whenever the right holder makes a general claim that some infringements have occurred.

Here two very important aspects should be noted. Firstly, the data that allows identifying a particular subscriber is personal data, because it is connected to a particular person. Secondly, this provision, allowing disclosure in cases of ‘alleged infringements’, can be interpreted as allowing disclosure of personal information in cases when a right holder claims that the subscriber is possibly infringing the intellectual property rights. This means that the competent authority could issue orders allowing ‘monitoring and analysis of all subscribers to a particular ISP,  

127 Emphasis added
129 Opinion of European academics on Anti-Counterfeiting Trade Agreement, 5 <http://www.iri.uni-hannover.de/tl_files/pdf/ACTA_opinion_110211_DH2.pdf> accessed 12 April 2012
130 Ibidem
131 Ibidem
132 Emphasis added
133 Ibidem
if a right holder could make a case that at least some of the ISP’s subscribers are infringing his or her IP rights (which in reality means always). Therefore it may be concluded that this provision allows for massive monitoring of data flows over the internet, including all the personal information that is a part of such data. The regulation established in ACTA significantly improves the position of the intellectual property right holders. Under the current regulation and case law both in the EU and in the USA, intermediaries (both internet service providers and Web 2.0 providers) are in general not obliged to monitor data flows transferred by users. Furthermore, data protection rules in the EU allow for the disclosure of internet users’ identity only in particular circumstances. ACTA would not only allow general monitoring of the internet content, but would also concentrate the power to do that in the hands of the intellectual property right holders. This far-reaching power is especially problematic in terms of data privacy and it has been criticized by several data protection authorities as violating human rights protection standards enshrined in the European Convention on Human Rights, in current EU law and, furthermore, in the Cybercrime convention that is also signed and ratified by the USA.

Furthermore, Art. 27(4) foresees that competent authorities may have the authority to order an online service provider to disclose relevant information, whereas in TRIPS a similar right is reserved for judicial authorities only. This should be considered as an insufficient safeguard of privacy because according to the provision, a non-judicial authority could allow access to information identifying an individual where an infringement is just alleged. The non-judicial authority could be ‘the executive or some regulator, whose independence and impartiality need not be ensured.’ The reference to the ‘fundamental principle’ of privacy is also very abstract and does not specify any sufficient mechanisms that would safeguard the relevant fundamental rights.

Art. 4 provides certain caveats regarding trans-border data flows. It reads as follows:

1. Nothing in this Agreement shall require a Party to disclose:
   (a) information, the disclosure of which would be contrary to its law, including laws protecting privacy rights, or international agreements to which it is party;
   (b) confidential information, the disclosure of which would impede law enforcement or otherwise be contrary to the public interest; or

---

135 Ibidem
141 Ibidem

24
(c) confidential information, the disclosure of which would prejudice the legitimate commercial interests of particular enterprises, public or private

2. When a Party provides written information pursuant to the provisions of this Agreement, the Party receiving the information shall, subject to its law and practice, refrain from disclosing or using the information for a purpose other than that for which the information was provided, except with the prior consent of the Party providing the information.142

Although at the first sight this article may seem to be providing certain safeguards with regard to trans-border data flows, its deeper analysis raises particular concerns. The first part of the article says that ‘nothing <...> shall require to disclose <...>‘, however, the wording much more in favour of data protection would be ‘the parties <...> shall not disclose <...>‘.143 The second part raises even more concerns, because it speaks only about the obligations of a party to the agreement (i.e. a state) that is receiving particular information but not about a private entity that receives particular information. However, the information, according to this agreement, will usually be received by a right holder, i.e. a private entity, and, only in cases of criminal proceedings, it is most likely to be received by a state. Therefore, there are no particular safeguards in terms of data processing in cases when it is received by a private entity. Furthermore, even in cases when information is received by a state, party to the agreement, the prohibition to use it for different purposes than it was provided for is only valid in cases when there was no different consent of the Party that provided the information, and also ‘subject to law and practice’ of the receiving Party. That leaves the provision (Art. 4(2)) basically without any effect, because the receiving party may treat the information according to its own law. In fact, this provision may even deprive the Safe Harbor Agreement of its effect,144 in the sense that it is allowed to treat the information according to the laws of the receiving state and disregard the laws of the state from which the information is originating. Furthermore, several of the countries that have signed ACTA are so far not recognized as providing an adequate level of data protection under Directive 95/46/EC.145 Therefore, in case ACTA enters into force, it could be used as a way to circumvent the requirement of adequate data protection under the directive.

As a result, the overall picture of the ACTA regulation is truly worrying, because in principle, substantial monitoring is allowed, coordinated by non-judicial authorities. That is in contradiction with the main principles of data protection in the EU, such as the necessity and the proportionality of data processing, as well as the consent of the data subject.

Was ACTA to enter into force, it is not entirely clear whether the safeguards that exist at the moment in EU law would prevail nor whether they would remain in force. Although an opinion has been expressed that ‘Whatever ACTA says or suggests, it does not detract one iota from ISPs’ or right holders’ duties of compliance with these directives’, it could be also argued to the contrary. As noted above, Art. 11 enshrines an obligation to the parties to the agreement to provide for the specific regulation, which means that the EU would have to change the existing regulation in

---

142 Emphasis added
143 Ibidem
144 In cases when information is transferred from EU Member State to the USA
favour of the new regulatory regime. Furthermore, if it was acknowledged that EU secondary law is contrary to the international agreement that is in force, the provisions of the international agreement may, under certain circumstances, be invoked directly in the national courts of Member States. Another question that would arise in case of ACTA’s entry into force is of ACTA’s compatibility with the Treaties of the EU and the Charter of the Fundamental Rights of the EU. In case of incompatibility, the decision to conclude ACTA could be annulled by the Court of Justice of the European Union. The Commission, as mentioned, already has posed the question to the Court.

