EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A
ECONOMIC AND SCIENTIFIC POLICY

Economic and Monetary Affairs

Employment and Social Affairs

Environment, Public Health and Food Safety

Industry, Research and Energy

Internal Market and Consumer Protection

Does it help or hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy

ITRE

EN

2011

Does it help or hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy

EUROPEAN PARLIAMENT

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A: ECONOMIC AND SCIENTIFIC POLICY

Does it help or hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy

STUDY

Abstract

This study investigates the interplay between Internet innovation and privacy. We propose working definitions of innovation and privacy and review the literature about their interaction. We interpret the possible tensions and problems in terms of market and system failures and analyse the relevant legal and policy aspects in relation to examples of privacy invasion and/or protection by innovating companies. Using a four issue framework we analyse relevant case studies such as cloud computing and online behavioural advertising. Following a gap analysis according to our model of failure, we present a series of recommendations aimed at different stakeholders. The study was based on desk research, key informant interviews, case studies and an interactive expert consultation held in Brussels in June 2011.

IP/A/ITRE/ST/2011-10 December 2011

PE 464.462 EN

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

AUTHOR(S) – in alphabetical order

Jonathan Cave, Neil Robinson, Rebecca Schindler (RAND Europe)
Gabriela Bodea, Linda Kool, Marc van Lieshout (TNO),
Quality Assurance review conducted by Scott Marcus (WIK-Consult) and Hans Graux (time.lex)

RESPONSIBLE ADMINISTRATOR

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

LINGUISTIC VERSIONS

Original: [EN]
Executive summary: [DE, FR]

ABOUT THE EDITOR

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

Manuscript completed in December 2011.

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

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS

ACLU	American Civil Liberties Union
AEPD	Agencia Española de Protección de Datos (Spanish Data Protection Authority)
AFIS	Automatic Fingerprint Identification System
Article 29 WP	Article 29 Working Party of the Data Protection Directive 95/46/EC
BEREC	Body of European Regulators for Electronic Communications
BEUC	The European Consumers Organisation
BT	British Telecommunications plc
CAGR	Compound Annual Growth Rate
Capex	Capital Expenditure
CEO	Chief Executive Officer
CNIL	Commission nationale de l'informatique et des libertés (National Committee on Individual Liberties – French data protection authority)
CPU	Central Processing Unit
DNT	Do Not Track
DPA	Data Protection Authority
DPI	Deep Packet Inspection
DRM	Digital Rights Management
Convention	European Convention on Human Rights (European Convention for the Protection of Human Rights and Fundamental Freedoms)
ECHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
ENISA	European Network and Information Security Agency
FIDIS	Future of Identity in the Digital Society research project
FRAND	Fair, Reasonable And Non-Discriminatory
FSA	Financial Services Agency
FTC	Federal Trade Commission
GPS	Global Positioning System
GSM	Global System for Mobiles
HTML5	Hyper Text Markup Language version 5
IaaS	Infrastructure as a Service
ICAO	International Civil Aviation Organisation
ICO	Information Commissioner's Office
IPR	Intellectual Property Rights
IPv6	Internet Protocol version 6
ISP	Internet Service Provider

ITRE	Committee on Industry, Research and Energy (European Parliament)
LBS	Location Based Services
NGO	Non-Governmental Organisation
OBA	Online Behavioural Advertising
OECD	Organisation for Economic Co-operation and Development
Opex	Operating Expenditure
P3P	Platform for Privacy Preferences
PaaS	Platform as a Service
PbD	Privacy by Design
PETs	Privacy Enhancing Technologies
PGP	Pretty Good Privacy
PIA	Privacy Impact Assessment
RFID	Radio Frequency Identification
SaaS	Software as a Service
TFEU	Treaty on the Functioning of the EU
US-VISIT	United States Visitor and Immigrant Status Indicator Technology
W3C	World Wide Web Consortium

LIST OF TABLES

LIST OF FIGURES

EXECUTIVE SUMMARY

What is the challenge?

There are many indications that today's 'Information Society' is still very much in its formative stage, but at the same time is already evolving towards a more complex and richer stage: the 'Data Society'. Unprecedented developments and unforeseen consequences flow from all facets of information and communication technologies to infrastructure, products, business processes and the societal practices constructed on the platform of these technologies. These in turn illuminate fascinating new perspectives that would have scarcely have been imaginable just a few years ago. The rapid rise of mobile platforms and smart phones provides one example of a more general convergence of previously separated telephony and data transport infrastructures that, just a few years after their implementation, have become ubiquitous among businessmen and youngsters alike, providing pervasive contact independent of time and location. Digitisation enables linking of all kinds of services, creating an ecosystem of interrelated Internet activities within which novel industrial and business arrangements arise and contend for survival. In particular, this evolutionary struggle has transformed the new position of the 'user' as the central focus of business models and – potentially at least – the king of the road. At the same time on the supply side, new and innovative (networks of) firms have emerged to challenge the dominance of old media and communication conglomerates.

A further development has possibly an even more profound impact upon the organisation of today's society. Formerly-dominant centralised systems that collect personal data increasingly coexist with an extremely fragmented and decentralised fabric of differentiated systems and entities that collect, aggregate, integrate, process, exchange and communicate personal data. The massive coverage and dense interweaving of this fabric makes it very hard for individuals to trace and to control the circulation and use of 'their' data, even if they want to. Some parts of this new landscape are themselves large, complicated and difficult for individuals to control effectively. The 'tipping tendencies' of social networking, e-commerce and some aspects of cloud computing drive the creation of large platforms that effectively centralise data from a host of users. This centralisation of personal information in the data centres of commercial giants such as Facebook and Google contributes to the increasing opacity of data activities. Networks and software tools capture – and combine - personal data without the subjects' clear consent or knowledge. People are sometimes confronted with personal data of which they were absolutely unaware in situations that may be highly undesirable. The fluid nature of the Internet (in particular the easy migration of data, but also the fluidity of organisations) makes control over one's own data very difficult if not impossible.

In a few instances, public dissent on particular data collection practices has led to high-profile court cases. The activities of some large players, notably Facebook and Google, have been affected by rulings of European and national courts; in a number of cases, this has produced clear improvements via the introduction of new technologies and services that obey stricter privacy regimes than their predecessors.

These developments have enriched the lives of European citizens, improved the efficiency and effectiveness of public organisations, and led to interesting new opportunities for economic growth. There are also less-desirable effects including unprecedented intrusions into the private lives of European citizens. On a more positive note, there are examples of innovative technology and business practices that enhance the privacy of European citizens. This ambivalence is hardly surprising; innovations are made and exploited in response to stakeholder interests; privacy-invasive innovations arise from the growing (often economic) value of personal information, and privacy-enhancing innovations reflect the growing awareness of and value attached to the privacy or control of such data.

In light of these developments, together with the on-going revision of the regulatory framework on privacy and data protection, it is timely that the European Parliament Committee of Industry, Research and Energy (ITRE) has requested a study on the relationship between Internet innovation and privacy.

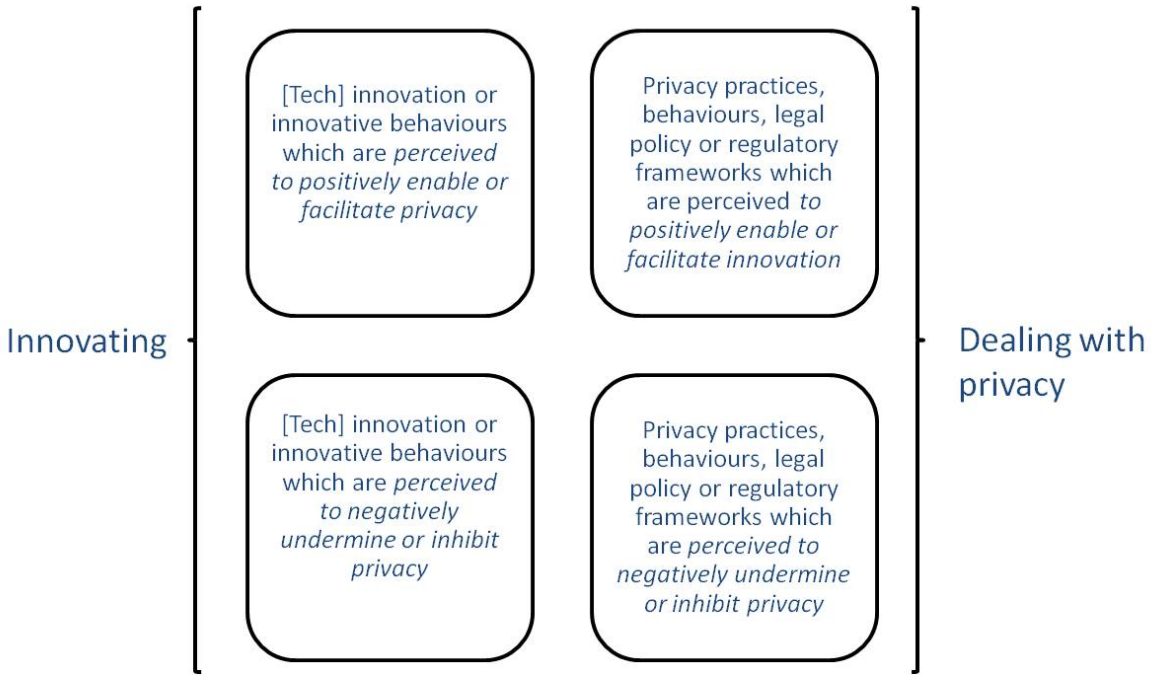
What approach has been taken?

The European Parliament requested a study on the relationship between Internet innovation and privacy that would identify the tensions and synergies and suggest approaches addressing the tensions and exploiting the synergies.

Internet innovation is a multi-layered phenomenon in which technological development, business processes, user behaviour and institutional changes all contribute to innovation (i.e. bringing something new in the market/people's daily life). Privacy is also a complex multi-dimensional phenomenon. This study adopts a broad interpretation of privacy along dimensions such as: the right to be let alone; the need for intimacy and secrecy; control over personal information; respect for individuality; and the dignity and autonomy of individual persons. With respect to the regulatory framework, we accepted the strong focus on the informational dimension of privacy ('data protection'), but noted the growing importance of other aspects such as spatial (a subjective sense of a private space free from observation), relational (freedom to interact with others and to generate 'mutual' private information – belonging to both parties, rather than to one or another), corporeal (the integrity of the body) privacy and privacy of action (meaning that the individual has the ability to perform certain actions that are deemed personal and private without the intervention of the government or other parties). We further note the increasing tendency for them to be subsumed within the informational dimension.

The relation between Internet innovation and privacy has been framed rather straightforwardly. We constructed a matrix in which the mutual influence of privacy and Internet innovation can be assessed (Figure 1). Internet innovation may be benign or may have detrimental impacts upon privacy; conversely, privacy (requirements and attitudes) may accelerate, hinder, improve or distort Internet innovation. There are clear examples of each quadrant of the resulting map:

Figure 1: Twofold relationship between privacy and Internet innovation



Internet innovation that enables or facilitates privacy can be found in the privacy-friendly social networks such as Diaspora, or privacy-friendly search engines such as IxQuick.

A more general example is provided by privacy enhancing technologies; unfortunately – and for a variety of reasons - such developments are as yet niche market products that enjoy only limited uptake.

The positive influence of privacy on Internet innovation in the top-right quadrant is exemplified by the activities of the Google Data Liberation Front that aims at providing data portability, and games seeking to increase privacy awareness such as Zynga's PrivacyVille and (for young children) Disney's Surfs Swell Island. Another interesting example is the UK attempt to facilitate switching between providers of Internet-related services (financial, utility and telecom services) which operates under a self-regulatory regime and allows users to express their preferences (willingness-to-pay) for privacy and other service characteristics, for example by choosing to pay more for services with greater built-in privacy safeguards.

The lower left quadrant of the matrix identifies the Internet innovations that impair or restrict privacy. Examples include: the Facebook Beacon service, which exposed private transactions and purchases and which was withdrawn in the face of fierce opposition); Google's Street View (in particular lack of effective data subject control), which led to court cases in countries such as Germany, Switzerland and the UK; novel 'cookie' practices such as the flash cookie and the everlasting cookie (a cookie that restores itself after having being deleted); and the use of Deep Packet Inspection (DPI) by Internet Service Providers (ISPs) to identify specific sorts of content (e.g. spam) – thus protection of email from unwanted commercial intrusion involves revealing to the ISP the contents of all mails.[1]

The bottom-right quadrant refers to the restricting influence of privacy on Internet innovation. Services mentioned above (e.g. Street View, Beacon) can be seen as examples of innovative technologies and business processes that arose at least in part to exploit private information in ways not directly controlled by existing protections. Such innovations will then lead to 'stranded investments' if successfully resisted (Beacon had to be abandoned and Street View had to be adapted to include opt-out schemes and face-blurring technologies), perhaps after some intervening period during which privacy is seriously compromised. Where the controls are effective, innovation takes a different trajectory than might otherwise be the case; for instance, Online Behavioural Advertising (OBA) is restricted in its use of collected personal data by requirements imposed by regulatory regimes such as the EU Data Protection Directive. Such influences on the course of innovation may be viewed as 'negative' if they also foreclose alternative solutions that might lead to improved business outcomes benefitting all parties (i.e. both service providers/sellers and consumers/customers) in ways not encompassed within the existing legal framework.

[1] DPI has often been used to detect spam (see e.g. http://www.cuartopoder.es/mecanicamente/las-operadoras-principales-enemigos-de-internet/978 - Accessed 12 September 2011). The Dutch telecom provider KPN admitted to investors in May 2011 using DPI to monitor mobile phone users' use of applications, triggering an investigation by the Netherlands' Ministry of Economic Affairs (see http://www.circleid.com/posts/dutch_isps_admit_to_using_deep_packet_inspection Accessed 12 September 2011). Another example of inadvertent or unexpected compromise is provided by the widely-available Whatsapp application(which allows users to exchange messages without paying SMS charges), but which apparently exposes usernames, phone numbers and text messages to outside scrutiny (see e.g. http://www.pcmweb.nl/nieuws/internet/miljard-whatsapp-berichten-dag - Accessed 12 September 2011)

How were the lessons of experience incorporated?

To study the relationship between Internet innovation and privacy, the legal and regulatory framework was analysed to identify essential elements and interesting yet not fully explored emerging issues, such as 'the right to be forgotten', the focus on transparency and consent and the implementation of privacy by design. Concrete empirical cases[2] were studied to increase our understanding of the current tensions:

- Radio Frequency Identification (RFID)
- Online Behavioural Advertising (OBA)
- Biometrics
- Location Based Services (LBS)
- Cloud computing

Desk research and additional interviews were used to create an empirical 'evidence base' to expose the interplay among the four 'corners' of our analytical matrix. Since Internet innovation is itself multifaceted we differentiated four dimensions: technology innovation processes; business processes and practices; user behaviour; and legal and regulatory regimes.

What are the conclusions of the study?

The (empirical) analyses of the regulatory framework and the five cases led to the conclusions in Table 1. The interested reader is referred Chapter 5 of the Report.

[2] Another case, DPI, is briefly discussed on page 42.

Table 1: Conclusions for the study Internet innovation and privacy

	Generic conclusions on privacy and Internet innovation
1	Negative implications of innovation on privacy outweigh positive ones
2	Privacy is a negative rather than a positive concern for innovation practices
	Conclusions on emerging technologies
3	Convergence of different Internet technologies with other technologies leads to greater privacy problems
4	Privacy-friendly technologies are under development but are not recognized as leading the way
	Conclusions on business practices
5	New business practices orient towards realizing as much profit from data as possible; privacy only offers a secondary incentive
6	It is difficult to develop new business practices focusing on implementing privacy-friendly solutions which are cost-efficient and profitable
	Conclusions on user behaviour
7	Awareness on the side of users for potential privacy infringements due to Internet innovation is low
8	Not much effort is invested in offering user-friendly and privacy-friendly systems
	Conclusions on legal and regulatory issues
9	Safeguarding privacy interests requires policy intervention
10	Self-regulation is sometimes used but is not easily achieved

The overall conclusion based upon the cases and other illustrative examples considered in this study indicate that the dominant tendency is for Internet innovation practices to increase tensions with safeguarding privacy.

The statement 'Personal data is the new oil' (or perhaps 'the new currency') underscores the current importance of personal data creation and use in new services and products. Two extensions complicate the relationship between Internet innovation and privacy:

The first is the highly fragmented and scattered nature of personal data production, collection, storage, processing, upgrading, enrichment, selection and distribution over a large variety of platforms and services. Users are – often unconsciously - one of the richest sources of new personal data.

The second is the expansion of the 'traditional' approach to data collection to include spatial and geographical data and even corporeal data (genetic information, disease related information, etc.). This is particularly salient in relation to the 'Internet of Things' and the convergence of information and communication technologies with biotechnologies (genetic profiling) and nanotechnologies (very small sensors and chips).

Public awareness of privacy intrusions is generally low and/or dominated by isolated and unrepresentative incidents. Long term risks are difficult to reconcile with short term advantage, especially in relation to complex concepts such as privacy. Combining this difficulty in comprehending privacy risks and benefits with limited and/or overly-complicated controls (themselves difficult to understand or evaluate), one should question whether individuals should bear full responsibility for e.g. managing the privacy implications of new technologies and business practices.

Privacy is a right in itself, but tensions arise in exercising this right in today's complex world where it needs to be balanced with profits, competitive advantages for business practices and other societal rights, interests and entitlements. This recognition of the effective limitations of informed consent and end-user control might lead to alternative approaches.

From the perspective of business practices, we conclude that policy intervention is necessary to ensure adequate privacy protection. Business incentives point too much in the direction of using personal data as an input to business processes, thereby automatically creating new or enforcing existing threats to individual privacy. Self-regulation thus far has not fully met the challenge, though examples such as the emergence of privacy-aware social networks and the success of public campaigns in compelling changes in Facebook policies show it is not entirely impossible as well.

What are the main recommendations of the study?

The rich material we found on the subject clearly indicates its relevance for policy makers, business sectors and the public at large. Though recommendations on the basis of our findings could be formulated for each of the involved parties, we have restricted ourselves to those recommendations that might be particularly interesting for the policy making community. The following Table presents our main recommendations, the stakeholders for whom they are most relevant, the aspects of the framework to which they relate and the supporting conclusions. Again, the interested reader is referred to the study to get the full picture and argumentation concerning these recommendations.

Table 2: Recommendations for the study Internet innovation and privacy

Recommendation / relevant level	Stakeholders					Framework level				Conclusion (see Table 1)									
	Global	European	Member State	Private Sector	Individuals	Legislation	Business practices	Emerging tech.	User behaviour	1	2	3	4	5	6	7	8	9	10
Privacy rights and responsibilities																			
1. Differentiate economic and fundamental privacy rights	✓	✓				✓				✓	✓			✓		✓			
2. Distinguish graduated privacy rights at the individual and small group level of identification.		✓	✓			✓				✓		✓		✓	✓				✓
3. Extend protections to privacy of action		✓	✓			✓				✓		✓						✓	
4. Clarify consent provisions (esp. regarding technical means for informing and obtaining consent).		✓	✓			✓	✓		✓		✓	✓	✓		✓	✓			
5. Explore means of pushing privacy responsibility up the stack and down the value chain		✓	✓	✓		✓	✓		✓		✓	✓	✓	✓	✓	✓	✓		
6. Incorporate realistic behavioural assumptions		✓		✓	✓	✓			✓							✓	✓	✓	✓
Rules and regulations																			
7. Take full account of other formal and informal privacy regimes	✓	✓	✓	✓		✓	✓	✓										✓	✓
8. Reconcile privacy rules with antitrust, consumer protection, intellectual property and other rules addressing market failure.		✓	✓			✓												✓	✓
9. Take the medium-term coevolution of innovation and privacy into account in Impact Assessment of innovation and privacy policies.		✓	✓		✓	✓				✓	✓	✓		✓				✓	
Coping with change																			
10. Adopt value-based approach that is neutral with respect to technology, business models, services, etc.	✓	✓				✓		✓				✓	✓					✓	✓
11. Implement a 'policy sandbox' for collaborative exploration of new policies.				✓	✓	✓		✓										✓	✓
12. Undertake additional translational and policy-related research.	✓	✓	✓				✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

A relevant issue to be thought through in the light of the on-going revision of the EU Data Protection Directive is the manner in which the economic value of personal data should be balanced in the portfolio of rights and obligations of individuals and organisations.[3]

The argument is based on the tendency for the increasing economic value of private information and the fundamental nature of privacy rights to combine in ways that neither optimise the benefits of using these data nor effectively protect individual privacy from infringing business practices. Introducing this aspect facilitates discussion of increasing individual control over their data via negotiated terms and conditions for releasing data to third parties and the rights of consent and choice. This is a delicate matter that requires intensive deliberation but current practices for using personal data and the resulting tensions between Internet innovation and privacy require that the issue be addressed.

This should be further extended to incorporate a broader conception of privacy in which a more fine-grained approach to privacy (both for individuals and small groups) should be combined with an extension of data privacy towards (at least) privacy of action.

Privacy by design and related concepts might offer a way to move privacy responsibility up and down the stack of involved parties (companies, governments, individuals) in concert with appropriate regulatory protections.

Privacy impact assessments and other instruments could be used to offer better risk assessment and understanding of potential and likely consequences, focusing upon medium and long-term risks that are likely to differ from short term risks and benefits.

This could contribute to restoring the balance in perspective concerning privacy risks and possibly conflicting business or societal practices and to produce more 'future-proof' and 'technologically neutral' approaches.

If the lack of measures for safeguarding privacy is perceived as a form of market failure, a clear basis for analysis and possible intervention is created that allows privacy policy to be integrated synergistically with consumer protection, intellectual property, antitrust and other policies.

We also recommend changes in the fundamental policy approach towards Internet innovation and privacy. This challenging recommendation includes a value-based approach to privacy policy that is neutral with respect to emerging technologies and business practices and that develops and refines policy formulation and implementation via a policy 'sandbox' intended to provide accurate and generalisable insights into likely developments and challenges through experimentation in a kind of living lab setting.

3 This issue surfaces in e.g. – The statement by Commissioner Reding (Reding 2011a) on the EP vote on the Voss Report, the recent Public consultation on personal data breach notifications under ePrivacy Directive (European Commission 2011), The European Data Protection Supervisor's opinion on net neutrality (European Data Protection Supervisor 2011), the recent ITRE resolution and November EP Plenary vote on the net neutrality resolution (BEREC 2011) and the CEO Roundtable (CEO Roundtable 2011). However, these citations do not directly emphasise the main idea of the current document - that due to the growing economic value of personally identifiable information, the absence of a well-defined and practicable economic property right (e.g. personal information as intellectual property) can lead to situations in which the human right is unenforceable and widely violated while the economic value is neither optimised nor equitably distributed.

A further recommendation is to improve our understanding of the economic and societal dimensions of privacy in a globalising world governed by powerful stakeholders with different frames of reference (sometimes more stringent towards safeguarding privacy, sometimes more open). Effective evidence-based policy requires mutual understanding on a conceptual level enriched with relevant, reliable and understandable empirical evidence. This in turn requires further research.

One area where further knowledge is needed is the interplay between the benefits and limitations of user empowerment, transparency, consent and control; another is the extent to which inappropriate and unrealistic rationality assumptions can be improved by insights from behavioural science. Others can be added; a selection is identified in the study itself.

1. INTRODUCTION

KEY ISSUES

- Innovation on the Internet offers a wide range of opportunities as well as threats to citizens' rights to privacy, and vice versa.
- Four main dimensions (technological, business, consumer/citizen, regulatory/policy) shape relations and determine impacts.
- How does it play out in practice? What shapes relations and what determines impacts? Which impacts are more likely? Which ones are potentially more beneficial, which ones more harmful? And, what are potential solutions for the problems identified?

The European Parliament's Committee on Industry, Research and Energy (ITRE) has requested a study on the promotion of innovation on the Internet and citizens' rights to privacy with the aim to seek independent advice from experts to inform the Committee on priority measures and actions in these fields.

A study on this relationship is considered to be highly relevant, given the very high pace of change in the technological basis of new Information and Communication Technologies (for instance the rapid rise of mobile devices that offer a multitude of new services), the corresponding business context (for instance the very rapid rise of social networks and actors that deliver services on top of these networks) and the evolving role of users (much more involved in the creation of new services and much more central in product and service development processes). Also, the changing landscape on privacy regulation, which is prominently visible in the current revision of the data protection directive (95/46/EC) underscores the relevance of this study.

This analytical study seeks to provide background on the debate. It investigates the two-way interaction between the promotion of innovation on the Internet and citizens' rights to privacy: its current shape, implications and likely future development.

The study distinguishes three, related, research tasks:

1. summarize EU privacy safeguards applicable to network operators and those providing services over the Internet and their relation to other regulations
2. review current and likely tensions in the EU between the Internet and related technologies and the right to privacy, including a presentation of current privacy intrusive practices; and
3. discuss ways to promote further Internet-based innovation and competition in the EU while respecting citizens' rights to privacy, for example by way of privacy-by-design.

This brief introduction outlines the research behind this report, and presents the overall structure of the report.

1.1. The research behind this study

The research behind this study uses a two-sided approach to investigate the relation between Internet innovation and privacy:

- *From the perspective of innovation*: the positive and negative impacts of innovation upon privacy; and
- *From the perspective of privacy*: the positive and negative impacts of privacy rights and concerns upon innovation.

These impacts are differentiated along four main dimensions: technological, business, consumer/citizen, and regulatory/policy. Each dimension emphasises different aspects of the relationship between privacy and Internet-based innovation; combining the different perspectives and weighing them in order to capture the most relevant ones delivers input for legislative intervention. The study introduces working definitions of Internet innovation and privacy, and starts from an assessment of the regulatory environment in Europe. It proceeds to a more concrete and case-based examination of this relationship, leading to a model for assessing new developments. Several empirical cases are used to illustrate the four different relations.

To enrich and validate the cases, we interviewed experts and stakeholder representatives to shed light on the relationships between innovation and privacy and to reflect upon issues of relevance for the final part of the study. The cases were also presented and interactively explored in a one-day expert consultation meeting. The resulting feedback was used to validate, enrich and improve the interpretation of the case studies.

Input from the interviews helped to categorise problems and potential solutions. The expert consultation meeting facilitated discussion of potential solutions to the problems identified. Project partners also explored these issues in other external workshops to extend the 'reach' of the study and to test the findings for robustness against different framings (e.g. in relation to the societal and economic impacts of the Future Internet).

The report of this study presents main findings on potential solutions for the problems identified, and casts these findings in a number of recommendations to the Parliament. Given the exploratory status of this study the recommendations should be seen as starting point for further policy actions which might need guidance by building up additional evidence on impact of the proposed policy actions.

The consultation phase led to interesting perspectives and has made possible a strengthening of the problem identification and potential solutions. Nonetheless, the results of the study are the sole responsibility of the project team.

1.2. Structure of this report

Chapter 2 provides background on the research that was conducted throughout the course of the study: it clarifies key terms and frameworks. It presents operational meanings of Internet innovation and of privacy used in the present study and summarises the legal and regulatory environment.

Chapter 3 discusses current and future tensions: it includes an analysis of stakeholders, common practices seen to protect and/or abuse privacy.

Chapter 4 presents research evidence and actual examples of practices. Case studies include cloud computing, online behavioural advertising (OBA), location-based services (LBS), Radio Frequency Identification (RFID) and biometric technologies. Chapter 5 provides conclusions and recommendations.

2. BACKGROUND

KEY FINDINGS

- Internet innovation is conceived as a multi-layered phenomenon in which innovation not only relates to new and emerging technologies but also to new and emerging business practices, new and emerging aspects of user behaviour and attitudes and new and emerging institutional (legal and regulatory) issues.
- Privacy is likewise conceived as relating to multiple facets considered relevant for individuals. These relate to the right to be let alone, intimacy, control over personal data, and respect for individuality, integrity and autonomy.
- The relation between Internet innovation and privacy is twofold: Internet innovation can be benign or detrimental to privacy, while safeguarding privacy can have positive or negative implications for Internet innovation practices. This forms the kernel of the conceptual frame used.
- The current focus on the informational dimension of privacy ('data protection') is broadened to include spatial and geographical dimensions and bodily dimensions (such as genetic profiling).
- The current revisions of the regulations on privacy (especially the European Data Protection Directive under revision) show new issues becoming more relevant, such as the right to be forgotten, transparency and control and privacy by design.
- This comes together with heightened attention for strengthening individual rights, enhancing the market dimension, revising data protection rules in the area of policy and juridical co-operation, clarification and simplification of the rules for international data transfers and a stronger institutional arrangement for better enforcement of data protection rules.
- Several examples can be provided that highlight tensions between Internet innovation and regulatory approaches to safeguarding privacy.

This Chapter provides some general background on privacy and Internet innovation and describes the conceptual framework governing our investigation and analysis. It introduces working definitions of Internet innovation and privacy (and how privacy differs from data protection), and lays out the policy context and socio-economic environment.

The Chapter concludes by considering the current legal framework – primarily at EU level, but with some reference to interesting and relevant Member State developments.

2.1. Working definitions of Internet innovation and privacy

2.1.1. Internet innovation

Innovation means introducing something new. It does not necessarily need to be something technologically new and may equally well refer to a new business process, a new legal framework or a new service. The concept of innovation thus is a multifaceted phenomenon that is not easily captured in a single slogan.

In the scientific literature one can find several 'definitions' of innovation that emphasize different aspects of how innovation should be understood.[4] It would be outside the remit of this study to delve too deep into the constituent elements of innovation processes.

In this study we will take the concept of innovation in its full breadth, thus entailing innovation of technology, of business processes, of institutional contexts. These processes are mutually interlinked, creating a complex and cyclical system in which feed-forward and feed-back loops connect the different 'spheres' of innovation with each other.[5]

The study will focus on Internet-based innovation: the Internet itself has evolved over the years and escapes an unambiguous definition. Basically, the Internet refers to the network of computer networks that connects devices by means of a shared protocol (the TCP/IP protocol). The Internet facilitates the exchange of data between any two devices connected to each other through this network of networks. Internet innovation then refers to all innovation processes (technological, organisational, etc.) that exploit this capacity of exchange and communication over the underlying infrastructure. These innovative practices refer to changes in the technological infrastructure (introducing broadband capacity, glass fibre instead of existing copper-based infrastructure, new protocols that enable higher throughput of data), changes in services such as reliability and vitality of the infrastructure through new standards (such as IPv6 instead of IPv4) and changes in the regulatory framework that regulate the use of Internet (for instance safeguarding the privacy of users).

The rationale for innovation will crucially depend on the actors involved, their objectives, goals and ambitions and their perspective on what is needed and what opportunities/challenges are at stake. These rationales no doubt are very different along the range of stakeholders: engineers and technicians focus on improving technical features, the business community focuses on developing new and challenging services, and policy makers focus on what is the - positive - impact on society and on what is needed for properly functioning infrastructure and services. They will cross each other's domains in that each domain posits constraints on other domains, thereby contributing to the construction of a so-called ecosystem of actors that are 'glued' together in this innovation system.

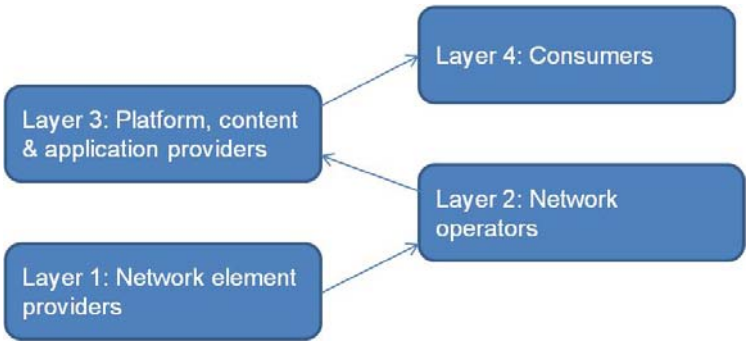
In adopting this ecosystem this study follows the value chain approach of Fransman (2010) who focuses on the ecology of buyer-vendor relationships. Though the layers are presented hierarchically (e.g. consumers on top of content, platforms and application providers) in reality linkages among layers go both ways. End-users may both consume and supply content and applications. Companies may be active in more than one layer. Actors in different (combinations of) layers and actors with different horizontal reach may innovate in different ways and be more or less sensitive to privacy and other aspects not directly captured in their business or scientific models (i.e. part of the negative linkage comes from the remoteness of innovators from privacy subjects). Privacy problems will show up in all layers.

4 See OECD (2005) (Oslo Manual) for an interesting overview of the various aspects of innovation and references to the scientific literature.

5 The cyclical model of innovation, as developed by Berkhout (2007) shows the many linkages within innovation systems.

The most prominent issues will be visible at the upper layers (especially layer 3 and 4) though network operators and even networked element providers (such as RFID suppliers) are confronted with privacy issues as well (for instance when fulfilling data retention obligations) and may therefore be motivated to develop innovative solutions.[6]

Figure 2: Internet value chain as depicted by Fransman (2010)



The value chain shown in Figure 2 details the functionality of each layer in the Internet ecosystem. Layer 1 captures network element providers such as Cisco, Samsung and others. Network operators are positioned in layer 2 (network operators), while Internet service providers are positioned in layer 3. The remainder of the study uses this view of the Internet ecosystem.

2.1.2. Privacy

The challenges in defining privacy are widely acknowledged despite its recognition as a fundamental human right in the 1948 UN Universal Declaration of Human Rights, the European Convention of Human Rights (1950) and most recently in Article 7 of the Charter of Fundamental Rights of the European Union (2000). Despite this, philosophers, legal scholars and others have argued that "nobody seems to have a clear idea what [privacy] is".[7] It is a double edged sword – individuals' 'fundamental right to privacy' is not considered to be absolute, and can thus be restricted under certain circumstances.

Although the privacy debate is not novel it has intensified since the 1960s and the widespread popularity of the computer and more latterly the Internet, which seem to threaten (especially) informational privacy and data protection.[8]

---

[6] Although nationality is not directly related to innovation, we note in passing that actors in the various layers are not exclusively European. All layers show a mixture of European and non-European actors. Layer 3 is dominated by a number of large US-based firms who - in principle - comply with European regulations (via the principles underlying the US-EU Safe Harbor agreement accepted in 2000). However, self-certified compliance may be imperfect and adherence may come after innovation, rather than being built in from the outset. Some of the largest innovative firms offering ICT-based services originate from the USA (Google, Facebook); Europe has few if any no ISPs in the top tier as measured by market capitalisation. Moreover, US innovation culture is different from that of the EU (the US has a far better record in converting R&D to market deployment, particularly as regards service and business model innovation, not least because the US environment encourages risk-taking and does not punish failure as harshly). Therefore, a greater proportion of the influential innovations come from a setting operating under very different privacy and data protection regimes.

[7] Thomson (1975).

[8] E.g. Daily Telegraph (2010).

Current thinking identifies a number of distinct framings of privacy. Solove[9] posits six 'traditional' approaches (each with their flaws and advantages in terms of their scope):

- The right to be let alone – Brandeis' argument – later elaborated by Justice Warren - raised concerns starting from the popularity of snap camera photography invented by Kodak Eastman in 1884. Their concern was that the media use of such technology would add to sensationalist reporting. They argued that the right to privacy revolved around a right to 'peace of mind' or 'relief' afforded by the right to prevent the widespread publication of photographs in the media.

- Limited access to the self – recognition of concealment and limited access to others.

- Secrecy – According to Richard Posner, "the right to conceal discredited facts about himself" – "to manipulate the world around them by selective disclosure of facts about themselves" can be regarded as privacy.

- Control over personal information – possibly the most popular (and perhaps the easiest to understand) approach to characterising privacy, the notion of control of personal information (personal data in the European context) forms the bedrock of much of the regulatory architecture flowing from international instruments and norms such as Article 8 of the Convention and Article 16 of Treaty on the Functioning of the European Union (TFEU) and the landmark European Data Protection Directive 95/46/EC.

- Personhood – advanced as a theory of privacy that where our identity or self-definition is at stake, the state may not intervene. Solove distinguishes two varieties of 'personhood': individuality, dignity and autonomy (respect for 'choosing' persons) and an anti-totalitarian construction (a right not to be too constrained by creeping state intrusion).

- Intimacy – an increasingly popular theory, this understanding of privacy is focused on the value that it provides in the functioning of human relationships, attempting to define "…what aspects of life we should be able to restrict access to or what information we should be able to control or keep secret."

In a transnational context it is important to understand that the terminology used to define privacy and related phenomena differs between common law and civil law traditions. Warren and Brandeis (1890) effectively defined a 'right to privacy' as a 'right to be let alone', which equates in continental Europe to the right of personality. Privacy is the superior principle from which other concepts derive, such as the US notion of 'informational privacy' (1960-70, see Cohen 2000) which corresponds to the European concept of 'informational self-determination'.[10] Data protection is intended to secure this; it was mainly developed in continental Europe around 1970 and quickly made its way to US and Great Britain.

[9] Solove op. cit. p 14. The 'right to privacy' was first articulated in response to information technology developments (photography and sensationalist 'yellow journalism' by US Supreme Court justice Louis Brandeis and Samuel Warren in Warren and Brandeis (1890).

[10] Bäumler *et al*. (1999) cite the census ruling of the German Federal Constitutional Court in 1983.

Much EU law currently broadly understood as concerning privacy (e.g. the Data Protection Directive 95/46/EC) focuses specifically on the protection of personal data ('data protection'). There are several reasons for this; examples include: 1) the relative ease by which challenges to a conceptualisation of privacy as control of personal information may be addressed; 2) the complexities of legally addressing other aspects of privacy in a consistent and comprehensive manner (e.g. the right to be let alone, secrecy or intimacy) in view of the legal, cultural and societal differences across a disparate community of some 500 million citizens; and 3) the institutional scope and boundaries of European policy making which until recently segregated policy making into realms relating to the Community, common security and foreign policy and police and judicial co-operation in criminal matters.

Nonetheless, like the focus of creative IPR on copying (copyright), this restriction (i.e. the focus of data protection) may also be seen as a reflection of a technological and organisational environment that has changed greatly since its inception; in particular, the embedding of information exchanges into a far greater range of personal interactions is seen by some as evidence that other privacy issues must be addressed when considering 'mere' data. In particular, the Internet constitutes a new form of (semi) public space, so privacy rights may need explicitly to be balanced against reasonable expectations and other rights such as the right to self-expression.

In this study we will use the concept of privacy in its various framings as presented above. The close relationship between privacy and personal data protection will be addressed where appropriate.

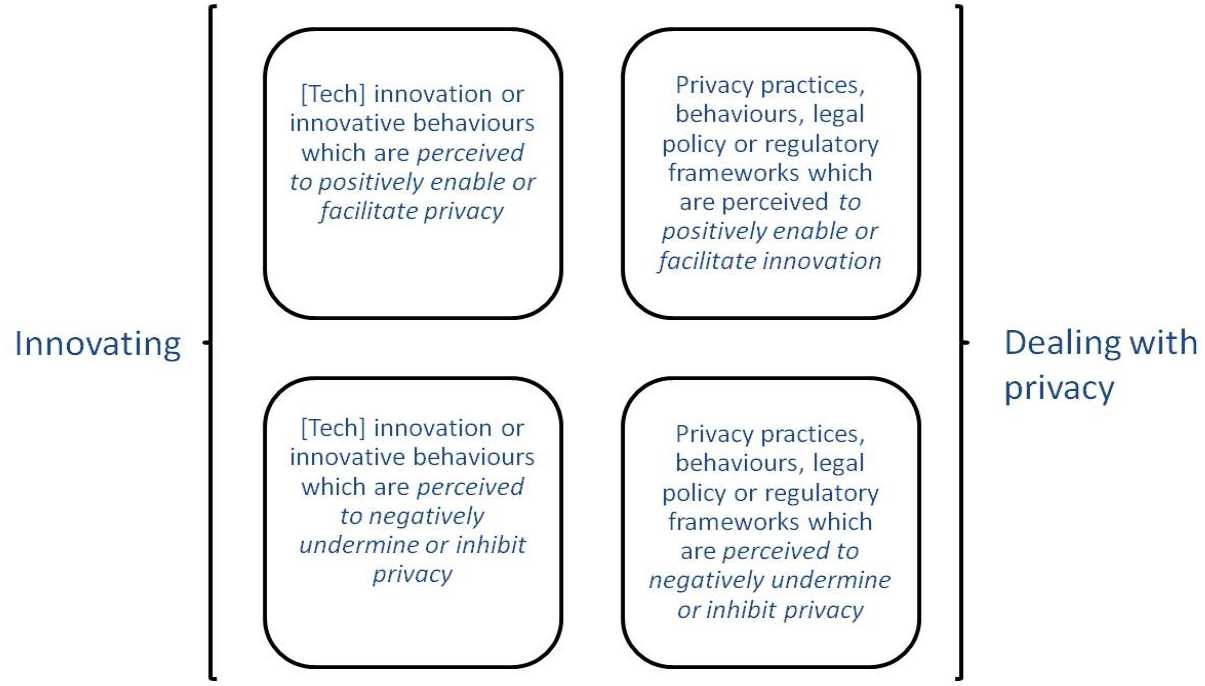
From concepts to framework

This Section reconciles the concepts of Internet innovation and privacy so that an in-depth study into the relationship between the two becomes empirically possible.

To start with, we already mentioned the two-way relationship between privacy and Internet innovation. We have interpreted the request of the European Parliament to study the relationship between privacy and Internet innovation as a request to study whether and if so how, privacy influences Internet innovation, whether and if so, how Internet innovation influences privacy and how to reconcile the results of both investigations. The influence of A on B can be either positive or negative. This is part of what needs to be unravelled.

This leads to the scheme as sketched in Figure 3. On the left side of the figure, the influence of innovation on privacy is presented. On the upper half one finds the positive influence, at the lower half one finds the negative influence. Similarly, the influence of privacy on Internet innovation is addressed in the right side of the picture, again with at the upper half a manifestation of the positive influence and at the lower half the negative influence. This figure is for illustrative purposes only. During the study we will bear this differentiation in mind and address it where appropriate.

Figure 3: Relationship between (Internet) innovation and privacy



The four quadrants of the matrix identify the different elements of the relationship between Internet innovation and privacy:

1. Innovation may positively enable or facilitate privacy - examples include various Privacy Enhancing Technologies, the use of blind authentication technologies and privacy friendly search engines (which shield users' identities);

2. Privacy practices may positively enable or facilitate innovation - examples include privacy by design practices using new service concepts (privacy icons, privacy impact assessments), decentralised biometric systems (which decouple identification from authentication) and face blurring technologies used to de-identify people.

3. Innovation may undermine or inhibit privacy practices – examples include DPI, new cloud computing service concepts that exchange personal data and OBA based on gathering data on personal search strategies.

4. Privacy practices may undermine or inhibit innovation - examples include regulations that prohibit collection of personal data sets which form the kernel of specific services and service strategies such as opt-in which may prevent easy targeting of customers.

Our analysis distinguishes four dimensions: legislation/policy, technology, business practices and user behaviour. Each of these relate to distinct features of the Internet innovation process (and its relation to privacy). By doing so, we will enrich our understanding of the dynamics between Internet innovation and privacy from separate yet mutually enforcing perspectives.

We will explore a number of case studies in which the relationship between Internet innovation and privacy is made visible. These case studies are chosen such that they cover the various elements of the value chain as depicted by Fransman (see Figure 2).

The case studies have been explored using the four dimensions we just described. Table 3 hereunder presents in a matrix the approach used in our case studies. For each of the four dimensions we will explore whether and if so, how, the relationship between Internet innovation and privacy can be demonstrated in each of the case studies.

Table 3: Overview of the empirical approach

Area	Innovation (practices)		Privacy (practices)	
	Positively associated with privacy	Negatively associated with privacy	Positively associated with innovation	Negatively associated with innovation
Emerging technology/research				
Business models/practices				
Behaviours/perceptions				
Legislation/policy				

The time frame used to identify innovative practices concentrated on innovative practices visible today or those that experts consider to be part of tomorrow's experience. Therefore, we did not take into account emerging technologies that may have severe privacy implications but that have not yet matured into business practices. An example is provided by the developing convergence of nanotechnologies, biotechnologies, new materials and cognitive sciences with information and communication technologies. This is likely to have severe impacts on privacy in the future[11] but is not included in this report, except insofar as its effects are already visible in the cases studied.

2.2. Main elements of current regulations applying directly to those in the Internet economy

This Section provides an overview of European level legislation and rules likely to be germane to the subsequent discussion on innovation and privacy. These rules stem from the European legal framework governing privacy and data protection including the General Data Protection Directive, the e-Privacy Directive and the Data Retention Directive. Some reference is also made to relevant EU Member State developments.

[11] Roco and Bainbridge (2003).

2.2.1. Directive 95/46/EC[12] - the General Data Protection Directive

The basis of the European legal framework regarding privacy and data protection, laid down in the General Data Protection Directive, is designed to protect personal data whilst at the same time encouraging the free flow of personal data within the Internal Market. The European regulatory regime created by this Directive begins from the perspective that the protection of personal data is a fundamental human right, a position reinforced by the latest interpretation of the right to personal data protection in the TFEU (Art 16). Article 8 of the Charter of Fundamental Rights of the Union, refers to the right to protection of personal data (again looking at privacy from the perspective of control over information) which anchor many if not all relevant legal norms in Europe. Article 16 of the TFEU replaces the TEC Provision on Data Protection in the First Pillar, describing the right to data protection, namely that:

> "Everyone has the right to the protection of personal data concerning them"

This means in practice that the legal framework starts from a general prohibition of the processing of personal data unless specific conditions are met. These include conditions relating to: consent; transparency (that data subjects are aware of the sort of data being processed and the purposes); that the processing is for specific, explicit and legitimate purposes, proportionate to the uses (e.g. adequate, relevant and not excessive) and that the data subject has certain recourse to remedies.

This regime is based around a number of globally accepted privacy principles, common across many jurisdictions, which have been shown to be, in philosophical and ethical terms, broadly comparable.[13] These include the Council of Europe Convention No. 108 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

These principles or goals include: legitimacy (Art. 7 of the Data Protection Directive 95/46/EC); purpose restriction[14] (implying data quality) (Art. 6 Data Protection Directive 95/46/EC); confidentiality and security (Art. 16-17 Data Protection Directive 95/46/EC); transparency (Art. 10 and 11 of Data Protection Directive 95/46/EC); data subject participation (Art. 12 of Data Protection Directive 95/46/EC) and finally accountability (Art. 22-23 of Data Protection Directive 95/46/EC).

There are various 'front' and 'back-end' measures which the Data Protection Directive sets up to meet these principles. This includes identifying just what exactly constitutes personal data; the use of consent; the definition of entities involved (e.g. data controllers, data processors and data subjects) and provision of mechanisms for accountability (e.g. that data controllers may be subject to independent scrutiny and that sanctions may be levied for a breach of the rules). The provision of privacy policies (as a means to establish clear and unambiguous consent) is another well known aspect of this regime, as are the rules for registration of data controllers and the prior notification of data processing activities by the data controller to public registers. The rules for transborder flows of personal data are also very well known.

---

[12] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[13] Robinson, Valeri, Cave *et al.* (2010).

[14] Personal data of an insufficient quality will inevitably be unsuitable for the purposes intended by the data controller; therefore data quality is an implied condition of the purpose restriction.

These rules state that personal data may only be transferred outside the EU if the receiving party is subject to a legal framework (either through laws, voluntary frameworks or binding contracts) that offers an 'adequate' level of protection.

Towards the end of the first decade of the 21st century, an increasing momentum was seen regarding whether an updating of this legal framework would be necessary, given a range of issues: the increasing use of personal data by public and private sectors and individuals; the apparent changes in cultural sensitivities regarding exhibitionism and access to information and of course the ubiquity of technology, particularly the Internet.

To inventory existing perspectives on this issue more clearly, a Consultation was organised by the European Commission in July 2009 on the legal framework for the fundamental right to protection of personal data, in particular in the light of new technologies and globalisation. As indicated by the then Commissioner Designate Reding, over 160 responses were received.[15] One of the responses to the consultation came from the Article 29 Working Party and the Working Party on Police and Justice, via their joint opinion WP168 (entitled 'The Future of Privacy - Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data').[16] This Opinion may be considered as important for the authoritative perspective it affords of the view of the future of the European set of regulations governing privacy and data protection by those who must oversee its implementation at the national level. In its contribution, the Working Parties stressed that they considered the European principles of data protection to still be valid, but that they recognised that

> "(t)he level of data protection in the EU can benefit from a better application of the existing data protection principles in practice. This does not mean that no legislative change is needed. To the contrary, it is useful to use the opportunity in order to:
>
> - Clarify the application of some key rules and principles of data protection (such as consent and transparency).
> - Improve the framework by introducing additional principles (such as 'privacy by design' and 'accountability').
> - Strengthen the effectiveness of the system by modernising arrangements in Directive 95/46/EC (e.g. by limiting bureaucratic burdens).
> - Include the fundamental principles of data protection into one comprehensive legal framework, which also applies to police and judicial cooperation in criminal matters."

Thus, from the perspective of the Working Parties, an optimisation/recasting of the Data Protection Directive appeared to be a viable option, in which its scope would also be expanded to cover former Third Pillar issues (presently partially covered by the Framework Decision 2008/977/JHA).

[15] http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/16&format=HTML&aged=0&language=EN&guiLanguage=en (visited 12 September 2011).
[16] Article 29 Working Party (2009).

At the beginning of 2011, the EU's Commissioner for Justice and Fundamental Rights and Citizenship, Mrs Viviane Reding, speaking at a meeting of the European Privacy Platform, indicated in broad terms the direction that the review of the current legal framework was taking.[17] This included the view that citizen's rights would need to be based on four pillars:

- "The first is the 'right to be forgotten': a comprehensive set of existing and new rules to better cope with privacy risks online. When modernising the legislation, I want to explicitly clarify that people shall have the right – and not only the 'possibility' – to withdraw their consent to data processing. The burden of proof should be on data controllers – those who process your personal data. They must prove that they need to keep the data rather than individuals having to prove that collecting their data is not necessary.

- The second pillar is 'transparency'. It is a fundamental condition for exercising control over personal data and for building trust in the Internet. [...]

- The third pillar is 'privacy by default'. Privacy settings often require considerable operational effort in order to be put in place. Such settings are not a reliable indication of consumers' consent. This needs to be changed.

- The fourth principle is 'protection regardless of data location'. It means that homogeneous privacy standards for European citizens should apply independently of the area of the world in which their data is being processed. They should apply whatever the geographical location of the service provider and whatever technical means used to provide the service. There should be no exceptions for third countries' service providers controlling our citizens' data. Any company operating in the EU market or any online product that is targeted at EU consumers must comply with EU rules."

The forthcoming legislative proposals[18] would thus likely cover the extension of general data protection rules to the police and judicial co-operation in criminal matters (ex-Third Pillar), the enforcement of data protection rules and reinforcing the independence and harmonisation of the powers of data protection agencies across the Member States.

[17] Reding (2011).

[18] According to the EU's Commissioner for Justice, Fundamental Rights and Citizenship, in a meeting with the German Justice Minister the new legislative proposal will be tabled in January 2012.

2.2.2. Revised EU telecom regulatory framework 2009

The revised EU telecom regulatory framework consists of a total of five different EU Directives[19] and an additional new regulation establishing the Body of European Regulators for Electronic Communications (BEREC). The most relevant parts of this framework for the purposes of this study are those aspects of the Citizens Rights Directive 2009/136/EC that amend the e-Privacy Directive 2002/58/EC.

The e-Privacy Directive is targeted at operators of public communication networks. It is designed to "particularise and complement" the General Data Protection Directive.[20]

With respect to data protection in the telecommunications sector (also a former First Pillar initiative), policy discussions have already resulted in an amendment of the e-Privacy Directive. Through this amendment, mandatory data breach notifications have become a part of European telecommunications law, and rules with respect to spamming and cookies have been strengthened. Principles which already exist such as accountability and privacy by design have thus already been reaffirmed and expanded in this regulatory framework, which may well be considered a glimpse into possible future changes of the Data Protection Directive. Transposition of the revised e-Privacy Directive was required by May 2011.

Article 4 of the ePrivacy Directive establishes measures for the security of processing building upon those already described in the General Data Protection Directive, namely that personal data should only be accessed by authorised personnel for legally authorised purposes, that stored or transmitted personal data should be protected against accidental or unlawful destruction, accidental loss or alteration and unauthorised or unlawful storage processing access or disclosure. Those entities covered by the revised e-Privacy Directive are required to ensure the implementation of a security policy with respect to the processing of personal data. Perhaps more interestingly, this article also empowers relevant national authorities to "audit the measures taken by providers of publicly available electronic communications services and issue recommendations about best practices concerning the level of security which those measures should achieve."

Article 4 (3-5) of the revised e-Privacy Directive 2002/58/EC also establishes a system for personal data breach notification. This set up a mechanism obliging providers of public e-communications networks to notify the personal data breach to the competent authority (regulator) without delay. In addition, a notification to their customers of the breach is required as well, if the breach is likely to adversely affect the personal data or privacy of a subscriber or individual.

---

[19] Namely:
- Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (Framework Directive) as amended by Directive 2009/140/EC (Better Regulation Directive);
- Directive 2002/20/EC on the authorisation of electronic communications networks and services (Authorisation Directive) as amended by Directive 2009/140/EC;
- Directive 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive) as amended by Directive 2009/140/EC;
- Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive) as amended by Directive 2009/136/EC (Citizens' Rights Directive); and
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive) as amended by Directive 2009/136/EC.

[20] Gadzheva (2008).

The rules say that notification shall not be required if the provider has satisfactorily demonstrated to the competent national authority that appropriate technological protection measures have been implemented to the data relevant to the breach and that these measures render the data unintelligible to anyone not authorised to access it.

Further rules give authority to the regulator to oblige the provider to notify, if it has not already done so, to lay down the format and content of the messages to be provided to the subscribers (e.g. the notification must describe the nature of the personal data breach) and to recommend measures that the subscriber could take. Notifications to the competent authority must also include any internal measures that the provider had taken. Other aspects include the establishment of guidelines by the competent national authorities concerning the criteria for issuing breaches, the format of notifications and the manner in which such notifications must be made ("the circumstances, format and procedures"), as well as making provisions for audits and imposition of sanctions. Verification of compliance may be performed on the basis of an inventory of breaches that the providers are required to maintain.

This revision of the e-Privacy Directive clarifies the rules of consent governing the placement of cookies on end-user equipment (Article 5 (3)). The amendment strengthens the rules for consent - clarifying the existing rule that the user must give consent only after having been provided with "clear and comprehensive information" – in the hope that this state of affairs might finally be improved through the possibilities of stronger enforcement provided for in the new wording. The exception is whether the cookie is absolutely necessary for the provision of a service that has been requested by a user or information storage is for the sole purpose of carrying out an online communication. It arguably tightens the previous requirement through the use of the word 'consent' instead of 'refuse'; with the amended Directive, Article 5 (3) states that the storing or accessing of information on the computer is only permitted if the user has given his or her "consent, having been provided with clear and comprehensive information" thereby making the placement of cookies based on opt in. These rules apply to entities storing information or getting access to info on users terminal equipment (for example, websites using cookies to facilitate third party advertising and also those analytics that record number of visitors to a website). This clarification in particular has received some considerable opposition from industry, who claim that it means that Internet users will be confronted with a wealth of pop-up boxes requiring their consent, which will ultimately be counter-productive since it will have the effect of de-sensitising consumers to the content and overall purpose of such messages.[21] The European Data Protection Supervisor noted that concerns over multiple dialog boxes seeking prior consent was industry spreading panic and said that the requirements could be met by e.g. browser settings under suitable conditions.[22]

[21] Goldfarb and Tucker (2011).

[22] Outlaw.com Commission advice on cookies is ambiguous, data protection watchdog says http://www.out-law.com/page-12081 (visited 12 September 2011).

Article 6 of the 2002/58/EC e-Privacy Directive establishes various rules on the processing of traffic data, chiefly that: requirements that it be erased when no longer needed (Article 6(1)); processing is permissible in order to perform subscriber billing and interconnection payments (Article 6(2)); traffic data may be processed for marketing and provision of value added services (Article 6(3)); that information on the types of traffic data being processed and the duration must be provided to subscribers or users (Article 6(4)) and that the processing of traffic data in accordance with Article 6 can only be undertaken by persons acting under the authority of the provider of the public communication network and publicly available electronic communications services handling "billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service".

Via Article 2(7) of the Citizens' Rights Directive, the existing rules on spam (unsolicited commercial electronic communications) in Article 13 of the earlier e-Privacy Directive 2002/58/EC were amended by prohibiting the practice of sending electronic mail for the purposes of direct marketing that disguises or conceals the identity of the sender and does not permit the recipient to respond and request the cessation of such communications. It also prohibits communications which encourage recipients to visit websites contravening Article 6 of the e-Commerce Directive 2000/31/EC (requirements for transparency of commercial communications).