Many of the provisions in ACTA that are capable of infringing the EU acquis are formulated as non-binding clauses, and, according to some researchers, therefore they do not constitute legal obligations. However, a different opinion has also been expressed, namely, that there will be constant pressure from the lobbyists to interpret those provisions as mandatory. As Prof. M. Geist has noted in his speech before the European Parliament, it is already happening as the IIPA, a rights holder lobby group, has recommended placing ACTA countries such as Greece, Spain, Romania, Latvia, Switzerland, Canada, and Mexico on the USTR piracy watch list for failing to include optional ACTA provisions in their domestic laws.

Concerns about possible infringement of the fundamental right to privacy by the agreement have also been expressed by several members of the European Parliament during the debates concerning ACTA. It should be also noted that Art. 36 of the agreement foresees establishing the ACTA Committee which would have, among others, the power to ‘consider matters concerning the development of this Agreement’ (Art. 36 (2) b), and to ‘consider any other matter that may affect the implementation and operation of this Agreement’ (Art 36 (2) e). Furthermore, the Committee may decide to ‘make recommendations regarding the implementation and operation of this Agreement, including by endorsing best practice guidelines related thereto’ (Art. 36 (3) c) and to ‘take other actions in the exercise of its functions’ (Art. 36 (3) e). The vague wording of these provisions may be interpreted as granting wide powers to the Committee in practice, which, considering the strong lobby of the representatives of IPR owners, may result in a strict application of the provisions of the agreement to the detriment of the internet users’ privacy.

The European Commission has recently released a Synthesis of the comments on the Commission report on the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights (the IPRED directive), where the views of the respondents quite clearly diverge on the question whether the directive should be revised and IPR enforcement strengthened. Whereas the right holders of IPR

---

147 See, in this respect cases C-21-24/72 International Fruit Company v Produktschap voor Groenten en Fruit [1972] ECR 1219, in particular pars. 7, 8, 19, 20, the latter setting out the conditions for direct applicability – ‘the spirit, the general scheme and the terms of the General Agreement must be considered’

148 The ground for annulment of the decision to conclude the Treaty in this case could be infringement of the Treaties, arising from the substantive provisions of the agreement. Case C-122/95 Germany v Council [1989] ECR I-973, Paul Craig, Grainne de Burca. EU Law. Text, Cases and Materials (5th edn, Oxford University Press, 2011), 353


150 Ibidem


clearly spoke for stricter enforcement, ‘the overwhelming majority of individual citizens, consumer protection organisations and academics strongly argued against any further (over)regulation of IPR infringements <...>. Internet content filtering and traffic monitoring on the internet were perceived as threats to fundamental rights (freedom of speech, right to privacy) or even censorship and therefore clearly rejected.”¹⁵⁴

Hence it could be concluded that IPR enforcement at the expense of privacy of all internet users is to be considered negative overall. Civil society should be always consulted when deciding on international treaties and legislative measures. It is unacceptable that international agreements having a major impact on the internet users’ privacy are being negotiated secretly and the opinion of the civil society is not taken into account. The problem is enhanced by the fact that ACTA has been negotiated by the European Commission – an institution that was not directly elected by the European citizens. It is the view of the author that only by taking into account the interests of all the stakeholders and conducting an open discussion, can measures be enacted that would have a major impact on a fundamental human right. Furthermore, the enactment of such measure could be hardly justified when facing world-wide protests and criticism against it. Under the current above-described circumstances, one would hope that the principles of democracy will prevail and ACTA will be either rejected in the European Parliament, or strictly evaluated by the Court of Justice of the European Union.

4.2 SWIFT case

Although the SWIFT case is related both to e-commerce and public security issues in the context of data protection, the case may serve as a useful illustration of the problematic differences and interaction between the EU and the USA data protection regulatory schemes. Furthermore, it is very important in the field of e-commerce as in the SWIFT case the data collected by private parties in order to perform commercial transactions was used for law enforcement purposes. Therefore, privacy and data protection in the context of e-commerce is directly affected by this case and its aftermath. The case will hereby be shortly discussed revealing the most important problematic aspects and possible developments in the area of trans-border data flows and privacy, focussing on the context of e-commerce.

SWIFT¹⁵⁵ is a Belgian-based company which provides a service of financial messaging. Its clients are close to 10 000 various financial institutions from 209 countries.¹⁵⁶ It has two operational centres, one of which is located in Europe and the other one – in the USA¹⁵⁷.