Member States had until May 25th as the deadline for transposition.[23] The Article 29 WP undertook a review of the implementation of the data breach notification regime in April 2011.[24]

2.2.3. Directive 2006/24/EC[25] (Data Retention Directive)

Again within the telecommunications sector, the Data Retention Directive 2006/24/EC introduced an obligation incumbent on providers of publicly available electronic communications services or of public communication networks to store certain communications data: electronic communication traffic and location data; information on subscribers and registered users but not the content of communications. Political momentum for the bringing into force of a means to harmonise the Member States retention of traffic data for the purposes of fighting serious crime, such as terrorism, stems from the terrorist attacks in London and Madrid in 2005 and 2004. The Directive to a certain extent relates to the possibility of the restriction of the scope and obligations defined by the Data Protection Directive, if the processing is a necessary measure to safeguard national security and law enforcement as provided for in Article 13(1) of the Data Protection Directive and Article 15 (1) of the e-Privacy Directive: for safeguarding national security, defence, public security and for preventing, investigating, detecting and prosecuting criminal offenses or the unauthorised use of electronic communications systems. Thus, the architecture of protections provided for in these Directives may legitimately be abrogated to a certain extent if they are necessary for crime fighting, national security and defence.

---

[23] For more information see Data Breach Notification in the EU: ENISA (2011); for a legal analysis see e.g.: Barcelo and Traung (2010).

[24] Article 29 Working Party (2011a).

[25] Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

In order that the Member States did not undertake such restrictions of scope and obligations in a haphazard manner thus undermining the internal market, the Data Retention Directive was established to harmonise Member States approaches.

The Data Retention Directive sets out mechanisms for the length of time these kinds of communications data must be retained by providers: for a minimum of six and a maximum of 24 months.[26] It also contains basic provisions on security but does not specify anything related to the potential recovery of costs incurred by operators in connection with data retention.

Finally, the rules for cross border transfer leave to Member States to define the procedures and conditions to be met for competent authorities to gain access to the retained data.

This Directive is an interesting example of the need for cross-pillar instruments: while formally a first pillar instrument (data retention harmonisation as a way of avoiding market distortions through diverging national obligations), it is clear that this Directive has clear consequences for (notably) former third pillar issues, given that stored data can only be used 'for the purpose of the investigation, detection and prosecution of serious crime'. This lead to the somewhat illogical situation that data for criminal investigations had to be retained as an internal market measure, before the Framework Decision governing the exchange of such information for criminal investigative purposes had been adopted.

Commissioner Reding in a recent speech remarked on how the Data Retention Directive stands at odds with the provisions for the protection of personal data contained in other legal frameworks.[27] She indicated that although the Data Retention Directive contains measures for the storage of personal data for certain specific purposes, it should still be undertaken according to principles common across the remainder of the body of EU law, specifically it should be proportional, not kept for longer than necessary, kept secure.

2.2.4. A comprehensive approach on personal data protection in the European Union: Communication of the European Commission (2010)609

In recognition of the increasingly complex nature of the European legal basis governing privacy and personal data protection and also noting the opportunity afforded by the Lisbon Treaty (in regard to changes in the process of law-making between the different EU institutions) in late 2010 the European Commission released its Communication on "A comprehensive approach on personal data protection in the European Union" (COM (2010)609). This Communication represented the latest thinking of the European Commission in respect of a possible new legal framework for privacy and data protection, resulting from public consultations held and the input of the Article 29 Working Party and the Working Party on Police and Justice on the Future of Privacy.[28]

---

[26] In the USA a recent memo by the US Justice Department (published October 2011) indicates retention procedures for the major US mobile phone providers (such as T-Mobile, Verizon, AT&T and Sprint). Retention policies for different items (IP session data, text message details, text message data, IP destination information, call detail records) vary considerably among the mobile phone providers, reason for Senator Patrick Leahy to start pleading for harmonization measures. See http://arstechnica.com/tech-policy/news/2011/09/secret-memo-reveals-which-telecoms-store-your-data-the-longest.ars (visited 3 November 2011).

[27] Reding (2011).

[28] Article 29 Working Party (2009).

This was based around a number of key objectives (given also the renewed focus on individual rights in Jose Manuel Barroso's Commission in January 2010):

- **Strengthening Individual Rights** – including reaffirming the fundamental right, increasing transparency of processing, consent, awareness raising mechanisms and making remedies and sanctions more effective;

- **Enhancing the Internal Market dimension** – covering the achievement of further harmonisation of data protection rules at EU level, different possibilities for simplification and harmonisation of notification system, clarification of applicable law, enhancing data controllers responsibility and the encouragement of self-regulatory and EU certification schemes;

- **Revising the data protection rules in the area of police and judicial co-operation in criminal matters –** consideration of the general application of general data protection rules and providing for certain limitations and exploring the need for specific and harmonised provisions;

- **The global dimension** – clarification and simplification of the rules for international data transfers and promotion of universal principles – maintaining the European regime as a 'gold standard' for protection of personal data by fostering enhanced co-operation;

- **A stronger institutional arrangement for better enforcement of data protection rules** – measures to strengthen, harmonise the status and powers of national Data Protection Authorities and improve co-operation and collaboration.

2.2.5. Privacy regulations and innovation

Following the summary of relevant legal frameworks provided in Section 2.3, we now turn to outlining the basis of how the aforementioned privacy regulations may touch upon innovation of the kind outlined earlier in this report.

In respect of the implications for technological innovation, we can see that the **'front end' aspects of the regulatory regime**[29] **are perhaps most germane**. We provide an indicative summary of some of the most pertinent examples below.[30] That is not to discount some of the other proposed recommendations: for example, there may be avenues for technological innovation for the possibilities to allow the automatic verification of data subjects preferences with regard to how their personal data might be used against lists of registered controllers held by a supervisory authority. Similarly, the exploration of a mandate that data controllers must appoint a Chief Privacy Officer might well be viewed as counterproductive for innovation, hindering technical innovation to protect privacy since it places a focus upon organisational structures rather than opportunities where technology might play a role.

[29] i.e. those of the legal framework which are realised via direct interaction with the data subject for example by permitting the data subject to exercise his or her rights through, for example, providing his or her clear and unambiguous consent.

[30] A more systematic account of the relationship between privacy and Internet innovation is given in section 3.4.

The focus on transparency and consent for the user in the new regulatory framework has both positive and negative implications for innovation and the way in which it might spur technological innovation. As regards the positive elements, technology is noted specifically in the Communication (for example with respect to Privacy Enhancing Technologies); other requirements (e.g. for 'user friendliness' of privacy notices) may also stimulate technological innovation.

For example, the provision of a principle of transparency in processing might spur innovation by companies leveraging the vast quantities of data available in, for example, a cloud orientated model to provide a real-time view of their personal data. Similarly, with a personal data breach notification regime, there are considerations about how technological innovation might support the provision of such notices when they might need to be read and understood by affected data subjects across a variety of platforms (mobile devices, tablets, PCs, laptops, e-Readers, games consoles[31] etc.).

Undoubtedly **the focus on enhancing control** over ones personal data perhaps provides the most fertile ground for spurring technological innovation. Here the Commission has outlined its objectives around strengthening the principle of data minimisation; improving the modalities for the actual exercise of rights of access, rectification, erasure or blocking of data, clarifying the 'right to be forgotten' and ensuring data portability. Indeed, the exercise of these rights electronically is specifically noted in the Communication on a new strategic framework for privacy and data protection.

Other aspects of the Communication might present more challenges in respect of technological innovation. For example, **how would a right to be forgotten be implemented?** One might imagine one technological way to meet this requirement would be via the adoption of a 'Digital Rights Management' type approach, where data has an expiry date, after which it cannot be accessed or viewed. Of course this still leaves open the question of by whom and how such an expiry date could be set.

Furthermore such a solution would also run into many of the same issues as Digital Rights Management (DRM) does in respect of copyright protections.[32]

Data portability is another interesting policy objective, not least because it seems to move beyond the personal data protection aspect of the Directive towards the free movement of data. Here, the implication is that a level playing field (a certain degree of interoperability) would be required in order to make this a reality since only then would it be possible for data subjects to move their personal data from one provider to another. This could be seen as beneficial for technological innovation as it removes or lowers barriers to entry for those firms wishing to innovate. However, as with similar discussions on standards more generally, others argue that companies might not be as interested in innovating if they had to constantly be adopting defensive business practices (by lowering prices) to remain competitive rather than focusing on delivering new products and services.

---

[31] e.g. see the recent Sony Online Entertainment data breach.

[32] DRM is seen by some as a digital way to perpetuate an increasingly untenable licensing regime regarding intellectual property.

Privacy by Design (PbD) has also achieved notoriety and interest in the policy discourse regarding the proposed comprehensive approach.[33] Privacy by Design is sometimes defined rather vaguely as an approach to the consideration and inclusion of privacy at the earliest stages in the design of a new product or service. To do this it would be necessary to try to evaluate the impact of the proposed innovation on the end-users privacy and then ensure to the greatest extent possible that the subsequent design and engineering effort takes full account of these implications. This philosophy is meant to encourage and incentivise designers and engineers to ask the question: what would be the consequence of what we are proposing to the end users privacy; and perhaps more implicitly: "can we achieve the same objective without using personal data or with less of an impact on the individual's privacy?" Privacy by design not only refers to technological solutions but to organisational and services solutions as well.[34] From an innovation perspective Privacy by Design may offer incentives in introducing novel technical and non-technical (such as organisational and user-oriented) measures in order to protect privacy. A recent study, published by the European Commission, shows that adoption of privacy enhancing technologies – forming the technological kernel of PbD – remains limited, due in part to market problems.[35]

Finally, there is also the question on the objective of clarification on the rules of consent. The case of behavioural advertising is noted as being an instance where it is not clear what would constitute 'freely given consent'[36] given the discussion about browser settings, in particular default settings, as possibly conveying consent.[37] Indeed, recent discussion in the United States about Do Not Track (DNT) legislation might be interesting in this context.[38]

2.3. The supranational European context

This section presents a short summary of other important supranational level instruments binding upon national level governments across Europe. Although these include the underlying architecture for the European Union to define and implement supranational European interpretations of the right to privacy, for present purposes they are considered separately because they have a more indirect effect on private sector agents (such as companies in the Internet space).[39]

The Court of Justice of the European Union (ECJ) interprets and applies EU law, specifically the interpretation and application of the treaties but also the interpretation of Directives.[40] Requests for preliminary rulings form the main type of procedure, where the national court is asked to request an opinion from the ECJ on the correct application of EU law.

---

33 See for instance EDPS (2010).

34 See http://privacybydesign.ca/ (visited 12 September 2011), the official website of the Canadian Privacy Commissioner Dr. A. Cavoukian, who differentiates between various dimensions in privacy by design. Privacy Impact Assessments provide an example of a non-technical measure to promote privacy awareness and privacy protecting measures.

35 European Commission (2010b).

36 Article 29 Working Party (2011b).

37 See the recent Article 29 Working Party Opinion (no. 187) on this issue http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (visited 12 September 2011).

38 E.g. US Senate (2011). DNT involves various ways for users to ask that their web activity not be tracked e.g. by means of cookies placed on end-user equipment. It is more interesting from the perspective of innovation (self-help against cookies and – presumably - other tracking technologies) than consent (DNT is similar to anti-virus software - it protects users (note viruses are also covered by article 5(3)) but those who do not use this are not thereby consenting to tracking (resp. infection).

39 Hustinx (2010).

40 Bodil Lindqvist (Case C-101/01) (2003) ECR I-12971.

In the main, other relevant procedures include infringement procedures brought by Member States or the European Commission for not complying with EU law (although there are also routes open to individuals via contacting an MEP directly and asking him to raise an Own Initiative report and also recourse to petition which requires a certain number of signatures). Member States and citizens can also try and annul EU actions that are seen to violate EU law (for example, cases against the Data Retention Directive[41] and Passenger Name Records[42]). However, there is no direct means by which a citizen can launch an infringement case against a Member State for violation of EU law. This possibility only exists for the European Commission or Member States. The implication of this for discussion about the implementation of EU level legislation and rules concerning protection of personal data by Member States is that private individuals can petition the European Commission, or a Member State, if they consider that the poor implementation of policy by a Member State has resulted in their fundamental human rights being affected.

The key implications of these procedures for those in the Internet value chain is that Article 16 TFEU in conjunction with Article 8 of the EU Charter of Fundamental Rights, establishes a general right to personal data protection and that its general applicability paves the way for harmonisation across the twin realms of privacy of electronic communications and the privacy of personal data (currently handled by two separate EU instruments).

Nonetheless, as more and more varied and innovative uses of personal data (for example, Location Based Services) begin to have an effect which exceeds the narrow frame of privacy as being concerned with the protection of personal data, it may be possible to see how the split of the articulation of a fundamental human right and also the competence to act to uphold that right (e.g. through policy initiatives or passing new legislation) may create uncertainty.

In European terms, the complexity of establishing both the definition of a fundamental human right to private life (Art 7 of the Charter of Fundamental Rights of the European Union) or the fundamental right to the protection of personal data (Article 8 of the Charter) and also the competency to act may become ever more of challenge for EU level policy makers grappling with innovation on the Internet.

2.3.1. The EU Charter on Fundamental Rights

The Charter of Fundamental Rights of the European Union became a formal part of EU law through the Treaty of Lisbon on 1 December 2009. The Charter of the Fundamental Rights of the European Union contains two articles in Chapter II, concerning Freedoms relating to privacy and personal data protection.[43] These are now binding at primary law level: following the Lisbon Reform Treaty, the Charter of Fundamental Rights now has the same legal standing as the other EU Treaties (such as the Treaty on the Functioning of the EU - TFEU).

---

41 EDRI: ECJ First Hearing on Data retention case: (July 2008) available at: http://www.edri.org/edrigram/number6.13/ecj-hearing-data-retention (visited 12 September 2011) and Out-law: Data Retention Directive has sound legal basis rules ECJ (February 2009): http://www.out-law.com/page-9783 (visited 12 September 2011).

42 See: Judgment of the Court of Justice in Joined Cases C-317/04 and C-318/04 European Parliament v Council of the European Union and European Parliament v Commission of the European Communities (May 2006) and Brouwer and Guild (2006).

43 EU Charter of Fundamental Rights available at : http://www.europarl.europa.eu/charter/pdf/text_en.pdf (visited 12 September 2011).

Article 7 of the EU Charter establishes the right to "respect for private and family life, home and communications" and Article 8 establishes rights concerning the protection of personal data:

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specific purposes and on the basis of consent[44] of the person concerned or some other legitimate basis laid down by law.

3. Compliance with these rules shall be subject to control by an independent authority.

The focus of the Charter is toward the EU's institutions, bodies established under EU law and, when implementing EU laws, the EU Member States. However, the issue of direct applicability is a matter of some controversy. Article 51 of the Charter itself sets out that it cannot extend any of the competencies of the EU. This means that it cannot be used autonomously as a basis for new EU regulatory initiatives, and could also imply that countries cannot be taken to national courts directly for violating (only) the charter. This latter rule (no direct applicability) is somewhat controversial, however, and its application by courts will undoubtedly still evolve.

2.3.2. Treaty on the Functioning of the European Union (TFEU)

Article 16 of the Treaty on the Functioning of the European Union (TFEU) details a new provision on the right to the protection of personal data. This essentially provides a legal base for measures required by the Union to fulfil the obligation from Article 8 of the EU Charter on Fundamental Rights, described above. Article 16 TFEU is the current version of the former Article 286 from the Treaty Establishing the European Community, as of the entry into force of the Treaty of Lisbon.

Article 16(1) establishes the right to the protection of personal data concerning everyone. Article 16(2) details that the rules relating to the protection of individuals with regard to the processing of their personal data shall be agreed between the European Parliament and the Council when such processing takes place by: "…institutions, bodies and offices" of the Union; "Member States when carrying out activities falling within the scope of Union law" and relating to the free movement of such data. Finally, this Article sets out that "compliance with these rules shall be subject to the control of independent authorities".

It has been suggested from private sector legal representatives that this might create an explicit right to the protection of personal data.[45] This is also reflected in the equality accorded to the EU Charter of Fundamental Rights by the Lisbon Treaty: Article 6 of the TFEU says that the EU Charter of Fundamental Rights "shall have the same legal value" as the TEU and the TFEU. There is also debate about whether Art 16 introduces a broader general right for the Parliament and Council to regulate personal data processing (including for the private sector). Based on the phrasing of article 16(2) as noted above, this would appear to be the case in relation to the free movement of personal data (i.e. the former first pillar as covered by the Data Protection Directive), and when the processing of personal data occurs in the framework of "activities falling within the scope of Union law", i.e. when the processing of personal data is incidental to another EU competence.

---

[44] C-543/09 of the ECJ indicated that Article 12(2) in the e-Privacy Directive 2002/58/EC was more about the purpose (establishing user informed control) than about the specific word used.

[45] Cooper, Tielmans and Fink (2010).

2.3.3. European Convention on Human Rights

Outside the EU context, the European Convention on Human Rights was adopted in 1950 within the framework of the Council of Europe.[46] Article 8 of that Convention provides for respect for ones private and family life, and home and correspondence, subject to certain restrictions. The scope of this article refers to protection from interference by a public authority "[…] except such as it is in accordance with the law, and is necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country[...]".

The European Convention on Human Rights permits individuals to bring a case to the European Court of Human Rights (ECHR) if they believe their human rights have been infringed by a state party. The Convention allows private individual to take an active role in the international arena but only against states and not the private sector. Therefore, (as in the Phorm case; see below) individuals have launched cases against EU Member States under the Convention at the ECHR for failing properly to regulate the activities of private parties (firms).

2.4. Examples of EU Member State policy initiatives

After having summarised the main European level legal frameworks and rules which lay out certain rights and norms to be followed, we now review some examples of European Member State policy initiatives.

Transposition of the European legal framework[47] is complemented by national interventions aimed at companies viewed as being at the vanguard of privacy enhancing (or, far more commonly) privacy invading activities. This Section considers specific examples which may be indicative of emergent 'policy'. We recognise that supra-national policy initiatives may also be instructive in this regard.

A notable recent example of relevance is the recent EU-US dialogue on privacy. In mid 2011 it was reported that regulators from the EU and US had undertaken a series of intensive meetings identifying areas of convergence between their respective approaches to regulating Internet privacy. Both Commissioner Reding and US Ambassador to the EU Kennard noted that differences between the two were overstated and that efforts to update privacy laws were converging. Speaking about the meetings, Commissioner Reding stated that: "a common belief that our approaches on privacy differed so much that it would be difficult to work together…can no longer be argued".[48]

---

[46] There are 100 instances of case law relating to Article 8 but perhaps the best- known is S. and Marper v the United Kingdom concerning the retention of DNA samples on the National DNA Database (Application 30562/04 and 30566/04 Strasbourg 2008) available http://cmiskp.echr.coe.int/tkp197/view.asp?item=19&portal=hbkm&action=html&highlight=%22THE%20UNITED%20KINGDOM%22%20%7C%208&sessionid=81827346&skin=hudoc-en (visited 12 September 2011).

[47] A broader overview of the transpositions of these relevant legal frameworks is of course available via the official EU implementation reports published by the European Commission as well as other notable studies and surveys; for example see the Directorate General Justice, Fundamental Rights and Citizenship of the European Commission Data Protection resources webpage at http://ec.europa.eu/justice/doc_centre/privacy/law/index_en.htm (visited 12 September 2011) and also Flash Eurobarometer No #226 Data Protection in the European Union: Data Controllers Perceptions: Analytical Report February 2008 available at: http://ec.europa.eu/public_opinion/flash/fl_226_en.pdf (visited 12 September 2011).

[48] EurActiv (2011). This view is not necessarily universal; a more recent and perhaps somewhat more sceptical view from the US is at pains to point out a raft of unintended (and unwelcome) consequences: http://republicans.energycommerce.house.gov/Media/file/Hearings/CMT/091511/Bono%20Mack.pdf (visited 12 September 2011).

Nonetheless, these meetings acknowledged significant remaining differences (e.g. over the 'right to be forgotten'[49]). Subsequently, in May 2011 Mrs Reding drew the attention of a European Business Summit in Brussels to the need for a common approach in an age of data flow globalisation build around security, interoperability and personal data protection.[50]

We now give a brief thematic overview of how Member States have interpreted and implemented the supranational legal framework in respect of a number of key concerns germane to this research.

2.4.1. Consent

The Phorm case

In 2009, the UK's Information Commissioner's Office (ICO) came under fire from private citizens, advocacy groups and the European Commission regarding its perceived inaction concerning trials conducted in 2006 and 2007 by British Telecommunications (BT) of Phorm's Webwise system, a technology that supports behavioural advertising using cookies and DPI. The core issue was that BT had not obtained the consent of its customers to participate in the trial under UK electronic privacy communications law. Subsequently, the European Commission issued infringement proceedings against the UK for poor implementation of rules governing electronic communications and privacy, citing "problems in the way the UK has implemented parts of EU rules on the confidentiality of communications

The European Commission had previously noted the high level of complaints about this case; then-Commissioner for Information Society and Media, Viviane Reding, assured the public that the EC would keep a watching brief on action by the UK's Information Commissioner.

Indeed, a subsequent statement implied the absence of 'rigorous enforcement' and 'proper sanctions' to enforce EU legislation on the confidentiality of communications.[51]

2.4.2. The right to be forgotten

Google (especially Street View) has come under intense regulatory scrutiny, particularly in Spain, Italy, France and Germany. It has come to be seen as an easy target ('the new Microsoft'), perhaps due to its size, importance, and/or the heterogeneity of its services. In consequence, most cases covered in the press seem to involve Google, though their implications (and others discussed in the case study) obviously go well beyond a single firm or service. Some of these cases attempt to force Google to implement the 'right to be forgotten' and/or to establish that Street View inherently constitutes a disproportionate collection of personal data (as Street View cameras were able to look into houses).

---

[49] This issue remains controversial even within Europe: the UK Information Commissioner and the UK Culture Minister have both argued recently that the right to be forgotten is unenforceable (see: http://www.research-live.com/news/government/right-to-be-forgotten-is-unenforceable-says-co/4006419.article, accessed 12 September 2011).

[50] Viviane Reding Vice-President of the European Commission, EU Justice Commissioner The reform of the EU Data Protection Directive: the impact on businesses European Business Summit Brussels (18 May 2011) at: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/349&format=HTML&aged=0&language=EN&guiLanguage=en (visited 15 November 2011).

[51] Telecoms: Commission launches case against UK over privacy and personal data protection (14th April 2009) available at: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/570 (visited 12 September 2011).

National action:

France: a court in Montpelier in March 2011 ruled that a person had a right to disappear from Google after a professor discovered it was possible to reach via the Google search engine an explicit video made when she was 18. The case began in 2008 when the discovery was made and following repeated requests from the woman, the company was finally ordered to remove the links by the Court.[52]

Spain: In a similar vein, the Agencia Española de Protección de Datos (Spanish Data Protection Agency - AEPD) initiated a case in the national court asking Google to remove links pertaining to five citizens who did not want to appear in search results, claiming that this was an invasion of their privacy.[53] Google's response has been to argue that this amounts to a form of censorship (since Google is not the content creator but rather the means by which information is made available) and that the 'right to be forgotten' is all but impossible to achieve in practice (removing hits from a website does not necessarily remove the site itself). In another case, a Spanish plastic surgeon successfully argued that the AEPD should ask Google to remove links to historically reported stories connecting him to a botched operation.[54] The AEPD contended that freedom of expression provisions did not extend to Internet search engines such as Google. The court mooted referring the case to the European Court of Justice to ascertain whether the AEPD had over-ridden European law. The Spanish AEPD is now launching a test case involving 80 people (including the aforementioned plastic surgeon) with similar concerns, which many say will set the legal standard for the 'right to be forgotten'.[55]

Italy: In 2008, three Google executives were given suspended six month sentences following a case involving a video of students taunting a teenager with autism.[56] Although the video was subsequently removed, the executives were convicted for not removing the video fast enough. The company argued that the case could stifle creativity since employees of hosting platforms, social networks and online services which permit users to upload content will be made criminally liable. The company claimed that the conviction "attacks the very principles of freedom" of the Internet; if platform providers were held responsible for every piece of content uploaded then many of the Internet's economic, social, political and technological benefits could disappear. Further illustrating the complexity confronted by the liability of service providers as common carriers (and the extent to which they should be liable for content, as illustrated by the case above) the Italian Data Protection Authority (Garante per la protezione dei dati personali) recently determined that as a general resolution data controllers must designate those companies that operate on its behalf as data processors within 60 days of this determination.

---

52 Ministère Public, FNDF, SEV, Twentieth Century Fox *et al.* vs. Aurélien D.

53 EDRI: Spain: Right to be forgotten and Google (2011) http://www.edri.org/edrigram/number9.2/spain-right-to-be-forgotten-google (visited January 2011). For more details on this and many other cases involving the AEPD and Google, please see Alonso (2011).

54 Plastic Surgeon's Legal Quest To Facelift Google Search Results (Forbes) http://www.forbes.com/sites/kashmirhill/2011/03/07/plastic-surgeons-legal-quest-to-facelift-google-search-results/ (visited March 7th 2011).

55 EDRI: Spain: Right to be forgotten and Google (2011) http://www.edri.org/edrigram/number9.2/spain-right-to-be-forgotten-google (visited January 2011).

56 CNET: Execs convicted in Google Video case: http://news.cnet.com/8301-30685_3-20000092-264.html#ixzz1OU90DaIF (visited 12 September 2011).

The implications of this in the fluid and complex web of transactions and relationships in the Internet space is the possibility that innovation may be affected by the obligation to formally distinguish each and every entity in an outsourcing relationship as a data processor.[57]

2.4.3. Public & private spaces

Physical space: In April 2011 Google announced that it would no longer capture new Street View images in Germany.[58] Google had been permitted to operate in Germany as long as a pre-publication opt-out scheme was implemented. 245,000 households made use of this to request their property be blurred. The company decided to discontinue its service despite a Berlin court ruling that street photography (of the sort undertaken by Google) was legal.[59]

Mobile and other networks: It was recently revealed that all Dutch mobile providers applied DPI to their mobile networks.[60] DPI analyses specific data relating to the kind of messages sent over a network, indicating e.g. whether a packet is part of a Skype message, streaming video etc. The Netherlands has a very dense network[61] of mobile connections; it is necessary to upgrade the infrastructure to cope with intense use of smart phones and other platforms. Dutch telecom provider KPN revealed[62] in a May 2011 business meeting its use of DPI to track use of specific applications. These include Whatsapp (a free alternative to text messaging) and Skype (a free alternative for voice telephony and chat). Concerns were voiced against potential privacy intrusions. The Dutch telecom regulator OPTA initiated an investigation into possible infringement by Dutch providers of specific articles of Dutch telecommunication law relating to personal data and privacy protection (secrecy of correspondence), security measures and delivery guarantees. Prioritising specific modes of traffic also contravenes the principle of net neutrality. In June 2011, OPTA concluded that there were grounds for concern but that more specific research was needed and handed the matter over to the Dutch Data Protection Authority (DPA). The European Data Protection Supervisor also voiced concern over potential privacy infringements through DPI and has requested BEREC and national DPAs to keep an eye on this subject.[63]

---

[57] Titolarità del trattamento di dati personali in capo ai soggetti che si avvalgono di agenti per attività promozionali - 15 giugno 2011.
(Pubblicato sulla Gazzetta Ufficiale n. 153 del 4 luglio 2011) (in Italian) 15th June
http://www.garanteprivacy.it/garante/doc.jsp?ID=1821257 (visited 12 September 2011).

[58] Google halts new Street View imagery in Germany ComputerWeekly.com (11 April 2011) available at: http://www.computerweekly.com/Articles/2011/04/11/246293/Google-halts-new-Street-View-imagery-in-Germany.htm (visited 12 September 2011).

[59] Berlin court rules Google Street View is legal in Germany DW-World (21st March 2011) available at: http://www.dw-world.de/dw/article/0,,14929074,00.html (visited 12 September 2011).

[60] http://www.gsmhelpdesk.nl/read.php?id=6075 (visited 8 November 2011).

[61] De Randstad, the industrial and service agglomeration encompassing the four largest cities of the Netherlands, is the third-largest site of intense mobile traffic in the world.

[62] http://tweakers.net/nieuws/74419/kpn-past-deep-packet-inspection-toe-op-mobiel-internetverkeer.html (visited 8 November 2011).

[63] EDPS 2011. Opinion 7 October 2011.

2.4.4. Responsibility for Privacy and security

In a related development that concerns the privacy of individual network access points as much as the privacy of personal data, Google Street View cars were found to be collecting data on Wireless (802.11) 'Wi-Fi' hotspots, including usernames and passwords necessary to gain network access. This was viewed by the French Commission Nationale de l'Informatique et des Libertés (CNIL) as a violation of the national law. In March 2011, the CNIL fined Google €100,000 for unfair collection of wireless network data via its Street View and Latitude software, after the company disclosed the practice in May 2010.[64]

Notably, the UK pursued a different approach, declining to undertake formal legal action against Street View, arguing that it constituted a minimal invasion of privacy. Instead, it requested a formal undertaking from Google that this practice would be discontinued. The competing explanations given for this practice (a source of data to help devices register on the network more quickly; a basis for unspecified future innovation; a simple mistake) make this relevant for the discussion on innovation. Note also that the issue of privacy in the sense of control over personal network access has arisen in other contexts; the UK, Germany and France have – or have considered - legal sanctions against users who fail to secure their wireless networks.[65]

More recently, Apple and Google have attracted regulatory interest from France and Italy for the storage and transmittal of varying levels of finely grained data regarding cell phone towers and Wi-Fi hotspots. The technological reason is convenience: both Google and Apple argued that without the capture and recording of such data the delay required by Android and iOS devices to locate and register on networks would have been far too long from the user standpoint.

2.4.5. Towards a more stringent consent test for cookies

EU Member States have more recently come under scrutiny regarding implementation of the revised ePrivacy Directive, especially the new more stringent consent test for cookies. The deadline for transposition was May 25th 2011. As of that date, according to publicly available information, only a handful of EU Member States had transposed the Directive or published measures associated with its transposition.[66] The main discussion so far appears to revolve around Article 5(3) (requirement to obtain explicit prior consent for cookies).

---

64 Wall Street Journal (2011) "Google fined in France over Streetview" (March 21) http://online.wsj.com/article/SB10001424052748703858404576214531429686752.html (visited September 2011).

65 http://www.pcpro.co.uk/news/security/358033/brits-could-face-legal-action-for-leaving-wi-fi-unsecured, http://www.eweekeurope.co.uk/news/germany-to-fine-users-for-unsecured-wlans-7020, http://www.google.co.uk/url?sa=t&source=web&cd=4&ved=0CCwQFjAD&url=http%3A%2F%2Fwww.hadopi.fr%2Fdownload%2FSynthesis-HadopiSurvey.pdf&rct=j&q=secure%20personal%20wireless%20networks%20illegal%20hadopi&ei=mwccTpDPMsiJhQfez5CvBw&usg=AFQjCNF7kUbAK1W-2AHz-ilGfKwC_RurSg&cad=rja (all pages accessed 12 September 2011). On the other hand, hacking into unsecured wireless networks is not a criminal offense in the Netherlands: http://news.techworld.com/mobile-wireless/3266058/hacking-wireless-network-routers-no-longer-illegal-in-holland/(visited 15 October 2011). Google's Global Privacy Counsel Peter Fleischer apologised for inadvertently collecting payload data from unencrypted Wi-Fi networks.

66 At the due date (25 May 2011) six countries (Denmark Estonia, Finland, Luxembourg, Spain and the UK) had brought the necessary transposition measures into effect. At the time of finalising this report (early November) nine other countries had followed suit (Latvia, Sweden, Ireland, Malta, Lithuania, Hungary, France, Portugal and Austria) while Germany has accepted the transposition measures but has not yet published them officially http://www.t-regs.com/content/view/442/1/ (visited 12 September 2011).

Some firms in the Internet services value chain contend that this may require the implementation of a variety of dialog boxes or pop-ups that might significantly impede the user experience.[67] Others note that the Directive leaves room for differing national interpretations and that the resulting absence of texts and likely delays in transposition impose great uncertainty on those wishing to operate. In February 2011, a Finnish law firm, for example, argued that Recital 66 provides an opportunity to mitigate or even 'evade' the prior consent requirement through browser settings reflected in the proposed Finnish Act on the Protection of Privacy in Electronic Communications (*Sähköisen viestinnän tietosuojalaki*).[68] This determined prior consent by establishing whether the user has set their browser to permit or deny cookies, which they described as a "triumph" of user friendliness over the privacy arguments in the e-Privacy Directive amendments. Nonetheless, this interpretation by Finland appears to fly in the face of the Opinion given in 2010 of the Article 29 WP on Behavioural Advertising which indicated that browser settings could be used to establish valid consent only in unique situations.[69]

The UK Minister for Culture, Media, and Sport appeared to be taking the same approach in a May 2011 open letter to industry (two days before the expiry of the deadline for transposition) explaining that the requirement of prior consent should be based on browser settings and thus that any enforcement action against companies under the e-Privacy Directive amendments would be delayed by approximately one year until there is widespread adoption of such browser controls.

Ultimately, with the continuing discussions on the evolution of the European framework regarding privacy and data protection (the General Data Protection Directive), it is interesting that the debate has focused on cookies and what means may be legitimately claimed to establish prior consent (e.g. browser settings) and how industry has claimed that the new rules will result in endless dialog and confirmation boxes confronting the user (thus having a detrimental impact upon the browsing experience) in contrast to the claims of others that the privacy invasive nature of cookie placement along with measures such as 'supercookies' and Flash cookies[70] constitute a important challenge for the privacy of Internet users, since the systemic complexity and opacity of how these operate (apparently in seeming defiance of the legal and regulatory framework described above) makes it difficult for consumers to be aware of their operation and exercise any meaningful degree of control over their presence or use.

This line of development illustrates two further important points. The first is that Member States clearly see the requirements of the General Data Protection Directive as a spur to innovation – developing and implementing more effective and efficient ways to comply with the spirit of prior consent than a literal reading of the General Data Protection Directive would imply. The second is that the argument against intrusive requests for consent constitutes at least an implicit recognition of the importance of a 'right to be let alone' in a user-defined Internet space.

---

[67] European Union ePrivacy Directive Update Industry Insights: the Adobe Blog for Omniture Technology (24 May 2011) http://blogs.omniture.com/2011/05/24/european-union-eprivacy-directive-update/ (visited 12 September 2011).

[68] http://www.castren.fi/Page/c1ccbac8-1bad-436e-bb79-e1ffaa00df14.aspx?groupId=a0231459-d54f-4ff6-8057-034a2b359a33&announcementId=b841f3d0-0d3a-4c72-b9b3-3f036b00332e (visited 12 September 2011).

[69] Article 29 WP (2010).

[70] Supercookies and flash cookies are cookies with powerful tracking capabilities which move the techniques of tracking into the realm of the persistent identification of visitors to a site through exploitation of browser functionality permitting them to view the history of which sites the user has visited see for example, Tirtea *et al.* (2010) and "Cookies, Supercookies and Ubercookies: Stealing the Identity of Web Visitors", 2010, available at: http://33bits.org/2010/02/18/cookies-supercookies-and-ubercookies-stealing-the-identity-of-web-visitors/ (visited 12 September 2011).

In connection to this 'right to be let alone' it is worth noting the recent debate concerning the extent to which providers of Internet services (for example, in this case Yahoo![71]) may infringe one aspect of privacy (contents of email) in order to protect another aspect of privacy (freedom from spam). Yahoo! has been accused by consumer groups of 'mining' users' emails for information useful in targeted marketing campaigns (in effect replacing untargeted commercial solicitations with targeted ones). In this sense, depending on the philosophical interpretation of privacy (noted earlier on in this report) the ISP may be caught on the horns of a dilemma between implementing potentially contradictory measures in an attempt to achieve two different privacy enhancing objectives.

The issue of prior consent again arises, though it has not been pivotal to date. On a higher level, it should also be noted that the issue of equivalent protection has resurfaced in connection with the revised Data Protection Directive, as legislators consider whether and how to respond to the very different stance taken in the US Patriot Act. A senior Microsoft executive has clearly indicated that under the Patriot Act it is not possible to guarantee the safety of data in the cloud.[72] The Patriot Act allows US authorities access not only to European data held in US data centres but also to data held in European data centres administered by US companies. Moreover, it is not – under current law – always possible to notify data subjects about such interception and access.

---

[71] http://www.bbc.co.uk/newsbeat/14077856 (visited 12 September 2011); Google also uses scanning, though Microsoft's Hotmail service does not – and makes this evident to users.

[72] http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225 (visited 12 September 2011). Note that the existing "Safe Harbor" provisions are self-regulatory in nature (though occasionally enforced by the US Federal Trade Commission – see http://writ.news.findlaw.com/ramasastry/20091117.html accessed 12 September 2011) and do not extend without complications to the cloud – see http://www.zdnet.com/blog/igeneration/safe-harbor-why-eu-data-needs-protecting-from-us-law/8801?pg=3&tag=mantle_skin;content (visited 12 September 2011).

3. CURRENT AND FUTURE TENSIONS

KEY FINDINGS

- Latest opinion poll data show that individuals regard the disclosure of personal data online as a necessity and that trust in Internet companies such as search engines, social networking sites and email providers is low.
- However, no-one seems to be willing to pay for enhanced privacy: Privacy Enhancing Technologies have largely failed to find uptake, few companies have implemented Privacy by Design and consumers show no great demand for companies to provide privacy enhanced functions (like email encryption).
- Private sector firms on the Internet conduct a variety of privacy invasive and privacy protective activities. This includes the sharing of customer or subscriber data with third parties, the deployment of applications without clear and unambiguous user consent but also the promotion of transparency, user education and anonymisation of user data.
- The Gap Analysis of the relationship between Internet innovation and privacy highlights a number of issues from different perspectives:
    - legal issues include ensuring appropriate protection for individuals, transparency, enhancing user control, improving awareness and ensuring free and informed consent;
    - sources of market failure include lack of recognition of positive externalities, a 'tragedy of the data commons,' imperfect and asymmetric information and market dominance;
    - sources of system failure include inadequate infrastructural provision, path dependency and lock-in to undesired situations and weaknesses in institutions, organisational interaction and capability.

3.1. Who cares about privacy?

The proposed new European legal framework regarding privacy and data protection articulates, as Chapter 2 has summarised, potential obligations with respect to the principle of transparency regarding the activities of data controllers. Any understanding of how such legal frameworks may affect privacy and innovation must be placed in the context of how individuals perceive privacy and 'value' it. The question is whether the increased transparency that these laws could afford might actually make a difference in how privacy is valued by citizens.

The question as to what constitutes 'value' in a concept as elusive as 'privacy' presents challenges. Privacy, as a fundamental human right, is regarded as an important enabling property of democratic liberal society. Without privacy, it is argued, there would be less freedom of speech or freedom of association (Bennett and Raab, 2005). The lack of privacy would have a chilling effect on human relationships, further rendering our every decision transparent (Lace, 2005).

Privacy as a facet of self-determination and what it means to be human is valued by scholars, jurists and policy-makers but in a different way to how it can be valued or appreciated by individuals. Given the Internet's role in acting as a highly effective vehicle for freedom of expression[73] these different approaches to understanding the value of privacy are brought into sharper focus in an online context.

It may become apparent therefore, that different types of actors in the online domain value privacy differently: policymakers have an appreciation of its value because of the role that privacy plays in delineating and characterising society and supporting the exercise of certain other interlinked fundamental rights. Businesses and economic agents value (or, more commonly, do not) privacy for the way in which it may enable or deny access to personal data. Finally, individuals can hold competing and at the same time contradictory estimations of what 'privacy' is 'worth' to them: for example – in an abstract sense recognising its importance in contributing to liberal democracy on the one hand, but trading it economically for benefits on the other.

Whilst much has been written about how businesses and governments 'value' (or not) privacy (e.g. see Solove; 2009 and Lace, 2005) there is still little consensus on how individuals appreciate differing and sometimes contradictory valuations.

The usual way in which individual attitudes and measures regarding concern for privacy have been identified is via opinion polls, of which the 2011 Special Eurobarometer report No. 359 on Data Protection and Electronic Identity is a case in point.[74]

This recent research contains some interesting perspectives regarding citizens' general attitudes to privacy. 74% of the respondents in this Eurobarometer survey considered that online disclosure of personal information was an increasing part of modern life. A majority of participants in the survey expressed concern over the recording of their behaviour via payment cards, mobile phones or the mobile Internet. The study reported that 58% of respondents said that they feel there is no alternative than to disclose personal information to obtain products and services.

The Eurobarometer research also reported that six in ten Internet users usually read privacy statements (68%) and that a majority (70%) that did so adapted their online behaviour. Levels of trust in companies active on the Internet was reported to be low: less than one-third (32%) trust (mobile) phone companies or Internet Service Providers and just over one fifth (22%) trust other Internet companies like search engines, social networking sites and e-mail services.

The research further discovered that 70% are concerned that their personal data held by companies may be used for a purpose other than that for which it was collected. A majority (75%) wanted to delete personal information on a website whenever they decide to do so.

Further afield, the A.F. Westin / Harris Interactive series of opinion polls on attitudes to privacy in the United States have gathered data on attitudes to privacy for a multitude of years.

---

[73] See for example the Chairman's Report from the Expert Meeting on Human Rights and the Internet, Stockholm available at: 2010 http://www.sweden.gov.se/content/1/c6/13/93/96/829645b7.pdf (visited 12 September 2011).

[74] Special Eurobarometer 359 / Wave 74.3 – TNS Opinion & Social: Attitudes on Data Protection and Electronic Identity in the European Union (July 2011) available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf (visited 12 September 2011).

Their analysis of data on privacy surveys going back to 1990 has led to the development of a Consumer Privacy Segmentation model based on similar questions asked in different surveys over time. These data show that in general (people responding to such surveys) can be divided into three categories (Westin, 2008):

- **Privacy fundamentalists** (25-35%) react very negatively to questions about access and disclosure of personal data;
- **Privacy pragmatists** (55-60%) generally weigh up the alternatives and attempt to undertake a reasoned or rational calculation;
- **Privacy unconcerned** (10-12%) do not express any interest in the privacy related questions being asked of them.

A 2008 poll using this model shows concerns of citizens regarding privacy and handling of personal data by Internet companies. 59% of online users do not feel comfortable with their online activities being tracked in order to customize ads or content (Westin, 2008). The poll also revealed an increased scepticism by online users that websites would really follow privacy and security safeguards. It stated the concern of users "that there would be no user remedies or protective regulation to control such web sites if they did not" (Westin, 2008, p. 6).

Current user approaches to privacy in online networks

The common understanding that 'digital natives' (i.e. those having grown up with technology and are familiar with it) are unconcerned about privacy and that familiarity with the technology determines appreciation of its implications was challenged at a recent workshop on Ethics and Corporate Responsibility.[75] Here, participants noted that tools provided as a result of technical innovation are seen as beneficial by those who have been borne into the 'Internet age'. They are regarded to be so much entwined with everyday life that not using them is inconceivable. However, they faced problems about the degree of control users may exercise over their digital footprint. This usually was not sufficiently regulated. They also experienced problems in not being able to exercise more authority over the how and to what purposes this data is used. They expressed a need for self-constraint (that is to say, a degree of responsibility) on the part of the consumer. One step forward is to increase awareness about privacy and the implications of sharing data online. Beyond awareness, a future in which services are offered with higher privacy standards but for a fee was regarded as not entirely out of the realms of possibility.

Emergent theoretical research on 'valuation of privacy' seems to indicate that current approaches to understanding these perceptions (such as opinion polls of the type described above) only reveals part of the story concerning how people 'value' privacy – perhaps reflecting the view of individuals concerning their view of the value of privacy as characteristic of liberal democratic society, compared to how privacy is regarded in an online context. Since policy makers may base their legal or regulatory interventions in part upon such data there is a risk that they might not be fully attuned to how people 'value' privacy. Put simply, the emergent field of research into the economics of privacy shows that different approaches to capture an understanding of value may result in different valuations.

[75] European Dialogue on Internet Governance (EuroDIG) 2011, Ethics and Corporate Responsibility Workshop, Belgrade, 30 May 2011.

Opinion poll and survey data tend to capture abstract views of privacy as a societally beneficial but abstract good whereas behavioural and economic experiments permit researchers and policy makers to understand how individuals may compromise their own privacy in order to achieve other benefits (e.g. discounts or savings in time or in convenience). This has two implications in terms of policy making. Firstly, how to sensibly craft public policy providing the framework in which data subjects can trade-off a *direct and immediate* valuation of their privacy based on empirical evidence from an *abstract and remote* valuation about the societal usefulness of privacy (as may be captured in broad opinion polls and surveys).

Secondly, the regime of notice and choice assumes a level of individual rational choice that is being challenged by theoretical evidence from the emergent field of behavioural economics. Designing a legal and policy framework that expects users to make finely grained choices (such as a notice and choice regime for third party cookies, for example) might risk further confusion and fragmentation (given the apparent increasing use of third party cookies on ad supported 'free' online services). This in turn casts doubt on the strong implication of the rational-choice-based approach that provision of more information (even in intelligible 'non-legalese', as stated in the 2010 Communication on 'A comprehensive approach on personal data protection in the European Union') will ultimately result in more 'rational' (and hence better) choices on behalf of the data subject (see for example McDonald and Cranor, 2008).

What is the rationale for valuing privacy or personal data? Why is this important in a policy context? European jurists and legal experts have argued that given its status within European law as a fundamental right (as described above), acknowledging the benefits of its monetisation is not a legitimate approach to the formulation of public policy. Such approaches, it is argued implies that a fundamental human right may be traded as a private good (Hustinx, 2009). However, scholars in the 'new economics of privacy'[76] argue that there are benefits, basing their reasoning around two main arguments:

- 'Control', 'choice' and 'consent' are watchwords and important characteristics of normative, legal and policy frameworks regarding privacy and, especially, personal data protection. Understanding what drives privacy valuations is important since this enables policy makers to better appreciate how informed individuals are when they make decisions about privacy and how their personal data is used. This might allow policy makers to determine whether there are opportunities to 'nudge' users to more socially 'beneficial' behaviours.

- There is a need to represent the value of privacy in order to better design policies which may proportionately address its protection against other societal needs such as openness, disclosure or freedom of expression.

Research in this area[77] hypothesises that consumers (especially in the confusing and highly dynamic online environment) may not express their privacy preferences in an economically rational manner i.e. where they take the time to read, understand consider and compare privacy policies of competing service providers. Rather, consumers may make decisions on the basis of rules of thumb or a biased interpretation of the balance between the short term gains and long term losses of disclosing personal information.[78]

---

[76] For example see the economics of privacy online resources page at: http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm (visited 15 November 2011).

[77] e.g. see the series: Workshop on the Economics of Information Security (WEIS).

[78] Known as hyperbolic discounting e.g. see Acquisti and Grossklags (2004).

Acquisti and Loewenstein (2010) find three factors that may undermine a consistent and stable valuation of privacy:

Firstly, the difference between Willingness To Accept (WtA - an estimate of the utility gained or lost by accepting some invasion into your privacy in return for something else) and Willingness To Pay (WtP - an estimate of the utility gained or lost when surrendering something else for an increase in your privacy). This parallels the well-known reference position effect;[79] people may demand as much as three or four times as much in exchange for allowing others to use their private information as they would pay to protect it.

Secondly, individuals have to cope with complexities of understanding whether they are being asked to value a certain type of information or to value the privacy of that information. The value of the information they can acquire often provides direct and instant gratification while the value of privacy may be linked to long term indirect consequences.

Finally, human beings exhibit a set of consistent, predictable deviations from the theoretically rational/optimising strategies in decision making behaviours. The literature concerning cognitive and behavioural facets of individual decision-making shows that these deviations may be driven by a range of behaviours including:

- lack of knowledge;
- lack of self control[80] and
- the fact that the disclosure or release of personal data involves
    - estimates of risk ("what will happen to me if I disclose my personal data?");
    - uncertainty ("what are they doing with my personal information and why?");
    - deferred costs ("how does not disclosing my personal data now help me in the future?") and
    - gratifications ("I think the chances of something going wrong at some point in the future are low but on the other hand I can immediately obtain some benefit").

Condensing these research findings leads to the following conclusions:

1. People might respond to opinion polls in a socially benign manner ("privacy should be safeguarded") that may be reinforced by questions posed at a relatively high level and not directly related to issues affecting the person's private life.
2. Overall, people experience problems in balancing simple short-term gains against long-run, difficult to assess risks. In economic experiments, this shows up as a pronounced willingness to trade privacy (as a longer term risk) for apparently modest direct benefits.

[79] Rafaeli and Raban (2003).
[80] Loewenstein and Haisley (2008).

3. Theoretical economic research also shows that the reference position effect (which reflects the framing of such choices in terms of surrendering privacy or regaining it) is relatively large.

In addition to evidence that citizens systematically depart from the predictions of rational choice models and struggle to act consistently in the face of difficult to compare risks, illustrative examples point to a degree of apathy even concerning the abstract valuation of privacy.

For example, in late 2009 the European Commission launched a public online consultation[81] and an open online discussion forum on privacy and data protection. The response to both the consultation and the online discussion forum, given the size of the population of the EU, was very modest (only a few hundreds, many of which were from non-EU and EU legal entities rather than EU citizens).

Secondly, in the aforementioned Italian Google Video case, it was anecdotally noted afterward that a number of Google Video users viewed the video before a user clicked on the 'Report Offensive Content' button.

This raises three issues:

- how to get individuals engaged in meaningful discussion;

- how any potential bias due to this apparent apathy may be addressed; and

- the degree to which scale economies militate in favour of technical 'fixes'.[82]

3.2. What do Internet innovators do to protect and/or abuse privacy?

3.2.1. Classification of activities

This Section will consider the deployment of Privacy Enhancing Technologies (hereafter PETs) and Privacy and Identity Management Systems (PIMs). It includes a model for monetising costs and benefits based on prior analysis from the Study Team and an analysis of how firms determine whether (or not) to implement privacy friendly policies. We apply this analysis to evidence from the interviews and the desk research portions of the study. Where appropriate, we quote the interviewees to support and illustrate our analysis.

---

[81] Archived version of the consultation available at: European Commission DG Justice – News – Public Consultations 14 November – 15th January http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm (visited 15th November 2011).

[82] Given the sheer quantity of online content uploaded to platforms such as YouTube and other social media, online providers must of necessity rely upon self-regulated moderation (filtering). This community aspect may drive companies towards technical innovation as a way to efficiently manage privacy risks. The alternative would require human editorial control over each and every piece of user generated content; an impossible task in today's information rich Internet landscape. This can be seen with respect to face blurring technology for example (see Section 4.4).

3.2.2. Why use personal data?

From an economic perspective, it is commonly understood that the rationale for the increased focus on personal data in the private sector revolves around a number of reasons. Innovation is but one, and stems from an underlying assumption that as more and more wealth is driven from a service led economy, the desire to: reduce transaction costs; gain a better understanding of current customers and tailor marketing and the development of new products and services to meet current and new demand becomes greater. In particular, more and better information about consumers is seen as important since it allows marketers to better target adverts to those interested in particular products and services, resulting in an increase in the success rate of advertising and reducing costs on both sides (sellers producing more goods and services for individuals that don't want them and buyers reading adverts for products they are not interested in).

One of the main ways of achieving such efficiencies is via the use of personal data, as a recent report from the OECD suggested, as the new 'oil'.[83] Other statements support this: for example, 'identity' has been regarded as the single organising principle of the modern service led economy.[84] Data and information about individuals is now the raw material for the development of innovative products and services as well as for price discrimination[85] and product differentiation. Intrusions into people's privacy by the collection and analysis of data about individuals allow greater efficiency in the marketplace because it can be used by sellers to better understand buyers' willingness to pay.

In this way they can more efficiently price products and services. Price discrimination is particularly worthy of note and the implications in respect of privacy have been considered in the theoretical literature. For example, in September 2000 there was public controversy when Amazon was discovered to be engaging in an experiment concerning price discrimination (also known as variable pricing) where customers saw different prices for the same product depending upon whether they visited Amazon's website from their own computer or not.[86] This was possible was via the mining of data about Amazon customers, such as their shopping habits and use of the service.

Received wisdom is that increased technological opportunities now available to gather information about people expands the capability to price discriminate (offer different prices to different people for the same products and services based on accurate information about their willingness to pay). Note that price discrimination is different from product differentiation (for which information about people is also useful) where different products (e.g. luxury versus regular types of coffee) may be offered to different people based on an understanding of their preferences. Information on individual's preferences may also be derived from analysis of data about individuals. In particular, mining personal data can allow firms to practice third-degree price discrimination (where price varies by some attribute correlated with the customer's willingness to pay) or even first-degree price discrimination (in which the firm is able to charge each customer the maximum price and thus capture the full value of the transaction). This may be considered to reduce or eliminate the consumer's share of gains from trade (the difference between the price they actually paid and the maximum price they were willing to pay) which consumers would otherwise enjoy as a direct consequence of the sellers' ignorance of consumer preferences.

---

[83] OECD (2010).

[84] Speech by John Madelin at the IAAC Members Annual Meeting 2006 available at http://www.iaac.org.uk (visited 12 September 2011).

[85] Odlyzko (2003).

[86] Wired: Online Prices Not Created Equal – 07th September 2000 available at: http://www.wired.com/techbiz/media/news/2000/09/38622 (visited 12 September 2011).

This may otherwise be described as the privacy of consumer tastes. This can be linked to two larger issues: firstly the fairness of such transfers from consumers to sellers and secondly the implications for overall efficiency (maximisation of total gains from trade). Under some circumstances (particularly when consumer privacy is eliminated and the seller captures the entire surplus), such discrimination certainly promotes both efficiency[87] and the profitability of firms able to use such information.[88] The concern expressed by some is that the overall economic gains may undercut governmental[89] willingness to address the equity issue by intervening to halt the use of personal data to price discriminate. Interviews conducted during the course of this study re-affirmed the view that overt price discrimination is a clear business driver but that its presence is hidden behind other measures including those implied by personalisation and recommendation systems. The value of private consumer preference information is such that a secondary market has emerged, with 'third party information brokers' playing an arbitrage role linked to the collection of such data and its re-use either through sale or direct marketing.

> Expert quote: "Behavioural advertising is already having a significant impact on privacy and data protection [...] What can be expected is that the new players will be motivated to push the boundaries of personal data use; and at the same time they will attempt to push for changes in laws to make that acceptable."

Nonetheless, as Odlyzko (2003) suggests, it seems that a possible future based on this model will result in a situation where individuals may have to pay more for their privacy. The consumer's willingness to remain anonymous, to shroud information from the seller which might otherwise result in a cheaper product, will ultimately cost more. This may be summed up in the maxim: "anonymity comes at a price".

Market structure considerations influence how players in the Internet value chain (identified in the model at the beginning of this report) increasingly seek to generate value by means of services that exploit individual data. In particular, traditional telecom operators have found that the decreasing margins from voice telephony[90] coupled with their unique access to a wide variety of information about subscribers, leads them towards monetising those subscriber data. The increasing technological and business complexity of their operations and ever present regulatory requirements (e.g. provisions on security and maintenance of access) reinforce this by putting greater pressure on margins and increasing the scope for operational data collection. Interviewees noted that traditional telecom operators are now acting as information brokers e.g. by reselling operational information; new privacy challenges arise as the rationale for use of personal data evolves from efficient provision of an established service to offering new products and services.

---

87 Indeed, some markets probably wouldn't exist without price discrimination; under the efficient regime of uniform marginal cost pricing, the – often quite substantial - fixed costs of internet businesses couldn't be recovered, but average cost pricing would lead to allocative inefficiency (deadweight loss).

88 Pigou (1920) introduced this taxonomy of price discrimination. Png & Lehman (2002) differentiate: complete discrimination; direct segmentation, where the seller conditions on some – but not all - individual characteristics; and indirect segmentation, where the seller differentiates offers by package size etc. to induce individuals to reveal their information by self-sorting. Price discrimination *may* improve efficiency, but may also consolidate market power or sustain collusion, especially when information about consumer characteristics is effectively 'controlled' by individual sellers to limit consumer mobility and thus blunt competition.

89 The risk arises if economic policy is overly centred on increasing overall economic output or business' profitability (share of total economic surplus), which does not necessarily raise welfare; economic rent-seeking may be directly costly to the economy as a whole. Certainly, the struggle to increase economic profits (rather than total surplus) provides business with powerful incentives to elicit and capture private information, leaving the human right to privacy vulnerable to economic rent-seeking.