The SWIFT case came into the public light in 2006 when the New York Times published an article revealing that SWIFT has been secretly providing access to the financial messaging data for the US Department of Treasury. The access had been provided after the US Department of Treasury issued subpoenas which were compulsory for SWIFT under the law of the USA.¹⁵⁸ After the publication of the matter, SWIFT has portrayed itself as a victim of the problematic interface of the EU and the USA data protection regulatory schemes.¹⁵⁹ Nevertheless, several European data protection authorities began investigations of the case that were later coordinated by the Article 29 Working Party. A very interesting point to note here is that the data protection authorities interpreted that allowing access to data for the U.S. Department of Treasury falls under the

¹⁵² Ibidem, 6
¹⁵³ The Society of Worldwide Interbank Financial Telecommunications
¹⁵⁶ Ibidem, 193
¹⁵⁷ Ibidem, 194
provisions of Data Protection Directive, even though in a relevant judgment in the PNR case, the ECJ has decided that the transfer of data for law enforcement purposes falls under the third pillar of the EU and therefore remains outside the scope of Data Protection Directive. The Belgian Data Privacy Commission, Article 29 Working Party and the European Data Protection Supervisor all came to the conclusion that SWIFT had not complied with the European Data Protection Directive. However, none of the institutions took any action against SWIFT. Apparently, the competent institution to act in this case was the Belgian Public Prosecutor; nonetheless he also decided not to take any action against SWIFT

An interesting action, undertaken by SWIFT after the data transferring had been disclosed, was signing up to the Safe Harbor Agreement. It is peculiar in two aspects. Firstly, as already mentioned, SWIFT is a Belgian-based company, therefore it is subject to European and Belgian data protection laws. As described in subchapter 4.1, the Safe Harbor Principles aim at ensuring that the US-based companies adhere to particular standards that are ‘adequate’ to the data protection provided for in the EU laws. Therefore, the very act of subscribing to the principles by a Belgian-based company is superfluous and does not change the legal situation, nor does it change the obligations that SWIFT is subject to under European and Belgian law. Furthermore, the Safe Harbor Principles themselves establish that ‘adherence to these Principles may be limited <...> to the extent necessary to meet national security, public interest, or law enforcement requirements’.

Subsequently, an ad-hoc agreement was negotiated between the EU and the USA. The European Parliament took a stand and did not ratify its initial version, however after some changes it was adopted in the European Parliament in 2010. The Agreement itself, even after the changes that were made due to the rejection by the European Parliament of the initial text, has some debatable aspects. Both the European Data Protection Supervisor and Article 29 Working Party have expressed the view that the agreement does not meet current European data protection standards.

The European Data Protection Supervisor has issued an opinion on the last draft of the agreement (already changed after the rejection in the European Parliament). Among the several criticisms expressed in the opinion, one of the main concerns is the possible incompatibility of the measures with the principle of necessity that is enshrined in Art. 8(2) of the European Convention of Human Rights. Some doubts were expressed as to whether the agreement will bring any added value for the purposes of law enforcement, having in mind the existing legal instruments that aim to stop the financing of terrorism.

161 Ibidem, 195
162 Ibidem, 195 – 197
163 Ibidem, p. 196
169 In particular, Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and Regulation (EC) 1781/2006 on information on the payer accompanying transfers
A very important aspect in terms of e-commerce is the problem of bulk data transferring according to the agreement. Even though the express provision on data transferring in bulk has been erased in the final version of the agreement, the lack of technical possibilities to filter data in the EU may result in transferring bulk data to the USA.\(^{170}\) That would be in contradiction to the necessity and proportionality principles enshrined in the European Data protection directive.

Another important aspect to notice is that the data transferred according to the agreement concerns not only private persons, but also legal persons. Some authors have expressed their concerns that ‘the bulk transfer of data opens the door to industrial espionage on European businesses’ financial transactions.’\(^{171}\) It could be added that the vast amounts of information about the transactions performed in the EU may provide the government of the USA with an oversight of virtually anything that is happening in the EU that involves any bank transfers. In the modern information society, such oversight grants an enormous competitive advantage to the USA.

There is no mechanism foreseen in the agreement that would ensure the control of data transfers by an independent judicial authority. Despite the concerns that were expressed after publishing the draft of the agreement,\(^{172}\) the control of data transfers remained in the hands of Europol,\(^{173}\) which, according to some scholars,\(^{174}\) has the interest of acquiring the information itself and therefore cannot serve as an independent assessor of data transferring legality.

The Article 29 Working Party has expressed its concerns regarding the judicial redress available to EU citizens under the agreement.\(^{175}\) In this respect the agreement contains two contradictory clauses. Art. 18(2) states that ‘all persons, regardless of nationality or country of residence, shall have available under U.S. law a process for seeking judicial redress from an adverse administrative action.’ However, Art. 20 (1) establishes that ‘this Agreement shall not create or confer any right or benefit on any person or entity, private or public.’ This latter clause seems to nullify not only the clause concerning judicial redress by the EU citizens, but also the other right-conferring provisions, such as Art. 15 (Right of access) and Art. 16 (Right of data rectification, erasure, or blocking). Furthermore, the fact that the European data protection authorities have basically no role to play in the mechanism of data transferring is also regrettable.\(^{176}\)
The report on implementation of the agreement
data flows between the EU and the USA. Firstly, it seems to be the area where infringements form
the law, rather than the law prevents infringements. Secondly, even the law that is tailored for trans-
border data flows under conditions that are highly debatable in terms of privacy protection
standards in the EU law, is being infringed again, followed-up by not more stringent sanctions than
‘recommendations’ by the Joint Europol Supervisory Body. The agreement that is tailored for
allowing almost unlimited access to financial transactions information in the EU, i.e. imposes clear
restrictions on the right to privacy, contains a clause which states that no additional rights are
conferred by the Agreement. Even though one should acknowledge that fighting terrorism is a truly
serious reason to impose certain restrictions on the right to privacy, however, even when data
collection is justified by this reason, there should be certain procedural safeguards in place, ensuring
that the main principles of privacy protection, such as restriction of privacy only when it is
necessary in a democratic society, are respected. Otherwise, we come to a situation where the
privacy of European citizens is protected only in the EU, but not elsewhere and the lack of
protection in the rest of the world is allowed by the EU itself. The problem grows deeper when one
analyzes the process of the conclusion of the agreement, and the way in which it was ‘pushed
forward’ by the European Commission, an institution that was not directly elected by the
European citizens. One could inevitably spot the similarity that exists between the European
Commission’s role played in the processes of concluding the SWIFT agreement and the ACTA
agreement. Unfortunately, the role played in both of the cases was not in favour of the right to
privacy of the European citizens and one can only wonder why.