90 European Commission (2009).

Furthermore, whilst some operators use information-generating and information-capturing technologies as tools for network management, others use them as a central component of the business model. This is particularly true of Information Society Service providers, not ISPs *per se*, but also providers of search engines, social networking sites and others. Although they may not have begun that way, many now base their business models on the optimal extraction and economic exploitation of information about service users.

Nonetheless, interviews conducted during the course of this study indicate that the market advantage for individuals to surrender their personal information is in general weighted toward disclosure of personal information rather than its protection, e.g. it is 'cheaper' for consumers to allow others to control and use their information than it is for them either to protect their privacy or to exploit this information for their own gain. The inequitable allocation of returns from use of personal information leads to inefficient and/or privacy-infringing use of these data. The market failed to deliver either optimal economic value or effective privacy protection.

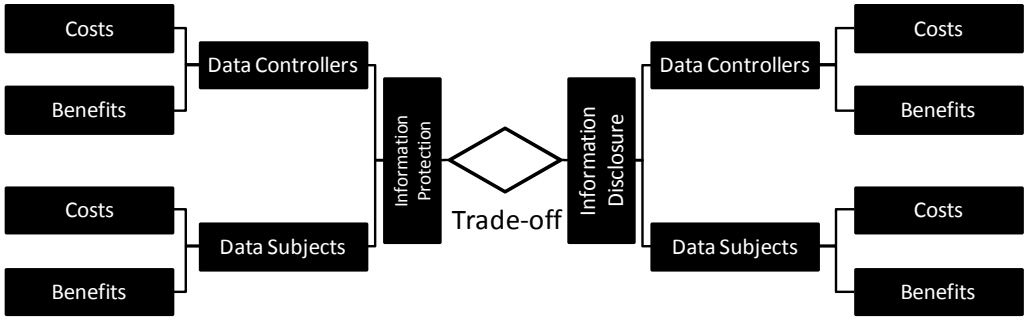
An interview conducted during the course of this study indicated that regulatory intervention was considered necessary to correct this imbalance in favour of fundamental rights, but any intervention should take the form of 'hard' technological tools rather than softer measures (e.g. via interpreting Privacy Impact Assessments as a process rather than a set of technological measures).

> Expert quote: "The economic advantage for individuals to give personal data away in general is larger than the economic advantage of shielding this information. This implies that the business case for innovative privacy technologies will be negative if no other conditions or constraints are taken into account."

3.2.3. A framework for economically valuing privacy

Since any appreciation of the valuation of something necessarily requires an understanding of both the costs and benefits associated with it, it makes sense to propose such a listing. Such a possible general framework defining costs and benefits of the disclosure and protection of information is indicated below in Figure 4.. This diagram may be used to understand how providers and consumers factor in different costs and benefits relative to their own contexts in order to exercise the value of personal information. The model is presented as a trade-off (appropriate since this concerns valuation) with a de-construction of the costs and benefits between information protection and information disclosure.

Figure 4: Cost / benefit framework for personal data disclosure and confidentiality



3.2.4. Information Protection

- **Costs of information protection for the data subject** The costs of protection of personal data may be indirect and include or incur cognitive and opportunity risks. For example, the cost of getting informed: the process of reading, assimilating learning and understanding the implications of privacy policies in order to properly exhibit 'informed' consent may be a high opportunity cost. Similarly, changing habits or behaviours associated with improving privacy also has costs: consumers have to learn different behaviours, perhaps pay for anonymising technologies or other privacy enhancing technologies or tools. Other costs could be expressed as delays or difficulties in using software or functions designed to improve the protection of information which may get in the way of the accomplishment of specific tasks. There are also costs which may occur if consumers do not wish to share data – namely that the more personal data is a requirement or pre-requisite for offering goods and services, the higher the opportunity cost for consumers who wish to protect their data (since they have to spend more time searching for firms that either do not collect personal data to offer the same products and services or whose personal data collection activities more closely match their preferences).

- **Costs of information protection for the data controller** For the organisation wishing to use personal data to obtain some kind of value from it, there are costs associated with establishing mechanisms for its protection. These may include the deployment of technologies to encrypt data held in databases, or establishing training programmes for staff or perhaps appointing a Chief Privacy Officer. There might also be costs involved with meeting regulatory or legal compliance requirements, for example in the European legal framework, prior notification and designing and preparing privacy policies, contractual clauses and so on. Such costs are often identified by firms as playing an important role in their decisions to deploy privacy enhancing measures – however, these may be understood as fixed rather than variable costs. Perhaps more importantly, there are implications associated with lost opportunity costs of not engaging in potentially lucrative data mining or gathering activities which could result in the more efficient extraction of consumer surplus. Firms may encounter opportunity costs and inefficiencies when potentially welfare enhancing data disclosures do not take place. There may also be a reduction in social welfare caused by the imposition of protective mechanisms: for example, if certain types of personal data revealing medical conditions were kept private then the efficiency and accuracy of the delivery of healthcare could be reduced - it would be more difficult to undertake analysis to determine propensity of certain public healthcare challenges.

- **Benefits of information protection for the data subject** If personal data is kept protected, then there are benefits which may be accrued to the data subject: most notably reduction in the risk that identity theft may occur or that the merchant is able to correlate personal information with data subject's willingness to pay for a certain good. Other research suggests that despite the concerns of data controllers that information protection mechanisms may result in reduction of benefits generated from using such information, many of the benefits associated with the disclosure of personal data may still be gained when data is protected. For example the imposition of restrictions on behavioural targeting had an impact (reduction in overall welfare) on websites with general content but *not* regarding ads on sites with specific content or for example larger advertisements (Goldfarb and Tucker, 2011). The policy implication of this finding is that for most websites which have general content a stronger cookie rule (as envisaged in the revised e-Privacy Directive) might result in less welfare.

- **Benefits of information protection for the data controller** There may be benefits associated with establishing measures that protect the personal data of customers. By implementing protective measures the firm may avoid future liabilities and costs associated with the implications of abuse or misuse of personal data, for example fines or costs associated with sending out breach disclosure notices. Furthermore there is an open question as to whether information protection practices may act as a determinant of choice on the part of the consumer. This is where information protection may act as a 'business enabler' and enhance revenue in the situation where consumers choose one merchant over another due to the perceived efficacy of information protection mechanisms.

3.2.5. Information disclosure

- **Costs of information disclosure for the data subject** Perhaps the most well known cost of information disclosure to the data subject is identity theft, but there are also other direct and indirect costs, for example: expected damages from incorrect or poorly stored customer data; segmentation and profiling which may drive the customer to services she does not need or cannot afford. Individuals may incur costs expressed as wasted time to delete junk emails, dealing with telemarketing or higher prices due to (adverse) price discrimination. Other examples of objective harms aside from identity theft include the unexpected use of the data subject's personal data against him or her at a point in the future. After a data breach, there may be costs associated with the consumer whose personal data has been breached or compromised switching to a competitor (paradoxically perhaps increasing the chances of another breach as it involves the resubmission of personal data to another entity). Some of the other costs may be difficult to monetise since they involve subjective harms such as the psychological damage or discomfort associated with feelings of being watched or monitored or 'chilling' effects resulting from a perception of intrusion. Costs associated with unintended consequences include the onward use of personal data in ways that the data subject did not envisage at the time the personal data was disclosed. Other indirect costs include the bargaining power obtained by third parties who are able to mine and interrogate personal data of customers across different transactions and platforms.

- **Benefits of information disclosure for the data subject** The surrendering of personal data by the data subject or customer implies that some benefit is received. This may be expressed as immediate monetary compensation (e.g. a discount) or intangible benefits (for example, content delivered according to retrieved preferences derived from the customers personal information). Customers might benefit from less junk mail (since the firm will know more precisely the interests and be able to better predict the needs of the customer thus sending less irrelevant messages. Prices could be reduced as a result of more targeted and less wasteful advertising and marketing and targeted advertising may allow other services to be delivered free of charge to the consumer. There are decreases in transaction costs associated with the secondary re-use of personal data that may accrue to data subjects – this can be seen in federated authentication schemes where the personal data provided by the customer to identify himself with one provider may be exchanged as a means for the customer to identify himself more easily to a second provider without having to incur the costs of retyping and repeatedly submitting the same information. Macro-economic effects might be possible to be seen to accrue from this data. For example the broader identification of trends and patterns (for example whether regulation is proving effective in facilitating a market for more privacy enhancing practices) is one example. Other secondary effects could be via advanced vehicle traffic management systems which, through the sharing of personal information (for example GPS inferred location; driving habits, source direction, duration and destination of journeys), may help to smooth out or address problems of demand or congestion.[91]

- **Costs of information disclosure for the data controller** Data controllers which collect personal data may incur direct and indirect tangible and intangible costs. Some may include the loss of business caused by consumers switching away from the company due to stories or perceptions about poor or untrustworthy data collection practices or, ex-ante, these concerns may put off future customers (for example disclosure of the practice of price discrimination). This is the lost opportunity cost of future business and the extent to which perceptions and fears about privacy deter consumers from engaging in transactions where such data is involved. Organisations using personal information may also incur other types of costs including the imposition of fines by regulators for poor practices regarding the use of information disclosed by data subjects. Examples of this abound but one particularly noteworthy instance was the £1m fine levied in 2007 by the UK's Financial Services Agency (FSA) against Nationwide.[92] Other similar types of costs include redress (covering the damages the customer has incurred or costs associated with issuing data breach notification letters) or legal fees. Examples of indirect costs may include the loss of stock market value which may occur following a breach of personal data. Other costs include the establishment and creation of means to collect and manage these stores of personal data (for example, through customer relationship management systems).

[91] e.g. see Hoh, Gruteser, Herring *et al.* (2008).
[92] Nationwide fined £980,000 over stolen Laptop *The Register* 14th February 2007 http://www.theregister.co.uk/2007/02/14/nationawide_fined/ (visited 12 September 2011).

- **Benefits of information disclosure for the data controller** By mining and using personal data submitted by consumers, it is possible for firms to create highly accurate pictures of consumer's demographic traits, preferences, behaviours and so on. These may come from IP addresses, cookies, click-streams and DPI tools.

  These datasets permit the firm to benefit in its marketing capabilities addressing specific target markets or customers, thereby lowering advertising costs (since ads are not targeted at individuals unlikely to be receptive to them). In addition, since advertisements are targeted to those individuals more accurately identified as expressing a preference for a product it is possible to increase revenues (as there is a greater chance of an advert's effectiveness).

- Furthermore the collection and storage of such expansive data on preferences may increase loyalty (since it imposes costs on consumers to move their carefully built preferences to a competitor).

- Firms are also able to compile aggregate trends and conduct analysis to better match supply to demand, minimising inventory risks and enabling highly accurate just in time logistic chains (as supermarkets might do through the mining of preference data about purchases collected by loyalty card schemes). The analysis and subsequent resale of information collected by credit reporting agencies may be used to allocate credit efficiently amongst borrowers thus contributing both to more efficient prices for existing customers (those determined to be lower risk by analysis of their personal data may be offered cheaper premiums) but also more customers (since customers ordinarily deterred from entering the market due to the fact that premiums are set above what they would be willing to pay could become interested).

- There are also the benefits that accrue to firms when they sell on personal data to others, when they realise that customers data is a tradable asset of economic interest to other firms. For example, users (or perhaps more rightly their attention spans) of social networking sites offered targeted behavioural advertisements by third parties become the 'product' and their privacy the commodity. the real customers of such sites are of course are those third parties who pay to access and analyse the personal data of users. The debate still continues as to whether this may accrue as a benefit even if the individual is not personally identified.

3.2.6. Privacy enhancing technologies (PETs)

Aside from the operational and procedural orientated measures to obtain compliance with different legal and regulatory requirements and meet privacy principles (e.g., establishing a privacy policy, appointing a Chief Privacy Officer, establishing a Privacy by Design programme), the use of technology to enhance or protect privacy is becoming increasingly of interest. This goes beyond the existing Article of the 95/46/EC on provisions requiring data controllers to take appropriate technological and organisational measures. Innovation, particularly technological innovation, provides a route to the development and rollout of such technology, known as Privacy Enhancing Technologies (PETs).

The deployment of PETs are seen as a way to permit the automatic and technological application of privacy and data protection principles. These principles are encapsulated in the legal and regulatory framework governing privacy and data protection instruments and relevant applicable national law, or organisational wide instruments such as Binding Corporate Rules (BCRs).

The 2007 European Commission Communication on PETS furthermore gives indicative examples including cookie cutters (programs that support the management of cookies or software placed on user machines), encryption tools, the Platform for Privacy Preferences (P3P) and anonymisation tools.[93]

The broader deployment and take up of such technologies has the potential to support the creation of an environment of trust and confidence for the conduct of e-Commerce and e-Government in the networked Information Society. PETs may support consumer-centric privacy[94] where it is possible to exercise rights and where consumers/citizens can participate more actively in a two way business interaction rather than being subjected to a one way process.

The absence of the widespread deployment of PETs may be attributed to their initial cost and uncertainty about the technology, but also uncertainty about the business benefit. The deployment of PETs may involve a trade-off for businesses as seen through the framework described above. PETs may reduce the possibilities of personal data as an economic resource.[95] Although we have seen that the perception of poor custodianship of personal data is an explanatory factor driving the gap between the reality of e-commerce and its ambition, articulating this to corporate decision-makers has yet to succeed. Similarly, there may be concerns about upfront costs, integration into existing IT systems and customer relationship management systems. There is also worry that the added complexity represented by the deployment and use of these technologies to the consumer will outweigh the opportunity cost of gaining new customers. The firm might end up in a net loose of business. This consideration of the intangible impact of the use of these technologies cannot be ignored. Anecdotal evidence from corporate sector players indicates that significant thought is given to the negative impact that the deployment of PETs might have – in terms of customers not participating in those services covered by PETs.

Table 4 presents a description of the benefits and costs for deploying and not deploying PETs within the private sector.Interviews conducted during the course of this study revealed that the market for PETs still does not function very well: there is limited demand and take up. This is perhaps due to the inbuilt structural imbalance of the use of personal data on the Internet previously described: the weight of economic benefit for the consumer rests with the disclosure of information rather than its protection.

---

93 Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs) COM(2007) 228 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:EN:PDF (visited 12 September 2011).

94 Shao and Smith (2007).

95 London Economics (2010).

Table 4: Model for understanding economic benefits of PETs

	Benefit	Cost
Deploying PETS	• Increased market share/more customers (use of PETS becomes an added-value factor in customer choice) • Increased revenue from existing customers who feel more comfortable in divulging personal information • Reduced costs of operating compliance/regulatory units (since demonstrating compliance becomes easier) • Leveraged economic efficiencies across the organisation from externalities caused by use of common technology	• Decreased revenue from loss of existing customers who do not participate due to usability/unfamiliarity • Decreased sales - lost opportunity cost from missing new business • Cost of dealing with customer queries (e.g. in call centre, technical support, customer service) • Cost of customer education & marketing programme • Lost opportunity cost from negative publicity/word of mouth • Cost of deployment and long term management
Not deploying PETs	• Efficiencies (resulting from ability to price discriminate/differentiate using identifiable information) • Maintenance of existing market share (as a result of not being seen to be taking risks by deployment of such technologies) • Maintenance of existing ICT infrastructure budget (as a result of not having to deploy such technologies)	• Decreased revenue or sales resulting from reputational damage of privacy breach • Costs of dealing with regulatory compliance requirements, post breach (e.g. audit) • Management, technical and support costs of dealing with incident • Costs of running an ongoing manual based regulatory compliance regime based on checking and authorisation.

This is of course related to the earlier discussion about the difference between what consumers may report in opinion polls generally about abstract attitudes to privacy (for example, that they express a high degree of concern) versus what happens in reality (they are willing to surrender personal data for a small of economic benefit).[96]

> Expert quote: "one should not be very optimistic on the market perspectives of privacy technologies. [...] Competition is not going to work on the prevailing market conditions."

Nonetheless, there is high political interest in PETs and the related concept of Privacy by Design. As we have seen, the European Commission's Strategic Communication on the new legal framework for privacy and data protection has singled out Privacy by Design as an important artefact of a possible revised regulatory regime. In addition, the 2010 European Commission study on the economic costs and benefits of PETs also noted from businesses, citizens and regulators in those countries consulted during the study that: "There is little evidence that the demand by individuals for greater privacy is driving PETs" and "Even in cases where PETs deployment is potentially beneficial for data controllers, deployment rate may still be low."[97] This study mentions perceived lack of benefits, perceived limited usefulness, direct costs, long term costs, lack of awareness, lack of consumer demand, refusal of consumers to pay for PETs, lack of political imperative and lack of enforcement as some key issues that hinder widespread diffusion of PETs into data services.

In the United States, interest in PETs & PbD has also been shown by the US Federal Trade Commission (FTC). In a recent report by the US FTC, PdD was defined as part of a proposed new privacy framework including also simplified consumer choice and increased transparency of data practices.[98] The FTC report defined PbD as when companies promote user privacy through their organisations and at every stage of the development of their products and services. It would appear as though there is a link between PbD and PETs.

Examples of PETs, which may be part of an overall PbD approach, include identity management (e.g. U-Prove) data tagging tools, transport encryption and other tools to make it easier for consumers to check and adjust their privacy settings (e.g. in browsers). Nonetheless, few PETs have become popular and there appears limited demand for products with such protections built in. The reasons for this lack of demand, aside from the previously discussed paradox between what consumers say their preferences are, versus their observed behaviour, include consumers lack of knowledge about the privacy risks associated with web-surfing, search, social networking and e-commerce and the limited understanding of how PbD and PETs might reduce or address these risks.

---

[96] Grossklags and Acquisti (2007).
[97] London Economics (2010).
[98] Federal Trade Commission (2010).

4. EMPIRICAL FINDINGS

KEY FINDINGS

- Technologies that are basic to Internet innovation are growing in complexity. Complexity is further increased through convergence of existing and emerging technologies. They extend the range of privacy intrusions by offering tools to capture and exploit spatial data ("Where are you?") and biometric data including genes ("Who – or what - are you?").

- Business practices tend to use ever more numerous and diversified personal data. This is encapsulated in the expression "Personal data is the new oil". The incentive for businesses to make ever greater use of personal data seems far stronger than any incentive for businesses to be prudent and reserved in their use of personal data or to offer safeguards to prevent personal data misuse and abuse.

- People are by and large not fully aware of the privacy risks associated with new Internet technologies and business practices. When offered a choice, people tend not to be proactive in guarding their privacy, letting immediate consequences – especially benefits - prevail over long term or indirect consequences – especially risks. When surveyed directly, however, people tend to show interest in their privacy; a significant fraction of the European public values privacy and wants constraints on unhindered collection and aggregation of personal data.

- It would seem in general that ordinary citizens should have the capacity to understand the impact of business practices on their privacy; however, the technological tools and the business practices offered are usually too complicated to enable them to fully grasp these impacts or understand the choices.

- Some cases involved varieties of soft regulation. Others show business practices focusing on reserved and prudent use of personal data. Overall, soft regulatory measures are not often used and business self-restraint is visible only in niche markets. Strong regulatory measures seem to be uniquely required in safeguarding the privacy of citizens and consumers.

- In some domains - notably homeland security - proposed laws and regulations could represent a direct threat to privacy.

We will now turn towards the case studies used to increase the understanding of the relationship between Internet innovation and privacy. Each case started with desk research into relevant features in relation to the identified dimensions. The desk research was complemented with expert interviews. Juxtaposing the results of the case studies with the expert interviews yielded input for a subsequent expert consultation that, in turn, helped to test and enrich the preliminary findings of our research. The consultation focused on the consequences of insights provided for policy making.

This Section presents a brief overview of the main findings per case study. Each case begins with a generic description that highlights the main trends and issues related to the case, continues with a description of the tensions between privacy and innovation, and concludes by inventorying elements of a mitigation strategy for the tensions identified.

The cases we studied cover:

- Radio Frequency Identification (RFID)
- Biometric technologies
- Online behavioural advertising (OBA)
- Location based services
- Cloud computing

4.1. Radio Frequency Identification (RFID)

Radio Frequency Identification (RFID) refers to a technology using radio waves or induced electromagnetism to read remotely data stored on tags. An RFID system typically consists of a tag (sometimes called a transponder), an interrogator (or reader), middleware, a back end processing system and the interconnecting networks. Typically, an RFID system comprises a multitude of tags and a relatively smaller number of interrogators (or readers). The tag contains data which can be stored either in the tag's own memory or on an embedded microprocessor and can vary from simple identification numbers to biometric data.[99] The tags can contain read-only data (data set at the production stage of the tag) or read/write (data can be changed subsequent to tag production). Tags can be passive (i.e. requiring the energy of the radio signals sent by the interrogator to perform an action) or active (having an internal energy source that enable an action by itself) and they can be read from various distances.

RFID technology is an advancement over widely-used printed bar-codes. Unlike bar-codes, RFID readers do not require contact or line-of-sight to acquire an ID. Instead, communication is possible through the human body, clothing and non-metallic materials.[100]

Owing to advancements in ICT, RFID has evolved from a technology primarily used in the military and agriculture to one with applications touching virtually every aspect of the life of an individual.

During the second half of the 20th century, RFID started being singled out as one of the most promising technologies. By no means new, RFID's potential outside its original domains of application (agriculture and the military) was only starting to be discovered and already attributed equally great potential in terms of generating sizable economic benefits. The versatility and broad scope for innovation of RFID, which can be employed in domains as varied as logistics and health care, was one of its main pros, only to be enhanced by the onset of the Internet of Things. RFID is already used for many different applications, such as in supply chain management, manufacturing process tracking, asset tracking, payment systems, airport luggage handling, and security and access control.[101]

---

[99] Lieshout *et al.* (2007).

[100] See for an introduction to RFID technology: http://www.aimglobal.org/technologies/RFID/what_is_rfid.asp (visited 12 September 2011).

[101] In the EU communication "Radio Frequency Identification (RFID) in Europe: steps towards a policy framework" many uses of RFID are listed under "why RFID matters". The communication can be downloaded from: eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0096en01.pdf (visited 12 September 2011). Also see Lieshout *et al.* (2007) for an overview of application areas.

The market for RFID technology is growing rapidly, with an estimated global value in 2010 of $5.63 billion, up from $5.03 billion in 2009.[102] In total, 2.31 billion tags were expected to be sold in 2010 worldwide, up from 1.98 billion in 2009. The public sector is the largest investor in RFID technology for applications including person identification, animal chipping, and public transport ticketing.[103]

RFID is broadly regarded as an enabling technology. Its main purpose is the identification of the object to which it is attached. It is often argued by the RFID industry that privacy issues arise not from the technology *per se* but rather from the systems that use the unique identification provided.

RFID raises a number of tensions that are presented below.

Emerging technologies

RFID is a rapidly evolving technology, sometimes described as a 'moving target',[104] making it more difficult to address potential privacy issues.

RFID tags are rapidly becoming smaller, cheaper, and smarter. 'Smarter' RFID chips can for example be equipped with microprocessors instead of just electronic memory. This could create both new privacy risks and new opportunities for protecting privacy, for example by making the microprocessor act as a controller that only discloses personal data to legitimate RFID readers.

Smart technologies and applications arising from the convergence of multiple technologies are enabling new possibilities for innovation in gathering and combining data, e.g. by combining RFID with GPS to track identified objects (and their owners). The data involved can originate from different domains (e.g. product information on an RFID tag, personal identifiers on a supermarket loyalty card, location information from the mobile phone) and combined in order to create new personalised services with increased value added for the consumer. However, these enhanced technologically enabled profiling possibilities also carry more privacy risks for individuals thus targeted.

Moreover, RFID is regarded as one of the building blocks for the Internet of Things, in which networks and the Internet will become **increasingly pervasive** and many objects will eventually become connected and able to communicate with each other. This however, raises questions regarding the limited or total **lack of consumer awareness**, and the **potential for undesired disclosure of personal data**.

RFID is also used in applications involving biometrics, such as fingerprint recognition for passports. Storing biometric information on RFID chips also poses privacy risks. Protecting these data requires strong security measures to prevent 'man in the middle' attacks or other measures to prevent illegal access to the data stored on the RFID chip.[105]

---

[102] See "RFID in 2010: The New Dawn" on http://www.idtechex.com/research/articles/rfid_in_2010_the_new_dawn_00002437.asp (visited 12 September 2011).

[103] *ibid*.

[104] As stated in the EU Communication on RFID on http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0096en01.pdf (visited 12 September 2011).

[105] Juels (2006).

Another potential tension is related to the use of RFID implants.[106] There are many beneficial uses for such implants, ranging from the accurate monitoring of medical conditions of hospital or residential patients, to the convenience of electronic payments[107] and to better access control of individuals to certain buildings. At the same time, there are also potential risks that accompany the benefits to be derived from the use of RFID implants, ranging from health to privacy risks (e.g. a chip can migrate through the body, causing adverse tissue reactions and sometimes a heightened risk of specific forms of cancer;[108] patient autonomy can be limited; individuals can feel monitored in their movements and other activities).

Further privacy issues are likely to emerge from the use of RFID in the workplace (i.e. the use of RFID for employee identification and access purposes, computer use in the context of a growing mobile workforce and home workers which will extend the tracking and tracing of employees outside their workplace and in their private spaces.)

Tracking by proxy (i.e. identifying and tracking individuals indirectly by tracking tagged items in their possession) is also likely to pick up and bring about new types of privacy concerns.

Business practices

RFID technology and related applications hold great promise and potential to benefit virtually every aspect of society. However, as mentioned in the EU Communication on RFID, the technology "will only be able to deliver its numerous economic and societal benefits if effective guarantees are in place on data protection, privacy and the associated ethical dimensions that lie at the heart of the debate on the public acceptance of RFID".[109]

The relatively recent attention from the EU regulator[110] regarding RFID and privacy has met with substantial resistance from the RFID industry. Although recognizing privacy protection as an important factor in promoting consumer trust in the technology, the industry interpreted the attention from the EU regulator[111] as having an overall negative impact for a variety of reasons. The industry considered it **unfair** that RFID should be **singled out as a privacy-invasive technology**. Equally, the industry considers RFID to be neutral as a technology with privacy issues related predominantly to the back end systems in their opinion. Moreover, privacy-preserving measures likely to be imposed on the industry (such as data encryption on the tag, the disabling of tags, etc.) would **add to the production costs**, putting the industry at a disadvantage. It was also argued by the RFID industry that mandatory privacy-preserving measures such as those mentioned above would **disadvantage the consumer**: for example, the automatic disabling of tags would deny consumers' access to after-sales services.

---

[106] Van Oranje Nassau *et al.* (2010).

[107] http://www.technovelgy.com/ct/Science-Fiction-News.asp?NewsNum=104 (visited 12 September 2011); the Baja Beach club in Barcelona already started in 2004 implanting chips that contain identification information and that could function as an electronic purse as well.

[108] See e.g. Covacio, S. (2003); more references cited in http://en.wikipedia.org/wiki/Microchip_implant_(human) (visited 8 July 2011).

[109] EU Communication on RFID : ds-dt01terra.tsn.tno.nl\\projects\\055\\0\\01067\\Werkdocumenten\\Cases\\eur-lex.europa.eu\\LexUriServ\\site\\en\\com\\2007\\com2007_0096en01.pdf (visited 12 September 2011).

[110] Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification SEC(2009) 585. SEC(2009) 586, C(2009) 3200 final, Brussels, 12.5.2009.

[111] *Ibid*.

The recent[112] European Privacy and Data Protection Impact Assessment (PIA) Framework on RFID, a joint effort on the part of the industry and the EU regulator, is a promising initiative in trying to assess and address risks related to RFID systems. The Framework advises on the generic methodology and uses of PIAs and differentiates between a light and a more comprehensive approach. Given that the PIA Framework has been adopted only recently, in 2010, it is still too early to estimate its effectiveness.

User behaviour

A possible privacy issue related to RFID is derived from the fact that the technology is relatively unknown to the public: the information available is insufficient to allow the public to come to an informed judgment on the balance of risks of RFID.[113]

The most recent pan-European survey[114] into public perception of RFID dates back to 2005 and indicates that individuals' awareness was low and perceptions were mixed. In the consultation document of the European Standardisation Organisation it is mentioned that "82% of the European citizens were not aware of RFID technology; of the 18% aware of the technology, more than half were concerned about tracking via product purchases, targeting via direct marketing, use of data by unauthorized third parties and the possibility of distance reading of tags."[115] More recent, though less comprehensive, surveys[116] indicate only **slightly improved levels of awareness and perception**.