Concerns about the SWIFT case have been raised not only by academics, but also by
some Members of the European Parliament, publicly discussing the possibility of bringing the

177 Report on the Inspection of Europol’s Implementation of the TFTP Agreement Conducted in November 2010 by the
178 Ibidem
179 EU-USA general agreement on data protection and the exchange of personal data (Statewatch Observatory)
accessed 22 April 2012
180 Ibidem
181 E.g. the Agreement was signed by the Council one day before the entry into force of the Lisbon Treaty, so as to
avoid the requirement of the European Parliament’s consent on the agreement. (As several countries withheld their
signatures, the approval by the European Parliament was still needed in the end.) Furthermore, referring the text of the
agreement to the European Parliament was deliberately delayed so as to fulfil the conditions for provisional application
of the agreement. Sylvia Kierkegaard, ‘US war on terror EU SWIFT(ly) signs blank cheque on EU data’ (2011) 27(5),
matter before the Court of Justice of the European Union.\textsuperscript{182} It is the author’s view that checking the compatibility of the agreement with the European human rights standards before the Court of Justice of the European Union would bring not only more certainty (considering the heavy criticism of the agreement) but would also redeem the reputation of the European Commission and the EU as such in terms of its capability of ensuring human rights protection in the legislative process. Furthermore, the mistreatment of private data, even by public authorities, once it has been provided in the course of e-commerce transactions, contributes to the atmosphere of distrust when using electronic communications to conclude contracts, which consequently inhibits the development of e-commerce. That is another serious reason to revise the agreement in light of the European human rights protection standards.

\textsuperscript{182} Valentina Pop, ‘Court only option against Swift agreement, says MEP’ (EUobserver, 17 March 2011) <http://euobserver.com/22/32010> accessed 22 April 2012
5. Certain aspects of e-commerce and privacy in the EU and the USA

5.1 RFID and the Internet of Things

RFID (Radio Frequency Identification) is a technology for automatically identifying objects and, possibly, subjects. An RFID chip can be as small as a grain of sand. It is usually attached to an antenna which has a form of a sticker, and is designed for wireless data transmission. The possible use of this technology includes areas like monitoring supply systems in retailers’ shelves, waste management, toll-payment transponders, banknotes, passports and human implantation. Most forms of its use raise privacy concerns. One of the main features distinguishing RFID from similar technologies (e.g. barcode) is that RFID can be used without line-of-sight contact and RFID readers can scan tags at rates of hundreds per second; furthermore RFID tags usually have unique codes that indicate the concrete item. This makes the technology very comfortable both to use and to misuse.

One of the foreseen developments of the RFID application is the Internet of Things – through the RFID tags attached to each object they would form a digital network which would reflect the characteristics and position of existing objects in a digital environment. The RFID tags could relate not only to subjects, but also to other objects, relations or values in a database. It is predicted that, by the year 2020, 50 to 100 billion devices will be connected to the Internet. However, considering not only all kinds of machines, but also other objects, ‘the potential arises to transfer all the objects would be connected and often controlled by electronic means, all the commerce could be called e-commerce’. Because it is suggested that all or most of the existing objects would be transferred in this way to the digital environment, an obvious problem of privacy arises. Whereas the access to objects and subjects in a physical world can be stopped by physical obstacles, in the digital world that may be much more complicated and a threat arises that anyone could digitally intrude the environment of any person, as long as that person is surrounded by RFID tagged objects.

However, it is not a black or white situation. There are various privacy enhancing technologies designed to protect the privacy of RFID end-users. They can be categorized into

---

184 Ibidem.
188 Ibidem.
191 Ibidem.
192 Ibidem.
following five categories: 1) deactivation of RFID (could be done both by software or physically, e.g. at the counter); 2) physical restriction of RFID reading; 3) function allowing readers to communicate directly with tags to control access to their content (only authorized RFID readers can be granted access to the RFID tag); 4) users delegating privacy management to a privacy agent (could take a form of a watchdog device that would inform users about reading processes or a form of a blocker tag – one that could block all RFID communication); 5) users personally authorize each read-out process.

Due to numerous different areas of its application, privacy in RFID is a wide topic, deserving separate research works focus. In this chapter, attention will be given to the comparative issues of legal protection of privacy in RFID development in the EU and the USA.

In both respective jurisdictions the issue has attracted the attention of the public and of the legislators as well. In the EU, the Commission has issued a recommendation directed towards Member States, aiming to provide guidance in first steps of regulating RFID. One of the most important provisions of the recommendation is point 4 which states that ‘Member States should ensure that industry, in collaboration with relevant civil society stakeholders, develops a framework for privacy and data protection impact assessments.’ The framework was drafted and endorsed by the Article 29 Data Protection Working Party in January 2011. According to the framework, there are two types of privacy impact assessments (full scale and small scale) depending on whether the RFID application is processing personal data, is linked to personal data or is likely to be carried by an individual.

Even though a privacy impact assessment of any RFID application is undoubtedly needed before its implementation, the current legal regulation of RFID in the EU could not be called satisfactory. Firstly, the above-mentioned framework for privacy impact assessment is drafted according to a recommendation and is endorsed by the Article 29 Data Protection Working Party. Therefore it is not mandatory for the entities that are willing to apply RFID. This is especially problematic considering that privacy is a fundamental human right and its protection should be guaranteed by the Member States. As a consequence, this choice of self-regulatory approach might not be totally suitable having in mind the often conflicting interests of industry and civil society. Here it should be noted that RFID applications are even more likely to infringe privacy than some of the other e-commerce areas, e.g. cookies on the internet (depending on the areas of their application, RFID chips could inform RFID scanner controllers about a set of personal information, such as various national registry numbers, personal possessions, health history, etc.). However, the soft-law approach by the EU and relatively inactive Member States leave the area to be regulated only by the basic laws of data protection in the EU which are not completely suitable in the area of this new technology. Therefore, an enhanced role of the EU and the Member States in securing privacy in RFID applications would be positive. However, Member States might be not willing to

194 Sarah Spiemer, Sergei Evdokimov ‘Critical RFID Privacy-Enhancing Technologies’ (March/April 2009)
197 Ibidem
200 This issue will be discussed in the following chapter.

33
regulate RFID because that would decrease the competitive advantage of the companies acting in that Member State (e.g. some privacy enhancing technologies would have to be implemented), therefore, it is important to regulate the issue on the level of the EU.

In the USA, although no legislation has been enacted at the federal level, there have been several States that passed laws regulating RFID.\textsuperscript{201} E.g., in 2008 Washington enacted a law that made it a criminal offense to scan an RFID device without the person’s prior knowledge and consent for the purpose of fraud, identity theft or any other illegal purpose.\textsuperscript{202} California has criminalized remotely reading someone’s RFID data on an identification document without that person’s knowledge or prior consent.\textsuperscript{203} Similar provisions have been enacted in Nevada, Vermont and Rhode Island.\textsuperscript{204}

When comparing the regulatory developments in the EU and the USA one might notice that laws in the USA are basically directed at prohibiting the misuse of RFID whereas in the EU laws are directed at guiding the use of RFID.

The application of RFID, despite its prospective advantages, in reality so far remains very narrow. E.g., in the EU in 2009 only 3\% of all the enterprises in all the Member States were using RFID and by 2011 that number increased to 4\%.\textsuperscript{205} It is the view of the author that, in order to facilitate the secure application of RFID, which could be acceptable to society, there have to be respective safeguards in the legislation which would ensure that the misuse of RFID is illegal and certain remedies could be turned to in such cases. These legislative safeguards, e.g. prohibiting unauthorised scanning of RFID, could facilitate the development of the related technologies, as society would trust them more. Consumers’ reluctance to purchase items that contain RFID tags can be illustrated by a public boycott campaign that was announced against Benetton (a clothing retailer) when news reached the public\textsuperscript{206} that Benetton was planning to embed RFID chips into clothing items.\textsuperscript{207} Consequently, Benetton has cancelled these plans.\textsuperscript{208}

However, one of the biggest American retail corporations - Wal-Mart - has gradually\textsuperscript{209} introduced RFID technology in their supply system, despite the public’s established privacy concerns.\textsuperscript{210} The intention was first announced in 2003,\textsuperscript{211} introducing tagging of merchandise

\begin{thebibliography}{99}
\bibitem{201} National Conference of State Legislatures, State Statutes Relating to Radio Frequency Identification (RFID) and Privacy (9 September 2010) \url{http://www.ncsl.org/issues-research/telecom/radio-frequency-identification-rfid-privacy-laws.aspx} accessed 8 April 2012
\bibitem{203} Ibidem, 192 – 193
\bibitem{204} National Conference of State Legislatures, State Statutes Relating to Radio Frequency Identification (RFID) and Privacy (9 September 2010) \url{http://www.ncsl.org/issues-research/telecom/radio-frequency-identification-rfid-privacy-laws.aspx} accessed 8 April 2012
\bibitem{206} Benetton to Tag 15 Million Items (\textit{RFID Journal}, 12 March 2003) \url{http://www.rfdjournal.com/article/articleprint/344/-1/-1/\%20} accessed 8 April 2012
\bibitem{207} Boycott Benetton campaign \url{http://www.boycottbeneton.com/} accessed 8 April 2012
\bibitem{208} Katherine Albrecht ‘Benetton has publicly retreated from plans to fit clothing with tiny remote surveillance and tracking chips’ (\textit{Boycott Benetton}, 9 April 2003) \url{http://www.boycottbeneton.com/PR_030407.html} accessed 8 April 2012
\end{thebibliography}
pallets, and in 2010, separate items started being tagged. Critics of the system point out that after the implementation of the system, retailers will be able to scan new types of personal ID cards and driving licenses (that contain RFID chips as well) and combine the information with the credit card data which would allow retailers to know the identity of the buyer the next time he enters the shop. Furthermore, critics contend that ‘unscrupulous marketers or criminals will be able to drive by consumers’ homes and scan their garbage to discover what they have recently bought.’ These concerns, although they may appear hypothetical at first sight, reveal the weak points of the unregulated application of RFID in everyday life. Whereas consumers may be able to boycott relatively small shops if they do not approve of RFID application, when it comes to retail ‘giants’, the lower price and other benefits that they offer may be much more difficult to boycott. This phenomenon demonstrates how the approach of self-regulation may, in the end, be harmful for the consumers because they may be willing to trade small amounts of privacy in exchange of particular benefits; however, this in turn would lead to other retailers following the same practice (e.g. due to effective competition in the area of supply management costs), which would cause all or most of the items bought anywhere to be marked with an RFID chip. Consequently, all the belongings of a person could be scanned by an RFID scanner not only when one is walking past the store, but also just by using the scanner near one’s home, because usually RFID chips can be tracked from a distance as well. This proves that RFID-specific legislation is needed in order to protect the privacy of the general public. Once it becomes a common practice to embed RFID chips into any item that is for sale, consumers will not have any real choice in the matter. That is why certain legislative safeguards are needed even before RFID chips are widely used.