All these and other RFID-related developments will pose new challenges for managing privacy. For example, the tendency of RFID tag developments towards smaller, transparent and even practically invisible tags gives rise to concerns that individuals may carry many RFID tags without being aware of them, and hence being **unable to exercise control.** In the US, this has led to consumer groups proposing US federal legislation that would give consumers a right to know about the presence of RFID chips in products.[117]

---

[112] Kroes (2011b). Privacy and Data Protection Impact Assessment Framework for RFID Applications 12 January 2011 http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf (visited 12 September 2011).

[113] See also the EU Communication on RFID on eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0096en01.pdf (visited 12 September 2011).

[114] Capgemini (2005).

[115] Draft ETSI TR 187 020 - Radio Frequency Identification (RFID); Coordinated ESO response to Phase 1 of EU Mandate M436 (European Telecommunications Standards Institute). docbox.etsi.org/STF/M436_RFID/Public/DTR-07044-v0012.doc, p. 46 (visited 12 September 2011).

[116] See for example Commission Staff Working Document, Results of the Public Online Consultation on future RFID Technology Policy "The RFID Revolution: Your voice on the Challenges, Opportunities and Threats" accompanying the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework {COM (2007) zzz final} SEC (2007) 312, Brussels 2007. http://ec.europa.eu/information_society/policy/rfid/documents/rfidswp_en.pdf (visited 12 September 2011).

[117] See "RFID Right to Know Act of 2003" on http://www.spychips.com/right-to-know-bill.html

Legal/regulatory issues

RFID poses a series of privacy and data protection challenges, linked to some of its characteristics, among which[118]:

- RFID tags include unique identifiers which makes it possible to reference them back (directly or indirectly) to their owners (tracking);
- RFID tag data and reading have no interface for the individual; this renders them virtually invisible or inscrutable, thereby limiting the individual's scope of choice and consent;
- the multitude of (envisaged) RFID-enabled applications and the vast range of domains in which they can be used can render RFID virtually ubiquitous;
- virtually invisible quality of tags through miniaturization (e.g. nano-RFID), embedding (e.g. woven tags; subcutaneous or implanted tags) or just ubiquitous spread;
- RFID has the potential to be a disruptive technology in that it changes the way in which individuals interact with each other and with their environment;
- RFID tag life exceeds its use purpose or data protection legal prescriptions;
- RFID tags do not include standard privacy features.

As such, several European Directives addressing privacy and data protection are also applicable to RFID technology, including the Data Protection Directive, and the ePrivacy Directive, as is the Charter of Fundamental Rights of the European Union, and in particular its Article 8,. (Many RFID applications fall only under the general Data Protection Directive and are not directly covered by the e-Privacy Directive.[119])

RFID, next to social networking applications and browser applications, have been defined[120] as the categories of applications that deserve special attention from the regulator. It is likely that they will be addressed specifically in the revised version of the Data Protection Directive.

> *"I see EU-led policy making on RFID as a very positive example. Here, Europe has been proactive and discussed issues related to privacy at a time before RFID was expected to get widely employed. This work is a very powerful building block for the development of the Internet of Things, where Europe is clearly taking the lead at least in terms of regulation."*
>
> (Interviewee on RFID)

---

[118] Gabriela Bodea (TNO) in Draft ETSI TR 187 020 - Radio Frequency Identification (RFID); Coordinated ESO response to Phase 1 of EU Mandate M436 (European Telecommunications Standards Institute) docbox.etsi.org/STF/M436_RFID/Public/DTR-07044-v0012.doc (visited 12 September 2011).

[119] See also the EU Communication on RFID on http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0096en01.pdf (visited 12 September 2011).

[120] European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, Brussels, 18 March 2010. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf (visited 12 September 2011).

Moreover, in recent years, RFID has been the subject of a number of specific regulatory measures meant to address privacy and data protection issues and thus improve consumer confidence in the technology. Already in 2006-2007 RFID was the subject of a large-scale European consultation.[121] Such measures follow critical opinions issued by the European Data Protection Supervisor,[122] the Article 29 Data Protection Working Party[123] and consumer rights groups. All urged that privacy-preserving measures be taken and **privacy-by-design principles be applied to RFID-enabled systems**. The opinions lead to the European Commission Recommendation of 12 May 2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification which outlined concrete measures to be taken in this direction. As a result, an industry-designed **Privacy and Data Protection Impact Assessment Framework for RFID Applications**[124] has been published; an initiative for RFID signage[125] has been started; and a number of related standardisation initiatives have been announced.[126]

Approaches/Solutions

Having RFID technologies closely scrutinized by European policy regulators has led to interesting forms of **co-regulation**. RFID is most probably the first technology for which a Privacy and Data Protection Impact Assessment Framework has been developed in the EU. Practical experience is needed to assess whether the framework will live up to expectations (e.g. increasing transparency on risks associated with using RFID).

Various other EU standards, among which signage for RFID, are currently being developed as part of a regulator-industry joint effort.

On the technological side, one can notice that a variety of techniques and solutions that meet security and privacy requirements are already available. Most notable developments have taken place in the area of encryption solutions for RFID applications. These **privacy-friendly** approaches have however not yet resulted in large-scale uptake due to their negative impact on cost effectiveness and user-friendliness of systems.[127]

Transparency tools that would enable individuals to check whether products carry RFID-chips and see what kind of data is stored are still in their infancy.

---

[121] European Commission (2006).
[122] European Data Protection Supervisor, EDPS (2008).
[123] ARTICLE 29 Data Protection Working Party, Working document on data protection issues related to RFID technology, WP 105, Brussels, 19 January 2005.
[124] Privacy and Data Protection Impact Assessment Framework for RFID Applications 12 January 2011: http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf (visited 12 September 2011).
[125] RACE Network RFID, Guidelines on the Use of the Common European RFID sign, Draft Version 1, July 2011, Brussels. http://race-networkrfid.org/files/pdf/draft-guidelines-for-the-use-of-the-common-RFID-sign-2.pdf (visited 12 September 2011).
[126] See EU Mandate 436: "Standardisation mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of Information and Communication Technologies Applied to Radio Frequency Identification (RFID) and Systems" and Draft ETSI TR 187 020 - Radio Frequency Identification (RFID); Coordinated ESO response to Phase 1 of EU Mandate M436 (European Telecommunications Standards Institute) docbox.etsi.org/STF/M436_RFID/Public/DTR-07044-v0012.doc (visited 12 September 2011).
[127] See for instance the website hosted by Gildas Avoine and others which captures an interesting library of 'RFID and security' papers. http://www.avoine.net/rfid/index.php (visited 8 July 2011).

Finally, the RFID industry warns against widespread use of control instruments for end users such as 'silencing' the RFID chips at the point of sale or putting them in 'deep-sleep mode' (so that they will not be activated when interrogated by a reader). Such types of controls would deprive customers of valuable after-sales services.

4.2. Biometrics

The origins of using bodily features for identification or authentication purposes date back to ancient China in the 14th century already using fingerprinting for signature purposes.[128] Since, with the rise of fast computer chips, a variety of techniques have been developed, from traditional fingerprinting techniques towards sophisticated and relatively fast DNA profiling techniques. The latter one is extremely accurate (the chance that two persons have a similar DNA profile is only 1 in 100 billion) but DNA analyses still take a few hours to be accomplished. This makes the technology unsuited for real time applications.

The market for biometrics technology is a growing market. A recent market study expects the market to grow from $4.2bn in 2010 to $11.2bn in 2015.[129] Within this market Automated Fingerprint Identification Systems (AFIS) capture the largest share, growing from $1.4bn in 2010 to $3.3bn in 2015. The iris, the vein (recognition by means of vein patterns) and the facial market will however experience slightly larger compound annual growth rates (27.5%, 25.4% and 24.2% respectively vis-à-vis 19% CAGR for fingerprinting technologies), hence closing the gap a bit and requesting a larger part of the biometrics market.

The market study stipulates that the major driver for growth in the biometrics market must be sought in concerns for national security. Many countries are in the process of developing identification systems based on facial recognition and fingerprints, in large part enforced through legislation which has been adopted in the aftermath of the attack at the World Trade Centre in 2001 and the bombings in Madrid (2004) and London (2005).

Though this feature of biometrics technology focuses on early recognition of criminals and terrorists, and will only be successfully used when it supports full identification of individuals, another branch of biometric development focuses on the development of decentralised authentication technologies, without need for identification of individuals. On card biometric algorithms can compare real life biometric features (fingerprint or iris scan) with stored biometric features. Verification of an individual's identity within the card may act as trigger for enabling specific services (e.g. by certifying that "this individual is authorised to enter this building or make this transaction" instead of reporting that "this is individual X, who is authorised to enter this building or make this transaction").

The following tensions can be noted:

Emerging technologies

Facial recognition technologies are becoming main stream technologies with social network provider Facebook offering opportunities for tagging recognized faces throughout the 'Facebook universe'.[130] This implies that people may be recognized on photos far outside their own control sphere (figuring on photos taken by others) and may be confronted with their appearance on these photos.

---

[128] Garza (2011).
[129] http://www.marketsandmarkets.com/PressReleases/biometric-technologies-market.asp (visited April 6, 2011).
[130] http://www.facebook.com/blog.php?post=467145887130 (visited 10 July 2011).

Google offers a service to search the web for images as search term. This may pose problems when one is not sufficiently aware of settings, for instance of Picasa albums.[131] Camera surveillance technologies become more sophisticated as well. Algorithms are deployed and developed that enable detection of specific kinds of behaviour (detecting signs of aggressive behaviour or signs of remarkable behaviour).[132] The combination with facial recognition techniques is used in football stadiums where photos are taken every three minutes of the entire stadium with intelligent cameras. Coupling with back end systems that show identities of all spectators (who have entered the stadium by means of biometric identity cards) enables fast detection of uproar and localization of 'hooligans'. Voice recognition may be part of the system.[133] DNA analysis can be done in only a few hours and detection times are expected to be shorter in the near future. Various countries already have national DNA databases, in which standard procedures exist for storage of DNA of criminal offenders. Conditions will be met for registering DNA material change with newer and faster DNA analysis techniques, leading to lowering the thresholds for using DNA profiles in fighting crime or tracking illegal immigrants. Emerging technologies which relate to **improved service quality** while **reducing faults and fraud in decentralised systems** are true single sign-on systems, biometrics security cards (with one time passwords), use of electro-physiological signals for verification and identification (heart, nervous system, brain patterns). **Embedded biometrics** (biometrics on cell phones and laptops), 3D facial recognition techniques and new iris scan techniques add to the existing stock of biometric applications. Key words for these systems are thus user-friendliness and improved user convenience.

Business practices

Biometric services are deployed as part of national and regional security. This is a blossoming market. In a recent overview the European Commission discerns eighteen different surveillance systems in use or in development for protecting Europe and European citizens against threats of criminality, terrorism and illegal immigration. Several of these systems deploy biometric technologies (fingerprints routinely taken when entering Europe and when requesting a passport; DNA collected in case of specific criminal activities).[134]

Decentralised biometric systems are used in a variety of business sectors as part of security and identification/verification measures. They are used for accessing buildings and equipment, for performing transactions, for premium services at airports. Decentralised biometric services are gaining momentum in offering competitive advantages when offering dedicated services.[135] One example is services that are offered to premium travellers: the registered passenger approach in which registered passengers (i.e. regular business class travelling passengers) are offered advantages over ordinary passengers by fast check-in lanes (on the basis of iris scan identification techniques). Companies are aware of potential feelings of exclusion this may evoke by other passengers and the problem of false negatives. The main incentives are to speed up airport processes and to improve travellers' convenience without compromising safety.

---

[131] See http://www.google.com/support/forum/p/Picasa/thread?tid=6f8143b26dfe743d&hl=en for a discussion on how to prevent photos from a Picasa album from become public and being used as a search term.

[132] Yang and Rothkranz (2010).

[133] http://www.security.nl/article/16564/1 (visited 12 September 2011).

[134] European Commission 2010. Overview of Information Management in the area of freedom, justice and security. COM(2010)385 final (visited 12 September 2011).

[135] EBP (2007) *Biometrics in Europe – Trend Report 2007*. http://staatswissenschaft.univie.ac.at/fileadmin/user_upload/inst_staatswissenschaften/Frisch/21063courseWebsite/Biometric-TrendReport2007.pdf (visited 6 April 2011).

Another often mentioned use of biometric identification is in the **fight against welfare fraud**.[136] Identity fraud is considered to be responsible for about 10% of unjustified claims on social security benefits. A 2002 UK study calculated a loss of 1.3 billion UK pound per year, a figure that was raised in a 2006 study to 1.7 billion UK pound per year. Biometric identity systems especially prevent so-called 'double dippers' to be successful. Concerns are about false positives (people who are wrongly identified as being double dippers) and problems with enrolment (which is still a hard to tackle problem with systems based on finger prints).

User behaviour

Not much is known about user acceptance of biometric technology. Societal resistance against centralised biometric databases is present and has gained momentum given recent initiatives to halt centralised storage of biometric features in a number of countries. A large number of societal interest organisations (60) have recently requested the Council of Europe to start a thorough investigation to European practices in storage of biometric data of European citizens.[137] The organisations question whether the European approach concerning biometric data storage is in line with the requirements of proportionality, subsidiarity, and security safeguards that should be given.

Decentralised biometric verification systems could help users frustrated with having to remember many different passwords for different systems, improving convenience and service delivery. However, systems such as company access cards enable individual tracking so guidelines are needed to prevent unwarranted use of registered information.

Legal/regulatory issues

In the domain of **internal security**, a number of regulations adopted in the previous decade have had major impacts on the relation between privacy and innovation. Most relevant to the European context have been the US-VISIT programme (which enforces the exchange of passenger data between the US and Europe for passengers visiting the US) and International Civil Aviation Organization (ICAO) biometric passport standardization initiatives. These activities did not go unnoticed. Two civic society organisations, Privacy International and the American Civil Liberties Union (ACLU) already in 2004 **called for a halt to the introduction of nation-wide biometric systems** as enforced by the ICAO regulations. As a UN organisation, ICAO is responsible for development of a standardised biometric passport that should contain two different identification techniques. The best technique at the time was facial recognition (85% correctly identified) followed by fingerprints (65% correctly identified); other biometric identification techniques scored even less.[138] Privacy International and others voiced concern that "the ICAO is setting a surveillance standard for the rest of the world to follow. In this sense, the ICAO is setting domestic policy, implementing profiling and ID cards where previously none may have existed, or enhancing ID documentation through the use of biometrics, and increasing the data pouring into national databases, or creating them when none previously existed."[139]

---

[136] ICO (1999).

[137] http://www.privacyfirst.nl/aandachtsvelden/biometrie/item/340-internationale-oproep-tot-europees-onderzoek-naar-gebruik-van-biometrie.html (visited 14 April 2011).

[138] https://www.privacyinternational.org/issues/terrorism/rpt/icaobackground.html (visited July 9, 2011).

[139] https://www.privacyinternational.org/article/pi-open-letter-un-agency-dangers-biometric-passport-standard (visited 9 July 2011).

The ICAO followed the US-VISIT regulations which demanded machine readable e-passports containing a facial image and two fingerprints in interoperable format by June 28, 2009 (the facial image should already be available August 28, 2006).[140] A first regulation (Council Regulation 2252/2004) adopted by the European Parliament and Council in 2004 promised timely introduction of e-passports with facial images and fingerprints. A second regulation in 2009 (Council regulation 444/2009) introduced additional requirements, for instance requiring personal passports for young children with fingerprints for those aged 12 or older (a provisional age limit) and additional technical requirements on security ("enhanced anti-forgery, counterfeiting and falsification standards"), access ("prevention of unauthorised access") and common technical standards for the facial image and fingerprints. In the preamble, the Parliament and Council refer to the Schengen Information System II and the Visa Information System as two systems that could profit from the automated recognition techniques and the availability of data concerning criminals and terrorists. As stated in the report: "The planned introduction of the Visa Information System in the EU creates a new demand for high volume, high quality fingerprints capturing all over the world. This also initiated the development of the largest biometric identification system." (EBP 2007, p. 18).

Currently, national biometric databases are coming under attack due to their potential privacy impacts they may have on the privacy of all citizens. The UK has physically destroyed its national biometric identity register.[141] In the Netherlands, the obligation to include biometric identification in national ID cards has been halted and national registration of biometric identifiers will no longer be pursued.[142] Notwithstanding these reservations regarding the need for and effectiveness of national databases, the requirement for passengers to have biometric e-passports have not been challenged. The withdrawal of recent national initiatives for collecting biometric data is in line with the observation of an interviewee:

> "Though biometric systems might offer some privacy protection [...] they only protect against specific threats. In a fundamental sense they have a large privacy impact by themselves."
>
> (Interviewee on biometric systems)

Approaches/solutions

A key privacy issue concerns **centralised systems** under development through national and supra-national initiatives relating to national and supra-national security and the fight against criminality, terrorism and illegal immigration. The importance of these objectives requires the strict regulation of such systems. Their effectiveness is not always evident, which is a reason for rigorous **impact assessment** of their effectiveness and record of false positives and false negatives. This raises broad human rights issues, of which privacy is a part.

---

[140] Unisys (2007).
[141] http://www.guardian.co.uk/government-computing-network/2011/feb/10/minister-destroys-national-identity-register (visited 8 July 2011).
[142] http://tilburgers.nl/d66-en-pvda-willen-vernietiging-van-vingerafdrukken/ (visited 8 July 2011).

The competitive advantages of biometric systems mainly accrue to decentralised systems. **User friendliness**, **user convenience** and **support for value added services** will contribute to the wider acceptance of biometric systems. This is part of the business strategies behind biometric market development. The wider public is already becoming accustomed to biometric technologies through their use in consumer equipment (e.g. cell phones and laptops) and company access cards.

While decentralised biometric systems may help assure users' privacy (by shielding unnecessary identification) centralised public biometric databases will attract on-going concerns about the security, integrity, accessibility and possible unauthorised or unforeseen re-use of registered data, identify theft and fraud and problems in enrolment and use of these systems. **Transparency tools** could offer support but are hardly developed yet.

4.3. Online behavioural advertising

The information economy promotes advertisement financed business models where payment for service delivery is organised by 'clicking behaviour'. OBA or behavioural targeting constructs profiles from information provided by users active on the Internet; these profiles are then used to offer personalised advertisements.[143] Information on users is collected and exploited in various ways; the most popular at present being the use of so-called 'cookies', small text fragments stored in users' computers that are used to gather information about surfing behaviour and to create user profiles. Another method is just-in-time contextual advertising based on 'live' user search patterns without storing cookies at the user's computer.

Exact figures on the size of the OBA market are scarce and divergent. According to eMarketer, the behavioural targeting market is expected to grow from $750m in 2008 to $4.4bn in 2012.[144] Behavioural advertising gets an ever larger part of the overall advertisement market, growing to 24% in 2012.[145] However, other sources show that in 2009 OBA accounted for less than 5% of US online advertising.[146] The concerns voiced over OBA include the proper positioning of ads, the need to avoid compromising or irritating situations for the consumer and privacy.

As mentioned earlier (see Chapter 2), cookies received heightened attention in Spring 2011 due to the May 25th implementation date for the revised ePrivacy directive (2002/58/EC). At this date Member States should have implemented the new directive, including measures regarding data breach notification, spam and cookies.

A 19 July 2011 European Commission press release identifies seven countries that had implemented the Directive in full: Denmark, Estonia, Finland, Ireland, Malta, Sweden and United Kingdom.[147] A study in the Netherlands on the effect of the old ePrivacy Directive (with less stringent measures on consent and choice related to cookies) showed that about half of consulted organisations fell short in of required privacy safeguards.

---

[143] ool *et al.* (2011).

[144] http://www.marketingcharts.com/direct/behavioral-targeting-ad-spend-poised-for-growth-with-help-from-online-video-5019/ (visited 6 July 2011).

[145] Other researchers argue that market share of OBA will remain modest and will not exceed 7% in 2014 of total advertisement revenues in the USA. See http://cyberlaw.stanford.edu/node/6592 (visited 3 November 2011).

[146] Mayer (2011).

[147] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/905&format=HTML&aged=0&language=EN&guiLanguage=en (visited 22 August 2011).

The need to request informed and explicit consent prior to placing cookies was considered to be detrimental for business opportunities. The Netherlands' parliament adopted the ePrivacy Directive by the end of June 2011 and accepted the revised version which requests those who place cookies to obtain prior informed consent, i.e. a) provision of clear and complete information to consumers consistent with the Dutch data protection act and b) obtaining user consent for storing and reading cookies.[148] The revised version adopted by the Dutch Parliament also states that storing and reading information on end users' equipment may be considered to be an act of processing of personal data. The UK accepted the 'cookie law' but the government informed companies that it would only start enforcing the law after one year had elapsed and that it prioritised finding a business friendly solution over direct enforcement.

Tensions in behavioural targeting fall in the following categories:

Emerging technologies

Technological innovation in networks, data collection and storage techniques point in the direction of greater variety in technological means that 'can do the job'. Essentially, as the commercial value of data increases, techniques to gain access to and control of (personally identifiable) data are becoming more sophisticated and technically complicated. The successor to the current HyperText Markup Language, HTML5, will improve access to and use of web applications but also enable more sophisticated tagging techniques that can be used for commercial purposes, such as behavioural advertising. HTML5 enables storage of cookies on multiple locations at a user's computing device, which can complicate their removal. As a proof of concept, a Californian programmer created the so-called 'evercookie,' which restores itself automatically when removed from a computing device (using HTML5) as a demonstration of how persistent cookies and tracking can be even in the face of user efforts. The 'evercookie' is one instantiation of technological progress that points in a direction of increasing transparency for users without effective choice and consent options. An alternative to using cookies to collect personally identifiable (profiling) information is device fingerprinting: a device is uniquely characterised by its determining features, which enables unique identification. No information is stored on the end users' equipment so tracking, etc. become even harder for users to control. This technique is generally perceived as being even more detrimental to safeguarding privacy.[149]

Business practices

The business models that underlie are underneath behavioural targeting and personal advertisements on the basis of cookies are becoming **increasingly complex**.

Many different actors are involved in OBA; website owners and publishers, advertisers, advertisement networks, affiliate networks, media agencies and suppliers of website statistics and other tracking techniques store cookies (themselves or on behalf of others) on end-users' equipment. A Dutch study regarding the effects of the revised Directive found that 40% of consulted organisations receive data (collected via cookies) used for OBA via a third party.

---

[148] Dutch Parliament (2011) Amendment of Telecommunication Act 32 549, nr. 39, 2010-2011, 21 June, 2011, https://zoek.officielebekendmakingen.nl/dossier/32549/kst-32549-39?resultIndex=1&sorttype=1&sortorder=4 (visited 15 October 2011).

[149] Kool *et al.* (2011).

Unlike the former simple model, in which the website publisher is the only actor involved in placing and reading cookies, current advertisement networks make use of aggregated data from a variety of websites. These networks collect data and offer them to advertisers and publishers for offering personalised advertisements;[150] they act as information brokers between advertisers and website owners and handle complex revenue sharing models. It is increasingly difficult for website owners to know which ad on their website is placed by which network and by which method (for example via behavioural advertising or otherwise).

Providers of behavioural advertising currently offer **limited transparency** to consumers. Consumers are usually informed about cookies and the purposes of data collection (if at all) via privacy policies or general terms of use. Consumers can unsubscribe (opt-out) via links in the privacy statement or general terms of use. 'Consent' is in most cases generic (via general conditions or browser settings) rather than an explicit and specific authorisation following provision of information by the entity wishing to store the cookie and prior to storing the cookie. In addition, cookies are often 'respawned' or restored by other (Flash) cookies after users have deleted them.

According to one interviewee time is needed to come with better solutions for privacy friendly approaches in OBA, given the relatively early stage of developments:

> *"The personalized ad sector is one of the new areas of activity with great innovative potential also with regard to privacy. It is still very much an area of research (e.g. predictive analysis) as the benefits of personalization are not fully understood."*
>
> (Interviewee on OBA)

User behaviour

Research shows consumers have limited knowledge and understanding of behavioural advertising and related terms (first and third party cookies, http or flash cookies).[151] When informed, they express concern about surveillance and indicate they would change practices; for instance, almost two thirds express resistance to unsolicited invasion of their computer. Consumers also know little of strategies (e.g. changes to browser settings) that could prevent or reduce cookie storage, or of the consequences of using such strategies. Thus, even when provided with means of self-protection, they lack meaningful choice.[152]

Legal/regulatory issues

One of the main issues in the revised ePrivacy Directive concerns **explicit and informed consent** for storing and reading cookies (Art.5 (3)). The Directive states that storing and accessing information on users' computers is lawful only "on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information about the purposes of the processing". The only exception is cookies that are absolutely necessary for services that users explicitly request.

---

[150] Article 29 Data Protection working Party (2010). *Opinion on online behavioural advertising*. WP171, adopted 22 June 2010.
[151] See for example McDonald and Cranor (2009 and 2010), Alreck and Settle (2007) and Turow *et al.* (2009).
[152] Kool *et al.* (2011).

Implementation of the revised Directive remains a matter of fierce debate. The Article 29 Working Party opinion on OBA (Opinion 2/2010, pp13-14) suggested that browser settings do not necessarily provide sufficient means to obtain informed consent. At that time, three of four major browsers (the opinion does not specify which) accepted cookies by default; users therefore do not choose to accept cookies in a meaningful way. The Article 29 Working Party also expresses concern over the increasing use of flash cookies that restore deleted cookies.

Approaches/solutions

A number of approaches can be identified that counter these tensions.

Implementation of the revised ePrivacy Directive involves implies that parties have to take into account **new regulations** concerning unsolicited use of cookies. End-users must be offered information about the entity wishing to place the cookie and the cookie's intended use, an explicit **opt-in** before cookies can be stored, and an **opt-out** at any point. Discussion currently centres on such issues as the conditions that must be met if browser settings are to provide a legally acceptable way to indicate acceptance of cookies.[153] The Article 29 Working Party opinion on OBA suggests that requiring both prior consent and periodic renewal (consent to storage has a limited lifespan) may evoke technological innovations which are more in line with privacy safeguards (such as headers that include the expiry date of the cookie).

Another alternative under development involves various so-called **Do-not-track (DNT) technologies**. Some new or updated browsers[154] now contain a 'DNT button'. These are not without problems; they must be included in browser settings and must be able to differentiate between various kinds of cookies offered. Another browser offers Tracking Protection Lists that allows the user to create lists of sites and third party advertising networks to block. DNT covers all sorts of tracking, including device fingerprinting.

However, the operational meaning of Do Not Track is unclear. It may mean that all data collection stops (a common consumer misconception), that data should not be processed or used data (e.g. for behavioural advertising) or that the individual should not be identified.[155] For the moment, Do Not Track practice is not standardised and there is no obligation for websites to offer it to users or follow Do Not Track instructions. Another unsettled issue is how long Do Not Track should last. Both the European Union and the FTC have called for the development of standards on this issue.[156] Consumers should still have the choice to opt in. The US introduced a 'Do-not-track-me-online' Act in the House of Representatives February 2011[157] to increase consumer control and choice. This proposed law complements a private initiative by a number of US companies who agreed an Advertising Option Icon: ads produced by behavioural advertising techniques are accompanied by an icon that gives access to information[158] about how the ad was produced and offers an opt-out.

---

[153] The regulations specifically apply to third party cookies. As noted above, first party cookies necessary for providing explicitly requested services are exempt from the need for explicit consent.
[154] Not currently including either Google (Chrome or Android browsers) or the European Opera Browser.
[155] Soltani (2011).
[156] Kroes (2011a).
[157] http://blog.seorevolution.com/2011/02/12/do-not-track-me-online-act-introduced/ (visited 8 July 2011).
[158] Note that 5(3) of the ePrivacy Directive is not limited to cookies; it covers any third-party storage of information on users' devices including e.g. malware (such as viruses, worms, keyloggers, etc.).

A similar initiative has been developed by industry organisations in Europe.[159] They offer a first step towards more transparency for users, but are probably not sufficient to comply with the Article 5(3) of the ePrivacy Directive.

The Directive might also restore well-established (though arguably less effective) means of influencing consumers by placing advertising on websites or pages visited by users without the use of stored cookies. This so-called just-in-time contextual advertising enables website owners and advertisers to serve ads on the basis of contextual analysis of the web pages visited directly.[160] The precision and effectiveness of this approach might be improved by the use of structured sequences of web pages which implicitly record users' prior behaviour by offering slightly different versions of the same page only reachable by specific clickstreams. In this way, the commercial advantages of cookies can be retained while minimising problematic privacy implications.