After the analysis of recent legislative developments and practice in the area of RFID both in the EU and in the USA, it is the view of the author that it would be the most beneficial if the two legislative trends in respective jurisdictions would be combined. Firstly, it is important that unauthorized scanning of RFID chips would be prohibited in the EU, as it is now the case in some of the states in the USA. This way consumers could feel safer with regard to the possible scanning of their belongings both outside and inside their home. Certainly, it is also important to provide for technical possibilities to control scanning. One of these possibilities would be to employ RFID chips that make a sound each time they are scanned. This would enable one to know when one’s item has been scanned. Another, perhaps more effective technical solution, would be to employ an RFID chip that would lose its capability to be scanned from a distance once the transaction is performed (e.g. at the counter in a retail shop). However, the possibility to scan the chip from a short (e.g. couple of centimetres) distance could be retained, in order to provide the consumer with a possibility to return the good without a receipt or for use of warranty services. This approach is in principle now enshrined in the Privacy and Data Protection Impact Assessment Framework for RFID Applications. However, it should take a stricter legislative form, and impose more concrete obligations on RFID application operators.

The RFID Lighthouse project between the EU and the USA forges to ‘develop a joint framework for cooperation on identification and development of best practices for Radio Frequency Identification (RFID) technologies and develop a work plan to promote the interoperability of electronic health record systems’. This project has preceded the current Recommendation on RFID of the European Commission and has been followed-up by a number of...
research projects aiming to explore the possible use of RFID.\textsuperscript{216} Even though the extensive research on the topic is to be valued very positively, the suitability of current regulation in both respective jurisdictions is debatable. Whereas in the EU it takes the form of a recommendation, and is therefore not mandatory and cannot be controlled, in the USA the regulation is fragmented, prohibiting unauthorised scanning or prohibiting the requirement of RFID chip implantation, and is enacted only in few States. The current practice in the USA where one of the world’s biggest retailers started embedding RFID tags to the items that it sells is worrying, especially considering that it is much more difficult for consumers to boycott it because of the benefits that it can offer. From the European perspective, the fundamental human right to privacy should be protected by the state in this situation even before the RFID is applied. In the American jurisdiction, however, where privacy is often seen as a good in the context of e-commerce, the trade of privacy in exchange for particular economic benefits for the consumers is already happening. It is the view of the author that it is extremely important to reconcile these differences in the beginning of regulating RFID, because later, when RFID will become a common practice, it will be more difficult to change the existing legislation. Furthermore, some common standards will have to be found due to the intensive exchange of goods between the two markets.

5.2 Cookies

A web cookie (also called HTTP cookie) is a set of data that an internet browser receives upon visiting a particular webpage. On each subsequent visit of that webpage the browser sends that data to the website which allows the website to recognize the same visitor and may act in various ways, e.g. it may offer a customized web service.\textsuperscript{217} There is a variety of cookies with different functions (first-party cookies, third-party tracking cookies, authentication cookies, session cookies, etc.).\textsuperscript{218}

The fact that cookies often collect private information ‘without permission and without payment’\textsuperscript{219} has prompted legislative responses. In the EU the issue of users consent to cookies is regulated by Directive 2002/58/EC on privacy and electronic communications which was changed in 2009 by the directive Directive 2009/136/EC. In the original version of the directive it was established that the user has to be provided with information about how his data is used, furthermore a possibility to deny the cookie storing operation had to be provided.\textsuperscript{220} The novelty in the directive of 2009 is the requirement of explicit user’s consent for storing such data in user’s computer.

The practical enforceability of the foreseen standards has an important role to play in protecting privacy. However, there have been a number of problems in the implementation of the 2009 directive. Firstly, half of the Member States have not implemented the directive on time.\textsuperscript{221} Furthermore, the way they have implemented it differs significantly, and in a significant number of Member States, the requirement to obtain users’ consent to using cookies is interpreted as complied


\textsuperscript{218} Christopher Pettigrew, ‘EU Cookie Law & Sharepoint – What’s Affected?’ (Life in SharePoint, 10 May 2012)  <http://www.lifeinsharepoint.co.uk/2012/05/10/eu-cookie-law-sharepoint-affected/> accessed 11 May 2012


\textsuperscript{220} Art. 5 (3) of the directive

with if the browser settings of the user allow cookies. Secondly, one could doubt whether the national data protection authorities are in fact sufficiently active in providing guidelines and enforcing the standards foreseen in the legislation. After the deadline of the transposition of the directive 2009/136/EC (that is 25th May 2011) there have been numerous publications in the media, raising questions as to how the directive should be implemented. Furthermore, some of the data protection authorities have expressly stated that they will not enforce the directive until the technical solutions are found. Here it could be debated whether the aim of strengthening users rights is best achieved by enactment of an EU directive, albeit with such limited guidance offered by the European Commission. As mentioned above, a high number of Member States interpret the requirement of ‘explicit consent’ as inferable from the internet browser settings. In effect, the practical implementation of users’ rights does not change. It could be argued that the provision itself should have been clearer or the relevant legal instrument ensuring the right, should be a regulation rather than a directive. Furthermore, some guidance on what could be suitable implementation of the directive could have been provided by the European Commission. Thirdly, one could doubt whether there are always sufficient technical means at hand in order to detect the infringements. Quite often infringements are detected by specialists in the field that are not working as data protection authorities. In addition, even when such infringements are detected, often the final outcome is termination of the infringement rather than an actual sanction for the infringer. This practice may encourage infringements, because undertakings face low or no sanctions when infringing the relevant standards, at the same time being able to profit greatly from the infringements (e.g. sales of personal data for the purposes of direct advertising). Moreover, on-line businesses have an incentive to develop new technologies that would be more and more privacy-invasive, thereby gaining a competitive advantage in comparison to those undertakings that are complying with the standards. Indeed, in the times when personal data is so valuable that it is called ‘the new oil’, stricter measures should be taken (and enforced in practice) in order to protect the fundamental human right to privacy.

However, one should also take into account the threats of over-regulating cookies. Whereas privacy is a fundamental human right and is to be protected, it should be also taken into account that wide selection of services offered on the internet are free to the end-user due to other means by which service providers earn their profit. Therefore the subtle balance has to be struck here, taking into account both interests of the end users – protection of their privacy and development of on-line services. After enacting the directive 2009/136/EC, concerns have been

---

222 E.g., explicit user consent is required in Greece, France, Latvia, Lithuania, whereas in Bulgaria, Czech Republic, Denmark, Estonia, Finland, Luxembourg, Poland, Romania, Slovakia, Slovenia, Sweden users consent to cookies is understood as expressed through internet browser settings. Field Fisher Waterhouse. Cookie ‘consent’ rule: EU implementation (13 February 2012) <http://www.ffw.com/pdf/cookie-consent-tracking-table.pdf> accessed 29 April 2012
224 E.g. The UK Information Commissioners Office has announced it will not enforce the respective law for a year, until suitable technical solutions are found. Gerald Ferguson ‘Cookies Crumbling? - An Update’ (Data Privacy Monitor, 25 May 2011) <http://www.dataprivacymonitor.com/enforcement/cookies-crumbling----an-update/> accessed 29 April 2012
225 E.g. The situation was such when it was detected that MSN uses ‘supercookies’ that are able to recreate identifying information after users delete usual cookies. David Burt, ‘Update on the issue of ‘supercookies’ used on MSN’ (Microsoft Privacy & Safety, 18 August 2011) <http://blogs.technet.com/b/privacyimperative/archive/2011/08/19/update-on-the-issue-of-supercookies-used-on-msn.aspx?Redirected=true> accessed 30 April 2012
226 Ibidem
raised about the disadvantageous position that start-ups find themselves in. As a considerable amount of website controllers’ revenue depends on effective advertising capabilities, the requirement might result in an overall decrease of internet business revenue. Even though these concerns should not be exaggerated – websites are still free to advertise and gain profit there from – the advertisements are likely to be not as effective in cases when users do not give their consent to using cookies. However, it is important to minimize the impact of privacy protection measures on internet business profitability. It is the author’s view that the requirement of obtaining a user’s explicit consent should be limited only to those cases when private information is processed by using the cookie. If no personal information is processed by the use of cookies, there is in fact no harm on users’ privacy. E.g., if the cookie is only used to count the number of visitors in the website, there should be no consent required.

Interestingly, two years after the cookie-related changes have been enacted in the EU, a bill has been introduced in the U.S. Senate which would allow users to opt out of tracking on-line (Do-Not-Track Online Act of 2011). Even though the basic approach enshrined in the bill is much more similar to the EU directive of 2002 rather than to the changes introduced in 2009, the trend of protecting users’ privacy with regard to cookies by federal legislation is very positive. It reflects the basic trend of USA privacy laws raising the privacy protection standards in the context of e-commerce. If these proposals were enacted, the legislative framework on privacy protection in the USA would become more similar to the standards established in the EU. That would pave the way towards an international treaty establishing general obligatory data protection standards in both respective jurisdictions.

---


229 2011, S. 913
Conclusions

1. The historically different approach to privacy in the EU and the USA is reflected in the differing legal regulation. The self-regulatory approach in the USA expresses the understanding that privacy is a tradable good in the context of e-commerce. However, as is demonstrated by the analysis, in the relationship between consumers and undertakings having a dominant position, the latter are able to offer consumers particular benefits in exchange of which consumers are ready to provide private information. Even though in the short term this exchange may seem equivalent, in the long run, consumers give up more and more of their privacy, which allows the undertaking to strengthen its position and further acquire private data in an abusive manner. This illustrates a major deficiency of the self-regulatory approach in the context of e-commerce and consequently it may be concluded that legislative interference is needed in order to properly protect privacy in the context of e-commerce.