Another approach is to inform users by presenting transparent **privacy policies** indicating what is to be collected and for what purposes before the cookie is placed or the information collected. On the other hand, current privacy policies are lengthy and difficult to read and primarily designed to minimise liability for the company. The pre-emptive and possibly repeated presentation of such policies would make the use of websites more cumbersome and intrusive, and would likely reinforce users' existing propensity to believe their privacy is assured whenever a privacy policy is present.

Radically different technical solutions under development include for instance techniques based on the so-called **contextual integrity** approach developed by Helen Nissenbaum and her colleagues.[161] It involves basing privacy rules on the norms and expectations appropriate to different environments, in the process making users much more aware of the context in which data are communicated and offering alternatives to storing information at the user's location regulated through the browser itself.

4.4. Location based services (LBS)

Services based on geographical position provide one of the more challenging sources of tension between Internet innovation and privacy. The informational dimension of privacy clearly extends to spatial components as well. Methods of determining users' geographical location include: satellite networks (Global Positioning System, GPS); mobile phone networks (GSM networks in Europe); Wi-Fi networks (where IP addresses are linked to specific locations); and combinations of these approaches. For instance, mobile phones connect through fixed base stations; the accuracy with which mobiles can be localised is high in densely populated areas with many base stations but diminishes in rural area with fewer and more scattered base stations. GPS provides very accurate locational information (within a few metres). Combining technologies and using triangulation (correlating positional information from various sources) can greatly improve location determination of a device. Privacy implications are of various kinds depending on locational accuracy and the data collected. Even the mere spatial coordinates of a specific individual *may* invade privacy if not properly used.

---

[159] http://www.youronlinechoice.com (visited 12 November 2011).
[160] Anagnostopoulos *et al.* (2007).
[161] "Contextual integrity ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within it." Barth *et al.* (2006).

On the other hand, aggregated or anonymised information (for instance traffic information combining data on the movement of travellers' mobile phone signals with signals from navigation tools) need not necessarily reveal individual travellers' locations.[162] In another development GPS-enabled cameras (including smartphone) are frequently used for geo-tagging of photos (even by default) and other applications.[163] Combining (mashing) geo-data with other data on specific sites creates 'recombinant' information of use to a larger community ranging from sharing information and opinions about points of interest to publishing locational and other personal data about offenders on public sites. The central point is that the inclusion of locational data can greatly increase both the positive and negative implications for data subjects by facilitating 'real world' contact.

A well-known specific class are the locational photo and video services are offered by Google and other companies.[164] Given the predominance of Google in this field many complaints of privacy violations were related to their Street View service. Among them:

- Complaints of privacy invasion through use of cameras mounted high enough to 'see' inside gardens and houses (Japan and Switzerland);[165]
- Demands to blur faces of individuals and car number plates in order to prevent recognition (Germany and Switzerland);[166]
- Requests to blur number plates and buildings in sensitive areas (Switzerland);[167]
- Request to introduce opt-outs for those wishing not to have their homes identified on Google Street View (Germany);[168]
- Collection and storage of Wi-Fi networks data during Street View recording; over 600 GB of data were collected between 2006 and 2010, when the practice became publicly known. According to Google, this collection was the result of faulty software and there was no intent to use or share the results;[169] and
- Long retention periods for unblurred material; the Article 29 Working Party urged Google to reduce retention for this type of material from one year to six months.[170]

---

[162] http://www.physorg.com/news11632.html recent initiatives in this field show China having plans for large scale traffic monitoring through mobile phones around Bejing in order to reduce congestion. http://www.fastcompany.com/1733470/china-to-control-traffic-population-flow-with-cell-phones (visited 8 July 2011).

[163] http://www.wired.com/gadgetlab/2008/05/how-to-geotag-y/ (visited 8 July 2011).

[164] Microsoft for instance has recently launched its service Street Side, which will focus on urban areas. Microsoft wants to combine its street view services with contextual advertising and other localised information. http://www.bbc.co.uk/news/technology-13047454 (visited 8 July 2011).

[165] http://news.bbc.co.uk/2/hi/technology/8049490.stm (visited 8 July 2011);

[166] http://www.theregister.co.uk/2011/04/11/google_street_view_germany/ (visited 8 July 2011).

[167] http://www.theworld.org/2011/05/google-street-view-under-scrutiny-in-switzerland/ (visited 8 July 2011)

[168] http://www.dw-world.de/dw/article/0,,6133854,00.html (visited 8 July 2011). Over 244.000 German residents indicated they wanted to use the opt-out option. Other countries are following suit such as the UK.

[169] http://www.associatedcontent.com/article/5929058/google_street_view_scandal_heats_up.html (visited 8 July 2011).

[170] http://www.edri.org/edrigram/number8.5/article-29-wp-google-street-view (visited 8 July 2011).

Tensions related to LBS and privacy can be categorised as follows.

Emerging technologies

New technologies are emerging that allow **precise positional location** of an individual (or at least of a device belonging to the individual) to within a meter.[171] Combinations of identifying and location tracking technologies (e.g. mobile GSM-based technologies with GPS technology, Wi-Fi locators and RFID networks) allow locational determination and tracking of individuals over space and time. **Geo-tagging** (e.g. photos and videos) is increasingly used, sometimes in combination with Internet services. Publishing locational data on the Internet extends access to private spatial data to a larger community.

Business models

Business models in location based services are based on **enriching available data** by adding additional, complementary categories of information. Equipping existing devices (cameras, mobiles, etc.) with location identifiers enables a new range of services that are interesting from a business perspective but that may endanger privacy by revealing individuals' **spatial whereabouts**. Sometimes these data are aggregated and sold to interested third parties. This does not necessarily infringe privacy, for instance when anonymisation or aggregation prevents identification of subjects. One case that received public attention involved a Dutch provider of navigation devices which sold its aggregated and anonymised data to (among others) the Dutch police[172], who used them to place speed traps. The Chief Executive Officer (CEO) of the Dutch firm promised to reorganise its services to prevent this possible use of the aggregated data because its clients (individual drivers) do not want their driving behaviour to be used to identify hot spots for speeding.

User behaviour

Data with location components have been used to generate profiles that can be used to **narrowly locate individuals**, leading to **loss of control** and **lack of choice**. The Data Retention Directive obliges service and telecom providers to store traffic data for a specific period of time - but only for law enforcement purposes. The relatively high number of German citizens choosing to opt out of Google's Street View services (see p. 78) shows that individuals prefer having choice. More generally, surveys show substantial privacy awareness in respect of location-based services; a recent study revealed that about 55% of those currently using location based services are concerned about loss of privacy;[173] 45% of 1645 surveyed people indicated that they feared burglary because thieves might know when they were away from home.

---

[171] In Europe these services will be offered through the Galileo-system, the European 'alternative' for the US-based GPS-system. Part of this system is the GMES (Global Monitoring for environment and Security) system. See http://www.gmes.info/ (visited 26 August 2011).

[172] http://www.engadget.com/2011/04/27/tomtom-user-data-sold-to-danish-police-used-to-determine-ideal/ (visited 8 July 2011).

[173] http://www.readwriteweb.com/archives/survey_over_half_of_location-based_services_users_fear_loss_of_privacy.php (visited 8 July 2011).

Legal/regulatory issues

As mentioned above, a number of legal tensions are related to the Street View services offered by Google. The Swiss Court of Justice ordered Google manually to **blur all faces** if necessary, considering privacy of those portrayed to have been invaded since no specific permission was requested. The issue remains unresolved; Google has announced its intention to take the case to the higher court.[174] Other courts have ruled differently; in the UK invasion of privacy was weighed against the effort requested from Google, effectively endorsing Google's announced intention to improve its practices and to use automatic blurring techniques. The German courts requested Google to introduce specific opt-outs and to use face-blurring technology. The different responses of national courts to similar practices under an ostensibly uniform law show the fragmented nature of national approaches to European directives. This challenges equal treatment and the Single Market; citizens experiencing similar privacy invasions will be protected differently in different European countries while service providers face additional complexity when rolling out specific services throughout Europe.

Returning to the broader theme of location-based services, regulatory requirements tend to favour **opt-in regimes** (as with cookies) for provision of telecommunication services based upon positional information. Users must be able to **withdraw consent** to the collection and processing of location information costlessly at any time.

In addition to the requirements of the ePrivacy and Data Protection Directives, an interesting additional feature is presented by the Data Retention Directive (2006/24/EC). This regulates mandatory storage of traffic and location data concerning both legal entities and natural persons and of the related data necessary to identify subscribers or registered users. Location and traffic data need to be stored by service and network providers in order to ensure their availability for investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

The European legal framework concerning the various regulations on location based services is very complex, as is noted in a FIDIS (Future of Identity in the Digital Society) report. The report concludes that the three European Directives referred to above: partially overlap; use **different definitions** of personal, traffic and location data; and put the regulatory burden on the shoulders of LBS providers.[175]

Approaches/solutions

Some approaches and solutions can be identified that help restore the balance between privacy infringements and offering privacy safeguards.

Due to public concerns and juridical rulings, companies have resorted to **soft self-regulatory measures** such as offering **opt-out** in case of Google Street View. These measures are not enforced by law (though court decisions have played a role) and can be changed by the company at any moment. Moreover, while they typically reflect public pressure and legal or regulatory decisions in only a subset of markets (though possibly the most important ones) for various reasons they may be applied throughout Europe.

---

[174] http://article.wn.com/view/2011/05/11/Google_Appealing_To_Higher_Court_Over_Swiss_Street_View/ (visited 8 July 2011).

[175] http://www.fidis.net/fileadmin/fidis/deliverables/fidis-WP11-del11.5-legal_framework_for_LBS.pdf (visited 8 July 2011).

Control instruments are available to individual users, such as **switching off GPS** or purchasing devices without GPS capability but location-based services almost by definition require at least temporary identifiable location information.

The main issues in this respect are whether such data are stored in the user device and whether they can be reused by third parties. Control instruments for such applications are not yet readily available despite the increasing use of geo-tagged information.

New technologies that may be used to safeguard individual privacy are emerging such as **automatic face blurring techniques.**

4.5. Cloud computing

In contrast to the location-based services just discussed, many of the privacy concerns around cloud computing stem from lack of geographic fixity. A logical link can be made between cloud-based data aggregation and the automated identification common in Financial Services: the company rapidly matches data in multiple databases and profiles to determine whether a card is likely to have been compromised. Such services point the way to an enormous range of possibilities that may be offered in the cloud.

Cloud computing is defined by the US National Institute of Standards and Technology as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources".

Cloud computing is expected to grow from a $68 billion market in 2011 to $150bn in 2014.[176] Growth rates are thus in the double digit domain (with a 16.6% growth from 2009 to 2011). The US share of the worldwide cloud services market is expected to fall from 60% in 2010 to 50% by 2014, while Western Europe's share is anticipated to grow from 24% in 2010 to 29% in 2014. Cloud computing is generally provided following one of three 'architectures': infrastructure as a service (IaaS), platform as a service (PaaS) or software as a service (SaaS).[177] Some successful examples of each can be provided: Amazon Web Services as IaaS, Google Apps Premier as PaaS and Facebook and payments and accounting handling such as PayPal as SaaS. Clouds also follow various deployment strategies: private cloud services provided to trusted users in single-tenanted environments; public cloud services offered to multiple, multitenant clients wanting shared-cost elasticity and accountability[178]; and various hybrids.

Currently, cloud computing adoption is principally driven by four factors:

- Cost reduction: computing costs are reduced as a result of sharing resources, exploiting economies of scale and eliminating overhead and duplication;

[176] Data from Gartner Group website: http://www.gartner.com (current as of 12 August 2011).

[177] IaaS providers offer computing resources (e.g. storage and processing) hosted via virtualisation - customers deploy and run their own software stacks to run services (e.g. Amazon EC2); PaaS provides a software platform on which users run software provided by them or by third parties (e.g. Google Apps engine, SalesForce Apex language); and SaaS involves applications hosted and delivered online via a browser that provide traditional desktop functionality (e.g. Google Docs, Gmail or MySAP).

[178] Public clouds are similar to 'utilities' but (at the moment) are more competitive, do not have a duty to serve, and typically offer a wider range of quality of service and pricing.

- Cost accounting: shifting computing costs from Capital Expenditure (Capex) to Operating Expenditure (Opex) increases flexibility (companies only pay for the services they need when they need them and can rapidly scale up capability on demand), reduces entry barriers (small firms can gain access to state of the art computing without the need for up-front investment), limits of capital obsolescence and moves risky specific technology assets off companies' books;

- Faster innovation and time to market: for users, access to off-the-shelf computing services reduces procurement and test cycles, while for developers and service providers the cloud gives immediate access to a large critical mass of potential customers with low costs of trying new services; and

- Green objectives: pooled resources enable use of centralised and more energy efficient data centres and efficient energy supply strategies.

Privacy and security concerns are creating new markets and services, becoming key features of product offerings. According to Forrester, 'security as a service' is predicted to become a $1.5 billion market by 2015. Although a 2009 study found half of respondents planned to avoid the cloud because of security concerns, by 2015 security is expected to be a principal driver of this technology.[179] This evolution promises to challenge the business models of those currently dominating the non-cloud security market; as the Forrester report puts it, this development will "challeng(e) traditional security solution providers to revamp their architectures, partner ecosystems, and service offerings" (Penn, 2010). Current market developments are reflected in prominent advertising campaigns by main cloud providers, and include prototype solutions such as HP's Cells-as-a-service or IBM's Virtual Machine Introspection service.

As for privacy, it remains to be seen whether good security will come at the expense of being locked into one provider and whether existing legal roles match the realities of the cloud's fluid and indirect relationships.

Tensions in cloud computing fall in various categories:

Emerging technologies

Cloud computing is not a new phenomenon but rather constitutes an **evolutionary approach** to shared use of IT resources common in other paradigms such as Service oriented Architectures (SoA), off shoring and outsourcing, data mashing and Web 2.0 functionality.[180] Compared to traditional IT outsourcing, cloud computing fundamentally changes the way organisations and individuals allocate responsibilities for data handling and provision of infrastructure, platforms and services.

[179] In other words, cloud service providers able to offer users assurance of security and privacy will enjoy an advantage in attracting subscribers and monetising their presence, while those providing privacy and security services over cloud platforms will attract the custom of users unconvinced by platform providers' assurances, unwilling to pay the price charged or those with niche security and privacy needs.

[180] Robinson, Schindler *et al.* (2010).

While traditional IT outsourcing typically involves negotiated fixed-term contracts for narrowly specified data storage and processing facilities, the quantity and even quality of cloud-based IT resources may fluctuate – often rapidly and dynamically in response to demand. Moreover, the geographic location of data is neither fixed nor transparent and (standard-form) contracts are signed via a routine online process.[181]

Business practices

Cloud solutions are **transforming sectors** such as aviation. The Air Transport Industry (ATI) Cloud, launched June 2011[182], is designed to provide premium IaaS, PaaS, desktop and SaaS applications and services to all stakeholders in the air transport industry. Through the combination of regional and airport based data centres, the ATI Cloud aims to provide end-users around the globe with simple and reliable access to a large catalogue of applications. The ATI Cloud is expected to bring considerable cost efficiencies and savings, and to provide complete compliance with all industry standards and consistency of performance service levels of air transport industry end-users around the globe. It is expected to improve agility, providing on demand access to applications and services based on workplace and business profile. Envisioned as a holistic concept, it is designed to serve a variety of domains including engineering functions, passenger booking, retail and logistics.

A recent study by researchers at the Queen Mary University of London, School of Law, highlights serious concern regarding the available **Terms and Conditions** for cloud services.[183] Problems arise on applicable law and jurisdictions, arbitration mechanisms, variations of contract terms, issues related to data integrity, data preservation, data disclosure, data location/transfer, rights over services/content, property rights and duties, warranty and liability schemes and service availability agreements. Concern is also expressed about the distinction between big players able to negotiate good terms and conditions and the smaller players who have to accept whatever is offered without much negotiation space. At this moment it is not clear whether such formal asymmetries will prevent SMEs from exploiting innovative capacities hidden in the cloud or whether they will take up cloud computing anyway.

User behaviour and perception

One tension already articulated concerns **user expectations** of privacy in the cloud. As has been indicated, real user behaviour may differ that expressed in surveys or revealed in other contexts. For instance, the gap between Willingness to Pay and Willingness to Accept highlights the potential valuation of chances to surrender control over personal data in return for valued services. The Facebook incidents already mentioned show users to be aware of privacy issues, which are factored into adoption and precaution decisions along with: user friendliness; ease, speed, reliability and quality of services; and ubiquity of user access. Reactions to cloud computing outages (e.g. breakdown of webmail services) show that users have high expectations for service continuity. Indeed, these may be unrealistically high, given the complex environment in which cloud services may operate. Facebook faces the integration of more than 1.000 websites every day, and sees users installing 20 million applications every day.

---

[181] Bradshaw, Millard et Walden (2010).
[182] http://www.sita.aero/content/air-transport-industry-cloud-becomes-reality-sita-launches-first-services-customers (visited 3 November 2011).
[183] Bradshaw, Millard and Walden (2010).

Businesses need to weigh expected interests of users in tuned services (based on profiling information that may come from various sources) and the desire of users to shield complete transparency from any business party. Transparency tools could help in finding the proper balance but are seldom offered. It is worth noting that these expectations cannot easily be reversed; because service interruptions are more immediately noticeable than privacy infringements, quality of service concerns may effectively outweigh privacy concerns, even if both are valued by users in the abstract.

Another issue that users put forward is **data portability;** together with interoperability it implies that data exchange between competing or cooperating services should become easier. Initiatives such as Google's Data Liberation Front – which is creating tools to facilitate users' movements of their data in and out of Google products – show that providers understand the commercial and other value of data portability as compared to lock-in. For users, clouds are hard to understand and issues such as data portability are not yet perceived as being part of ordinary business deals. Still, there is evidence that users employ a variety of strategies to shield their personal data and the resulting profiling information.[184] 'Whitewalling' (clearing one's site regularly) and 'social steganography (hiding real information that only can be understood by those 'in the know' amid publicly available information) are two of the strategies identified. Of course, to the extent that privacy protections are – or are perceived to be – specific to providers, jurisdictions and technologies, data portability can heighten privacy concerns (for good or ill).

Legal/regulatory issues

The definition of data controller and data processor receives renewed interest. The Article 29 WP has issued an opinion paper on the definition.[185] Relevant issues are what constitute controllership in a cloud context and whether it is necessary to differentiate consumer to consumer (e.g. Facebook), business-to-consumer (e.g. Google Apps) and business to business (e.g. SAP's Business cloud) arrangements.

It is not clear whether customers are able to exercise informed **choice and consent** over data stored in a cloud. In 2009, Facebook angered many users by – ostensibly in response to user feedback – incorporating a range of new privacy controls, but making many types of content public by default.[186] More recently, Facebook introduced a further potentially privacy invasive practice by enabling facial recognition software to automatically 'tag' (identify) friends in uploaded photographs. Concerns are phrased against the possibility that without someone's explicit consent photos will be tagged by others, thereby increasing transparency but reducing control, choice and consent.[187] It also announced introduction of new services that would reveal commercial interests of its consumers, hoping this might trigger similar interests by friends (and friends of friends).[188] (About a year ago, it was indicated that Facebook breached its own privacy policy in its top ten applications by sharing information on user IDs and other information in any of its 550,000 applications.

---

[184] Boyd (2010).
[185] Article 29 Working Party (2010).
[186] http://www.guardian.co.uk/technology/2009/dec/10/facebook-privacy
[187] See http://nakedsecurity.sophos.com/2011/06/07/facebook-privacy-settings-facial-recognition-enabled/ (visited 4 July 2011).
[188] http://www.nytimes.com/2011/09/23/technology/facebook-makes-a-push-to-be-a-media-hub.html?_r=2&ref=technology (visited 3 November 2011).

Though it was argued that Facebook could not be blamed for this leakage, it is a manifestation of the problem of both (lack of) informed choice and consent and of the formal notion of data controller in this respect.[189]

The concepts of **ownership and confidentiality and** the role of **law enforcement** are problematic in cloud computing. Data ownership will usually be settled in contractual terms. By sharing and pooling data and collecting, aggregating and enriching them using other sources, ownership may become blurred, especially when data collected at a location falling under a specific jurisdiction are subsequently enriched with data stemming from a location under another jurisdiction. This creates problems in identifying or agreeing the applicable law.[190]

Approaches/solutions

The tensions mentioned above have their counterpart in approaches that try to lift these tensions or that are aimed at preventing other tensions.

Offering services through the cloud challenges safety, security and continuity of services. Security measures may be directed towards 'anti-identification' measures as well, to prevent unwanted data linkages. **Strong encryption** can ensure data protection and privacy in the cloud. By requesting a password, a token and a personal identifier (which could be a biometric feature) one can increase the level of protection against unwanted intrusions and/or misuse of stored data in the cloud. Progress has been made in uploading encrypted data into the cloud and even allowing cloud service providers to perform computation and searches without the need or the opportunity to decrypt the stored data. Current encryption techniques are however still quite expensive in both computation and bandwidth and show little sign of becoming practical.[191] A recent study by the European Commission shows many organisational factors hindering the uptake of Privacy Enhancing Technologies such as encryption and anonymisation. The report mentions perceived lack of benefits, perceived limited usefulness, direct costs, long term costs, lack of awareness, lack of consumer demand, refusal of consumers to pay for PETs, lack of political imperative, lack of enforcement, as some key issues that hinder widespread diffusion of PETs into data services.[192]

Some EU-funded projects call for a **federated, virtualised e-infrastructure**, in consortia of public and private providers, focusing on a variety of security techniques.[193] The move from IaaS towards PaaS and even SaaS is not straightforward, however, and loss of coherence amongst the main actors may be detrimental for the overall outcome of these approaches. At the same time, federation may reinforce 'privacy monocultures' leading to dangers of lock-in and the potential for small breaches to spread rapidly. As one interview emphasised, the need for standardisation is apparent in cloud computing as well.

[189] http://nakedsecurity.sophos.com/2010/10/17/facebook-apps-leak-data/ (visited 4 July 2011).
[190] Robinson, Valeri and Cave *et al.* (2011).
[191] Ryan (2011).
[192] London Economics (2010).
[193] SIENA consortium (2011).

"Cloud Computing highlights the need for global standards"

(Interviewee Cloud computing)

When looking at major companies, one has to conclude however that attention for privacy measures is still quite limited. The Apple Software Development Kit for its iPhone Operating Services, for instance, only pays marginal attention to security measures that can be taken to shield and protect personal data.

5. KEY FINDINGS AND RECOMMENDATIONS

KEY FINDINGS

- The evidence derived from our research leads to ten conclusions (Section 5.2).
- Overall, we find that Internet innovation and privacy are not in balance, with an increasing tendency to invade privacy associated with new and emerging Internet technology, business practice, product and service innovations.
- These Internet innovations are increasingly interwoven and integrated and reliant on use of personal data. The associated promise and threats lead in turn to new developments; but privacy-intrusive Internet innovations dominate over privacy protection.
- New business practices use personal data as the new oil - both a valuable resource input and a store of value whose benefits different parties struggle to control. They increasingly extend to spatial and corporeal/cognitive dimensions ("Where are you", "Who are you?").
- User awareness is limited. Understandable and practicable privacy-friendly policies are rarely deployed, not as effective as their marketing would suggest and largely confined to niche markets.
- Hard regulatory measures are needed to restore and sustain a healthy balance. Soft regulation (including self- and co-regulation) is sometimes tried and may be preferred on the grounds of cost and potential effectiveness but are not always accepted or complied with by the relevant business sectors.
- We propose 12 different recommendations for: privacy rights and responsibilities; rules and regulations; and coping with change.
- These are concerned with: legislation and regulation; emerging technologies; business practices and user behaviour.
- They also take effect at different levels: global issues; European issues; Member State; companies; and individuals.
- The privacy rights recommendations include a dual construction of privacy as an economic as well as a human right and proposals for reassigning liabilities intended to facilitate the ability of the Internet ecosystem to deal with new privacy issues as they arise.
- The governance recommendations range from hard regulation to self- and co-regulatory options designed to be better suited to the dynamic nature of Internet innovation and the increasing economic value of personal data without undermining respect for privacy as a fundamental human right.
- The recommendations for coping with change are intended to balance necessary flexibility with a 'future-proof' stance intended to provide the regulatory certainty needed to encourage beneficial innovation.
- The importance of global issues must not be under-estimated as this report has demonstrated many of those companies innovating are based outside of the EU – in particular the increased efforts to achieve convergence between EU and US approaches is worthwhile in this regard.

5.1. Introduction

This section summarises our main findings regarding the relationships between Internet innovation and privacy described in detail in the preceding Chapters. In particular, some generic lessons can be drawn from the empirical material in Chapters three and four. The conceptual frame considers the two-way relationship between Internet innovation and privacy. The relationship is both very intimate and highly dynamic; it is usually inappropriate to consider only one causal direction; rather, we refer to the *mutual shaping of technology and society*.[194] The empirical material evidence amply demonstrates this reciprocity, summarised in Section 5.2 as a set of conclusions that highlight the main thrust of our findings.

We then present a set of recommendations to the European Parliament for options to explore. The recommendations extend the arguments presented in this study in directions the study team considers fruitful for tackling the manifold challenges identified here.

5.2. Conclusions on privacy and Internet innovation

Throughout the study the relationship between privacy and Internet innovation has been described using the dimensions identified in the conceptual framework: emerging technologies; business case; user perspectives; and legal and regulatory approach. Each shows its own specific set of tensions with regard to privacy and innovation. The five cases illustrate this relationship in terms of current concrete developments. Each shows a wide variety of technological, business process, service and institutional innovation related to the Internet and demonstrates how these innovation processes are more often than not entangled and integrated. Our focus on the privacy implications led to the identification of specific issues and challenges, detailed in the following ten conclusions.

5.2.1. Generic conclusions

All cases studied demonstrate the mutual relationship between privacy and Internet innovation, especially via the positive and negative privacy impacts of innovations in regulation, regulatory, technologies, business practices and user involvement.

Conclusion 1: Negative impacts of innovation on privacy outweigh positive ones

A first conclusion is that current innovations are more likely to infringe upon than to protect the privacy of users. This is markedly true of the technologies and business practices in the cases studied.

The two main drivers are the increasing potential to capture personal information and the increasing value that can be realised by its use (often via new business models). Technological convergence and new services make more aspects of human behaviour available in digitised form (spatial data, gene data) to new business processes and services; this hinders easy application of data ownership and control. There are some positive aspects as well but these are more marginal. The balance reflects the tension between the human rights value of privacy and the economic value attached to use of private information.

[194] Oudshoorn and Pinch (2007). Oudshoorn and Pinch (2003).

Conclusion 2: Privacy is a negative rather than a positive concern for innovation practices

The cases also show evidence of the impact of privacy concerns on innovation practices. By and large, user privacy is perceived by businesses more as a cost or liability than as a potential source of value, especially in view of the weakness of user demand for paid-for privacy protection (see below).

Attempts (generally by niche players) to approach privacy more seriously face difficulties in embedding their solutions in everyday practices or in using this to counter the power of dominant players.

The net result is the lack of a positive business case for enhanced privacy protection or user empowerment.

5.2.2. Conclusions on emerging technologies

The empirical material led to the following conclusions concerning the relationship of emerging technologies and privacy:

Conclusion 3: Convergence of different Internet technologies with other technologies exacerbates privacy problems

Several cases show that the dominant dynamics produce more complicated technological infrastructures and a convergence of previously separated technological fields, leading to an increase in technological complexity with detrimental consequences for privacy.

The emergence of cloud computing creates complex relationships between computer networks and servers and thereby complicates assessment of privacy issues. Another example is location based services that make use of different location services (GPS, GSM, Wi-Fi or RFID-based or any combination of these). The convergence of ICT systems with entirely new fields such as genetic profiling in case of biometrics is a third example.

Within the resulting interconnected networks, architectures and service concepts it becomes ever more difficult to deal adequately with privacy issues, because the technological environment is more complicated and induces new modes of gathering, processing and dissemination (a larger variety) of personal data even as it makes it harder to trace, monitor and audit them.

Conclusion 4: Privacy friendly technologies are under development but are not recognized as leading the way

In attempting to counter the privacy threats posed by or expected from widespread use of Internet-based services privacy-friendly alternatives are developed. Examples include privacy-friendly alternatives to dominant social networks. These alternatives are not easily recognised outside a niche market.

Privacy enhancing technologies and tools meant to increase transparency of data processing are under development as well. Unfortunately, they have to serve multiple agendas; addressing user concerns, managing liabilities and exercising real control over privacy threats. They are also hampered by negative business impacts.