2. After the analysis of current legislation, case-law, recently proposed legislative developments and international treaties, it could be concluded that two contradictory tendencies exist in the area of e-commerce and privacy in the EU and the USA. First clear tendency that has received major public attention recently is the one of restricting on-line privacy in favour of intellectual property rights enforcement. This trend can be illustrated by SOPA and PIPA proposals in the USA and the ACTA agreement. All of these initiatives have now been halted due to the active resistance of civil society, which has manifested in wide-spread protests and petitions.

3. Second important tendency is the one of raising the standards of on-line privacy protection both in the EU and in the USA. This can be illustrated by the current data protection reform that is in process in the EU and several legislative proposals that aim to ensure privacy protection in the USA. The latter tendency could have the effect of USA privacy protection standards becoming more in alignment with the respective standards in the EU, which would have an overall positive impact as the e-market between the two economies would become more uniform.

4. When assessing the two tendencies together, one of which reduces privacy protection in the context of e-commerce and the other one increases, a question arises why the same legislators act in such contradictory manner. After the analysis of the relevant literature it should be observed that one of the main reasons of the privacy restricting tendency is the strong lobbying by the IPR holders’ industry. Another possible explanation considering the historical context may be that governments are willing to be more in control of the on-line content in order to prevent reoccurrence of such phenomena as the Wikileaks.

5. However, the unprecedented wide-spread resistance of civil society against restrictions of privacy and other fundamental rights clearly shows that the societies in both sides of the Atlantic are willing to protect their privacy on-line. That is a clear indication for the legislators that legislative developments should strengthen privacy protection and not diminish it.

6. With respect to SWIFT and Safe Harbor Agreements it could be concluded that the current legal situation regarding both of the agreements is not completely satisfactory. According
the deeply enrooted different approaches to privacy in the respective jurisdictions, it may be understandable that it is difficult to reach an agreement on detailed aspects of privacy protection in the context of e-commerce in the short term. However, it would be beneficial to both of the economies if in the long term common standards of privacy protection would be enshrined in an international treaty. Current legislative proposals in the USA that aim at raising privacy protection standards indicate that it could be feasible to conclude an international treaty establishing minimum standards of privacy protection that are not lower than the ones currently existing in the EU.
Bibliography

Statutory Material

2. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (28 January 1981), CETS 108
16. Opinion of the European Economic and Social Committee on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A Single Market for Intellectual Property Rights – Boosting creativity and innovation to provide economic growth, high quality jobs and first class products and services in Europe, COM(2011) 287 final (18 January 2012)

17. The USA Health Information and Portability Accountability Act, 1996, H.R. 3103
18. The USA Gramm-Leach-Bliley Act, 1999, S. 900
19. The USA Children’s Online Privacy Protection Act 1998, H.R. 4328
20. The USA Video Privacy Protection Act, 1988, S. 2361
21. The USA Fair Credit Reporting Act, 1970, S. 1114
22. The USA Stop Online Piracy Act, 2011, H.R. 3261
23. The USA Protect IP Act, 2011, S. 968
24. The USA Do-Not-Track Online Act 2011, S. 913
25. The USA Cyber Intelligence Sharing and Protection Act, 2011, H.R. 3523
26. The USA Do-Not-Track Online Act, 2011, S. 913

Books


Journal articles


Cases

47. Malone v. United Kingdom App no 8691/79 (ECHR, 2 August 1984)
48. K.U. v. Finland App no 2872/02 (ECHR, 2 December 2008)
50. Case C-465/00 Rechnungshof v Österreichischer Rundfunk and Others [2003] ECR I-04989
52. Cases C-21-24/72 International Fruit Company v Produktspach voor Groenten en Fruit [1972] ECR 1219

Web resources

60. ‘Romania has stopped ACTA ratification’ (FreePL, News from Poland, 24 February 2012) <http://freepl.info/1785-romania-has-stopped-acta-ratification> accessed 24 March 2012
65. Albrecht K ‘Benetton has publicly retreated from plans to fit clothing with tiny remote surveillance and tracking chips’ (Boycott Benetton, 9 April 2003) <http://www.boycottbenetton.com/PR_030407.html> accessed 8 April 2012
77. Commission Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A coherent framework for building

87. Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, C(2009) 3200 final

88. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, COM(97) 157 final

89. Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, COM(97) 157 final


91. Council of Europe, ‘Case Law of the European Court of Human Rights Concerning the Protection of Personal Data’ (March 2009)

92. Council of Europe, ‘Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Summary of the Treaty’

93. Council of Europe, ‘Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Explanatory Report’

94. Council of Europe, Committee of Ministers, ‘Explanatory Report’

95. Council of Europe, Treaty Office, ‘Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Status as of 13 May 2012’

96. Council of Europe, Treaty Office, Convention on Cybercrime, Status as of 15 April 2012


100. European Commission, ‘How will the EU’s reform adapt data protection rules to new technological developments?’


105. EU-USA general agreement on data protection and the exchange of personal data (Statewatch Observatory) <http://www.statewatch.org/Targeted-issues/EU-USA-dp-agreement/eu-usa-dp-info-exchange-agreement.htm> accessed 22 April 2012


133. Pop V, ‘Court only option against Swift agreement, says MEP’ (EUobserver, 17 March 2011) <http://euobserver.com/22/32010> accessed 22 April 2012


143. The Egmont Group of Financial Intelligence Units <http://www.egmontgroup.org/about> accessed 21 April 2012