Some privacy-friendly technologies have been developed or are being developed in response to user demands for more privacy, such as ‘Do-not-track’ and face-blurring technology to prevent identification. One class of such systems, which can be user-friendly as well, can be found in decentralised biometric identification systems. These examples show that innovative privacy-friendly alternatives are possible but are still marginal.

5.2.3. Conclusions on business practices

Internet innovations extend to business practices, service concepts and new Internet functionalities. The case studies present several examples of these evolving business practices. In relation to privacy the study yields the following conclusions:

Conclusion 5: New business practices tend towards realizing as much profit from data as possible; privacy only offers a secondary incentive

Many new and emerging services make use of personal data. With the on-going evolution and dissemination of Internet technologies the opportunities to develop interesting service and business concepts on the basis of gathered personal data increases.

OBA provides one example: data giving insight into personal preferences, attitudes and characteristics allow companies to offer better tuned services; this in turn may limit consumer mobility. The resulting increase in complexity (in the above example the rewiring of customer/provider relationships) leads to more complicated business environments as well, with complex networks of business partners centring around one business concept.

Cloud computing provides another example in which application providers and cloud users have only indirect contact via the platform provider and may not be able to identify, implement and enforce appropriate privacy processes.

Dealing with personal data in these complicated environments may thus increase potential privacy breaches and violation of privacy. With business profits being tuned towards use of personal data, dealing with privacy becomes secondary.

If it is not necessary or required, companies tend to avoid too much transparency since this may especially be beneficial to their competitors. Even where personal privacy is not at stake, there is a growing trend towards group profiling and targeted use of personal information to unduly influence consumer choice or behaviour for instance by employing targeted communications to obtain access to private information (spear phishing[195]).

Moreover, on-line identities may not correspond to people in one-to-one fashion.[196] Individuals may have multiple on-line personae, and identities used by third parties to provide e.g. address, property, registration and other public profile information may conflate many individuals with the same name. This raises fundamental issues around the adequacy of individual data privacy to encapsulate privacy concerns, 'imprecise identification' and consent (see Bargh, 2002). The practical consequence is fairly straightforward – currently, privacy is framed – in Europe - as an (inalienable) individual right. In future, as with other fundamental human rights, it may need to be recognised as a collective right as well. There may even be a case for considering whether 'co-private' information can be protected in the same way (e.g. when one of the parties reveals something the other(s) might wish to protect).

[195] Langheinrich and Karjoth (2010).

[196] Examples include the use of anonymised data to create 'near-identifying' profiles or the use of e.g. automated tagging in photos to create pseudo-personal data (because the accuracy of the association of the name to the image is not certified by any legal person). A further set of examples (likely to expand in future) arises from the activities of 'information aggregators' who use automated 'scraping' of data from electronic sources to create 'profiles' on the basis of 'mere' names, addresses, etc. (e.g. 192.com).

Conclusion 6: It is difficult to develop new business practices focusing on implementing cost-efficient and profitable privacy-friendly solutions.

It is difficult to turn existing privacy-friendly approaches into viable business propositions. By and large, companies understand their customers' privacy concerns and are willing to take these into account. We found a few interesting examples of new products or services developed with privacy built in from the outset. But these remain the exception (see conclusion 4).

In particular, dominant players were unlikely to adopt comprehensive, effective and understandable privacy solutions; when prompted by user concerns, they are more likely to respond with difficult-to-use privacy options or to offer privacy protections in exchange for access to personal information. This is a joint consequence of the fact that the value of personal data to the firms able to collect such data as part of service provision exceeds data subjects' willingness-to-pay to protect such data. To further develop this conclusion, we turn now to user behaviour and attitudes.

5.2.4. Conclusions on user behaviour and attitudes

Users play pivotal roles in Internet innovation. Increasingly, users are central to the innovation process itself, as co-creator of new services and originators of new ideas. Users develop apps for mobile applications that may be interesting for other users as well. Therefore, it might be hoped that their privacy preferences could be reflected from the outset of product and service development. The study revealed the following tensions with regard to users, Internet innovation and privacy:

Conclusion 7: User awareness of potential privacy infringements due to Internet innovation is low.

We found several examples demonstrating that users largely lack awareness and understanding of the fate of their personal data, what they can do to protect themselves or ways to take advantage of the value these data can command. This is for instance the case with OBA; users hardly understand what cookies are and how to deal with them. Similarly, surveys (dating back to 2005) show low user awareness of the prevalence of RFID, let alone its privacy implications.

Other examples show however that relatively large groups of users will act to protect their privacy (e.g. by opting out of specific services) – when offered a real choice.

One should acknowledge that the technical complexities of services offered (cookie-based services for instance) often make it hard to grasp their full technical implementation or implications and also that such (partial) ignorance may make users prone to snap judgements that in turn discourage providers from overtly addressing privacy issues.

It is also possible to question whether informed consent or choice can or should always be expected from users.

Conclusion 8: Not much effort is invested in offering user-friendly and privacy-friendly systems.

Relatively few cases hint at the development of services combining user-friendliness with privacy-friendliness. Exceptions include decentralised biometric identification systems that shield personal data while offering authentication opportunities – e.g. by allowing people to use anonymised fingerprints to authenticate tickets to public events.

But many other cases show an inherent tension; user-friendliness may come at the expense of privacy-friendliness such as OBA that offers relevant and advantageous advertisements to customers based on reuse of their information. The tension arises in relation to the division of the gains from trade between buyers and sellers.

Privacy-friendly alternatives, such as means for users to withdraw consent that they provided earlier, data portability when changing service providers, intelligible and concise privacy statements or the availability of a meaningful 'menu' of privacy options when accepting a service (instead of a take-it-or-leave-it choice between the default option and rejecting the service) were all too rare.

5.2.5. Conclusions on legal and regulatory issues

The study shows several instances of policy intervention to correct irregularities which confront existing practices. In a number of cases, regulation of specific policy interests (competition, or the fight against terrorism) had immediate negative privacy impacts.

In other cases, inconsistencies between the privacy regulations in different states or between public regulation and industry codes produced gaps or even conflicts. The balance between promoting innovation and safeguarding privacy is a delicate one.

Overall, the study gave rise to the following two conclusions regarding the role of legal interventions and regulations in maintaining the proper balance between privacy and Internet innovation.

Conclusion 9: Safeguarding privacy interests requires policy intervention

The economic incentives for using personal data for providing new Internet services far outweigh those for prudent approaches to using personal data.

The conclusions presented on emerging technologies, business practices and user behaviour reveal the imbalance between the opportunities offered by converging and emerging technologies and emerging new business practices on the one hand and the safeguarding of privacy on the other hand.

Unfortunately, the overall conclusion has to be that legal boundaries and regulatory constraints are necessary in order to safeguard privacy, even considering the possibility that the behaviours and attitudes of firms and citizens vis-à-vis privacy may gradually converge. The incentives for offering privacy-friendly services and refraining from using personal data simply are not strong enough to safeguard individual privacy. This is as much the case for private parties that see personal data as a means to improve their businesses as it is the case for public organisations that want to use personal data in the fight against criminality, terrorism and the like.

Recent lawsuits have drawn attention to cases where people surrender privacy rights for protection from threats contained in what would otherwise be considered private communications – the issue in this case is whether consent to spam protection can implicitly entail consent to third-party scanning of email contents for commercial purposes. As a consequence, data subjects are likely to become (or remain) overly cautious, while data users are likely to continue to 'push the envelope.' This can be seen to some extent in the contrast between the demand of consumers for regulatory protection and their modest willingness to pay for privacy services or to adopt privacy-aware changes in online behaviour.

Beyond this the operation of market forces in ensuring consistency are hampered by national differences, though these can be surmounted; data exchanges between the EU and the US – which would otherwise have been hampered by the unavailability of 'equivalent protection' in the US – were made possible via 'safe harbour' arrangements. These arrangements also offer a potentially fruitful way of proceeding within the EU, especially when differences in national approximation of data protection (and other privacy rules) could impede the free movement of data within the 'Digital Single Market' or when the development of new technologies, business models and services raise privacy issues not wholly resolved within the contemporary legal and regulatory framework. It is noteworthy that the Safe Harbor agreement is essentially co- (rather than self-) regulatory and thus falls between the US approach which regards privacy as an economic right and favours self-regulation and opt-out and the European construction of privacy as an inalienable and fundamental human right requiring formal legal protection and opt-in.[197]

The agreement was concluded between the EU, the US Department of Commerce and various industry and NGO representatives and is based on adherence to seven clear principles.[198] Participation by US firms is voluntary, but enforcement of the conditions (ensuring that they offer protection equivalent to that provided by their EU counterparts) is provided by the US Federal Trade Commission.[199] Evidence on the effectiveness of the agreement and the extent to which formal government participation is required is mixed.[200]

Conclusion 10: Self-regulation is sometimes used but is not easily achieved

Some degree of soft regulatory measures can be found, but their usefulness is hard to demonstrate. Co-regulatory (not self-regulatory) arrangements in which industry codes and standards are enforced by regulators (e.g. RFID PIA Framework) can benefit from higher levels of compliance and greater technological awareness, but may be prone to 'creep' or used to limit competition. In the case of the RFID industry, self-regulation involved additional issues (e.g. security, standards, interoperability) in addition to privacy. In other situations, individual firms changed their behaviour in response to user demand and/or the threat of potential regulation (e.g. Google Street View changing from opt-out to opt-in) thereby lowering the threshold for users to exercise choice and control.

But the same negative business impact that frustrates the growth of a market in privacy services limits the scope and effectiveness of pure self-regulation. In the case of OBA, for instance, acquiring as much data on personal preferences and personal profiles is central to offering the best advertisements on a personal basis, so privacy protections could reduce profitability – and even the scope for businesses to compete in their ability to meet specific customer needs.

---

[197] See e.g. Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data, Eur. O.J. L281/31 (Nov. 23, 1995) and http://itlaw.wikia.com/wiki/Safe_Harbor_Agreement#cite_note-1.

[198] See http://export.gov/safeharbor/eu/eg_main_018475.asp.

[199] "It is up to either a U.S. government body (e.g., the Federal Trade Commission or the courts) **or** a U.S. self-regulatory body (e.g., BBBOnLine or TRUSTe) to enforce the terms of the safe harbor." (http://itlaw.wikia.com/wiki/Safe_Harbor_Agreement) (emphasis added).

[200] See e.g. Schriver (2002); Leathers (2009) cites heavy criticism of the effectiveness of the agreement on both sides of the Atlantic including the Google-Doubleclick merger case; Leichtenstern, *et al.* (2011) finds widespread violations; and Schmierer (2011) presents a critical legal analysis of the need for formal regulation on top of existing legislation.

Next to these two main conclusions we also noticed that in some cases regulatory practices are influenced by inputs from external domains, such as in case of biometrics and internal security.

Finally, several examples were found in which existing legislation is (perceived to be) ambiguous or in need of clearer and consistent definition of key concepts (such as the definition of personal data, traffic and location data, and the precise meaning of terms such as choice and consent).

5.3. Recommendations

The Recommendations below are grouped for ease of exposition. Of course, the categories overlap slightly. This section briefly describes each group and the overall rationale associated with it. This is followed by a Table that summarises the recommendations, identifies the stakeholders, and relates them to the conceptual framework and the conclusions from which they flow.

5.3.1. Privacy rights and responsibilities

The development of the Internet as a social construct has changed the societal, legal and economic meaning of privacy; this in turn calls for changes in the system of rights and responsibilities needed to provide affective protection without reducing either the ability of Internet users to use the Internet for their own benefit or the power of the Internet ecosystem to devise new solutions to privacy problems.

The conception of privacy embedded in inherited legislation reflects assumptions about the ability of individuals to understand the privacy consequences of their Internet behaviour and to control the positive and negative impacts. To update the concept of privacy without either surrendering legal certainty or foreclosing future evolution, the first set of recommendations call for an enhanced view that recognizes that privacy is: an economic as well as a fundamental right; shared as well as individual; not limited to protection of individual data.

From this perspective, it is possible to argue for changes in liability or responsibility. For instance, as individuals are equipped with tools to monitor and control their privacy, they are better able to take responsibility for protecting their rights; on the other hand, as technical privacy protections become more deeply embedded in Internet systems, they may be less visible to and understandable by end-users; finally, the new services and relationships that have developed on the Internet justify a reworking of the responsibilities of different parties (e.g. as data controllers or data processors).

This change should seek to rebalance the ability, the incentives and the understanding needed to protect or infringe privacy rights, taking full account of the way responsible parties actually make decisions.

5.3.2. Rules and regulations

As a combined consequence of changes to the nature of privacy in the Internet ecosystem and privacy awareness and attitudes, it is necessary both to reconsider privacy rules and to place them in a broader context that includes other attempts to deal with privacy issues and other policies that have privacy consequences. These are particularly urgent in view of the global nature of the Internet and the migration of an increasingly wide range of activities on-line.

As an inevitable consequence, many parties (government, business and civil society) are taking action, and many more forms of policy (e.g. technical, competition, consumer protection, etc.) are seen to have privacy implications. In some cases, these complement privacy rules, e.g. by implementing specific rules for specific circumstances, or by harnessing market forces to enhance privacy); in other cases they may lead to conflict, inconsistency and damaging uncertainty.

In all cases, the interplay of policies challenges existing methods for impact assessment and policy evaluation.

The second group of recommendations addresses these governance issues.

5.3.3. Coping with change

The Internet ecosystem has not only changed the relation between privacy and (technical, economic and societal) innovation; it continues to do so.

The above recommendation categories are primarily intended to catch up with these changes, but it is equally desirable to build in appropriate flexibility to avoid distorting future development and to enable the self-organising and 'generative' Internet to align innovation with privacy advancement.

There is an inherent trade-off between commitment and flexibility; policies that are too vague or too flexible will not provide the assurance needed for beneficial experimentation and innovation; those that are too detailed, prescriptive and inflexible may not deter privacy-invasive practices that bypass the 'letter of the law' and may inadvertently preclude the development of superior technical, contractual or behavioural alternatives to command-and-control laws and regulations.

The third set of recommendations is intended to lead to a framework that differentially encourages mutually beneficial innovation through technologically neutral value-based regulation that provides a clear, consistent and durable framework for deciding whether and how to respond to changing business models, services and Internet-based relationships. This inevitably means extending the current knowledge base as well, so we also make recommendations for exploiting on-going research, additional translational research and new policy-related research to fill current knowledge gaps.

Table 5: Recommendations and relevant stakeholders

Recommendation / relevant level	Stakeholders					Framework level				Conclusion									
	Global	European	Member State	Private Sector	Individuals	Legislation	Business practices	Emerging tech.	User behaviour	1	2	3	4	5	6	7	8	9	10
Privacy rights and responsibilities																			
13. Differentiate economic and fundamental privacy rights	✓	✓				✓				✓	✓			✓		✓			
14. Distinguish graduated privacy rights at the individual and small group level of identification.		✓	✓			✓				✓		✓		✓	✓				✓
15. Extend protections to privacy of action		✓	✓			✓				✓		✓						✓	
16. Clarify consent provisions (esp. regarding technical means for informing and obtaining consent).		✓	✓			✓	✓		✓		✓	✓	✓		✓	✓			
17. Explore means of pushing privacy responsibility up the stack and down the value chain		✓	✓	✓		✓	✓		✓		✓	✓	✓	✓	✓	✓	✓		
18. Incorporate realistic behavioural assumptions		✓		✓	✓	✓			✓							✓	✓	✓	✓
Rules and regulations																			
19. Take full account of other formal and informal privacy regimes	✓	✓	✓	✓		✓	✓	✓										✓	✓
20. Reconcile privacy rules with antitrust, consumer protection, intellectual property and other rules addressing market failure.		✓	✓			✓												✓	✓
21. Take the medium-term coevolution of innovation and privacy into account in Impact Assessment of innovation and privacy policies.		✓	✓		✓	✓				✓	✓	✓		✓				✓	
Coping with change																			
22. Adopt value-based approach that is neutral with respect to technology, business models, services, etc.	✓	✓				✓		✓				✓	✓					✓	✓
23. Implement a 'policy sandbox' for collaborative exploration of new policies.				✓	✓	✓		✓										✓	✓
24. Undertake additional translational and policy-related research.	✓	✓	✓				✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

5.4. Recommendations in detail

5.4.1. Privacy rights and responsibilities

Recommendation 1: *The definition of privacy rights should be expanded to differentiate economic and fundamental aspects.*

Currently, some non-data aspects of privacy - privacy of action or choice (which is threatened by social engineering and by unwanted influence or distraction), personal security (threatened by e.g. cyber-bullying or cyber-stalking), privacy of network access and freedom from Spam - receive little formal protection, in part because their importance was not recognised when the legal framework was devised.

The law primarily protects informational privacy as a human right. But the increasing availability and economic value of personal data combined with the absence of economic rights to data weaken the protection and exercise of data subjects' human rights and economic interests.

An economic right would allow subjects to take control of their data, determining their value and controlling their use. A common foundation would ensure that the protections given to the personal data part of Internet exchange are consistent with those given to (or withheld from) other activities for purposes that the Data Protection rules seek to prohibit. Individuals could exchange rights to collect and reuse certain data for access to other data or Internet services (including e.g. personalised services). Prices could depend on the degree to which the individual is identified or actively involved in managing or shaping the data. This would facilitate negotiated transfers of data rights in which both parties are informed of the extent and nature of the data and the uses to which it may be put are clearly defined and can choose from a meaningful range of alternative 'bundles' of data rights.[201]

The ability to transfer some (but not all) privacy rights can improve the effectiveness of fundamental privacy rights, allowing intermediaries to help individuals to remove data from public and private databases and invest in, shape and market their profiles through selective creation and dissemination of personal information.

Recommendation 2: *A graduated approach to privacy rights should be developed to cope with weak identification and shared privacy*.

Currently, personal data privacy rights are attached to individuals. However, in the Internet environment, there are at least two ways in which this may be inappropriate as noted in Conclusion 5. Identification is not always perfect and some information is 'jointly private' to groups of people. One potential policy approach is a graduated scheme that provides different rights and responsibilities depending on how precisely a person, individual characteristic or group is identified. This could be instantiated in rules resembling those use to protect or the rights or control the actions of other groups, e.g. in relation to prejudice, trespass, etc.

[201] This transition is already in progress; secondary markets have arisen that involve the further processing and reuse of personal data and (more recently) to give individuals paid-for control over their personal data in the Internet domain, but they lack legal foundation.

Recommendation 3: *Privacy protection should be extended to privacy of action*.

Conclusion 5 notes that information is often provided to people in order to influence their behaviour[202]; this may be relatively benign (e.g. subliminal advertising[203]) or harmful (e.g. cyberbullying or cyberstalking) or may 'merely' create a subjective sense of interference, surveillance or insecurity. Present legal protections are relatively weak[204] but more could be done; data protection regulators have tended to regard all data that shapes personal choices as personal data (just as they have concluded that IP addresses are personal data). This is a practical rather than a principled conclusion; until the issues are resolved, it is simpler to retain them than to exclude them.

Extending privacy rights beyond personal data would seem to address this more directly and provide an additional legal basis for measures against other privacy invasive practice.

Recommendation 4: *Consent provisions should be clarified*.

Many existing privacy protections are based on informed consent to data collection, processing and reuse and to the receipt of communications based on those data. Some procedures may be so frequent and specific as to constitute an invasion of privacy in themselves. The user experience can be improved by automated, delegated and/or federated consent provisions, particularly in relation to targeted solicitations; at present, privacy rules come into play only when the information is sufficiently targeted. In addition to rules governing information aggregators and others who collect and redistribute publicly-available information, the practices noted in Conclusion 9 (esp. consent to email scanning for anti-Spam purposes) suggest that the extent, frequency, scope and other attributes of consent should be clarified or supplemented by *ex ante* rules or codes of conduct.

Recommendation 5: *Explore means of pushing privacy responsibility up the stack and down the value chain*.

As noted in the conclusions, Privacy by Design and other ways of 'pushing privacy up the stack' can help to minimise the burdens of privacy protection on users and providers. On the other hand, differences in preferences, competence, etc. suggest that one default approach may not fit all cases and may excessively lock end-users to specific providers. Differentiated solutions may not interoperate, reducing the openness and connectivity of the Internet with no countervailing increase in privacy or security.

---

[202] Thaler (2008).

[203] Bargh (2002) – while subliminal advertising *sensu strictu* is prohibited in the EU http://ec.europa.eu/avpolicy/reg/tvwf/advertising/index_en.htm), various indirect ways of influencing users' behaviour that are not caught by the legal definition have been developed.

[204] Fraudulent messages are to some extent addressed by consumer protection and advertising rules; the UK Malicious Communications Act (1998) criminalised cyberstalking and the United States has a variety of laws concerning cyberstalking and cyberbullying.

There are currently no clear principles balancing privacy responses at different 'levels' or clarifying conditions under which privacy obligations can be contracted out. This lack of clarity may account for the fact (noted in Conclusion 6) that relatively few companies have implemented privacy by design and few PETS[205] have attained any substantial degree of market success.[206] Further clarity around reallocating privacy responsibility could foster more efficient and effective arrangements.

This is not limited to automated or technological solutions. As indicated in e.g. the cloud case study, the data subject, data controller and data processor roles may not be stable or the most efficient locus for responsibilities[207] - especially when technological change places activities that were once the province of (regulated) companies in the hands of individuals.

Privacy rules drafted for companies may not extend to user-generated and user-managed content in ways that are enforceable, effective, efficient, proportionate or likely to further the objectives of the original regulation.

It is not obvious how this challenge should be met; one approach may be to supplement the first recommendation's transparent and flexible system of transferrable privacy rights with a requirement that platform providers make available a menu or an opportunity to negotiate collection and access starting from a suitable default position.[208]

Recommendation 6: *The behavioural and rationality assumptions underlying the rules should be tested against current behavioural science research findings*.

As noted in Conclusions 7 and 8, both legal and economic approaches to privacy assume rational and informed choice – at least as a 'gold standard.' In this respect, the problems considered in this document clearly justify and guide government regulation in some circumstances. But the evidence of rationality is not reassuring.[209] More concretely, individuals may be unable to evaluate or understand privacy choices offered by private firms.[210] Analogously to regulations mandating disclosure (e.g. the Ecolabelling Directive) there is potential scope for a regulation specifying the form and content of privacy policy disclosures, or at least for a minimum standard specified in terms of content and 'usability.'

---

[205] Including those that minimise data collection (thus reducing reliance on legal protections), those that implement legal requirements by giving users control over their data and those that preserve privacy by encryption or anonymisation of collected data before re-use.

[206] Rubinstein (2011).

[207] For example, those providing platforms, or platforms on platforms (like a newspaper's comment facility or Disqus.com) may not be suitable as liable parties.

[208] This is similar to the solution being worked out in relation to the 'cookie law' prior consent provisions, which might be met through users' browser preferences if initially set to reject cookies by default or if those preferences must explicitly be set during installation.

[209] They show persistent differences between individual willingness-to-pay and willingness-to-accept (strong reference position or framing effects) and between individual stated valuation of privacy concerns and those revealed in purchases of PETs or bundled privacy protections or precautionary activities e.g. data minimisation and active profile management.

[210] See especially the discussion of cognitive bias in Brown (2011).

5.4.2. Rules and regulations

Recommendation 7: *A 'mutual recognition' system should be deployed at a global level to accommodate fast-moving changes and differences in interpretation*.

Unified law works best within unified jurisdictions; the normally problematic pace of legal change in rapidly-changing environments is likely to be even slower when changes must be negotiated across countries, especially those occupying different places in the Internet value chain, and therefore likely to have different perspectives and priorities. A more flexible and efficient approach could be agreement of basic principles according to which different rules – and differences in regulatory implementation and/or industry practice – could be reconciled informally when first encountered, and harmonised as more data becomes available and other factors adjust.

Such arrangements could be agreed at European level[211] (to facilitate the Digital Single Market), among Member States[212] or among firms in one country interacting with or acquiring interests in firms in other countries or serving customers in other countries. Periodically, the set of agreements could be assessed and the implementing legal instruments adjusted as necessary. More active promotion of co-regulatory arrangements may be needed, as purely self-regulatory measures regarding e.g. OBA have proven ineffective.[213] Government monitoring and enforcement can be used to back 'self-regulation' in response to market forces[214], industry standards, norms or (binding) codes of conduct. Such measures should - but do not always - conform to the Better Regulation principles[215] and reflect the superior information of those closest to actual Internet services.

Recommendation 8: *Privacy rules should be reconciled with other kinds of economic regulation*.

The RFID and cloud computing case studies show how market competition can affect both innovation and privacy. But market discipline depends on the mitigation of the market failures identified in e.g. Table 3 regardless of whether they are concerned with markets for Internet services, privacy or innovations affecting privacy rights. Therefore, privacy rules must work in concert with consumer protection and competition rules.

---

[211] Though legislative recommendations are beyond the remit of this report, the Safe Harbor agreement provides a potential model.

[212] Such agreements might range from specific certification requirements to general principles lacking legal precision; To reconcile flexible national interpretation with Single market principles, they could be structured along the principles of: non-discrimination (e.g. Fair, Reasonable And Non-Discriminatory (FRAND) rules); reciprocity (to limit free-riding and allow exchange of mutual concessions between countries); binding and enforceable commitments (including rules for handling jurisdictional issues); transparency; and 'circuit breaker' protections for exceptional situations.

[213] The possible ineffectiveness of pure self-regulation was noted by the European Data Protection Supervisor http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2011/EDPS-2011-08_Behavioural%20advertising_EN.pdf (visited 12 October 2011). In addition, purely market-based or self-regulatory approaches may render existing codes and approaches obsolete, possibly inhibiting market entry especially when tied to proprietary technologies and business practices, or when membership of the 'standardising body' is restricted. Such rules may become too numerous or complex to permit informed choice by end-users. Their monitoring, compliance and enforcement may be patchy, selective or ineffective (Soghoian 2010).

[214] This may be demand-led – as was the case with the implementation of Facebook user privacy controls – or supply-side – as in the case of Microsoft's explicit and overt commitment not to scan Hotmail messages as part of anti-spam measures. The responsiveness of consumers to differentiated privacy offerings is substantiated in Tsai *et al.* (2007).

[215] Typically, these include transparency, accountability, targeting, proportionality and consistency. For a discussion in the context of self- and co-regulation, see Cave *et al.* (2008).

Recommendation 9: *Impact Assessment and evaluation of policies relating to innovation and/or privacy should take the long view*.

The – sometimes unexpected – evolution of innovation, markets, attitudes to privacy and relation between innovation and privacy dictate that Impact Assessments of innovation- (resp. privacy-) related policies should include medium-term privacy (resp. innovation) impacts. In addition, it would be useful to examine in detail cases where innovation and privacy practices have evolved to address and minimise the burdens associated with specific rules.[216]

5.4.3. Coping with change

Recommendation 10: *Privacy governance should be placed on a value-based footing that is neutral with respect to technology, business models, services, etc*.

Many issues arising in relation to new technologies (e.g. mobile devices, cloud computing, etc.) business models, uses[217] etc. stem from the difficulty of transposing privacy rights.

Rules focused on specific technologies[218] may distort market development, non-market Internet activity and innovation itself. The same applies to changing relationships; the cloud and behavioural advertising case studies show the problems that arise when the party best-placed to bear liability (e.g. a cloud service or social network platform provider) cannot easily monitor or control users who may infringe the privacy of other users[219] with whom they have no direct contact or privity of contract. Similar, though not identical, challenges arise in respect of other providers of intermediary services such as search and/or data mashing.

A potential solution is to extend the data owner/data processor dichotomy to reflect multilateral Internet-based relationships, for example by regulating Service Level Agreements and allowing platform providers to transfer liability to third-party (e.g. cloud-hosted) providers of privacy services.

A further undesired consequence of the changing environment is the need frequently to revisit, if not the Directives themselves, at least the enabling measures and (under the new comitology) Delegated Acts. A potential solution is the endorsement at the EU level of a preference for value-based over rule-based regulation.

---

[216] E.g. whether the 'cookie law' provisions of the current Directive will lead to innovative, effective and non-intrusive ways of obtaining prior consent.

[217] Examples include the advent of natural user interfaces that render browser-orientated rules (specifying hyperlinked disclosure of conditions or 'click-to-accept' mechanisms) obsolete or irrelevant; new or alternative methods of geo-location with different points of control, accuracy and longitudinal traceability); and alternatives to RFID (from passive barcodes to other near-field devices) in implementing the Internet of Things.

[218] The Directive itself calls on data controllers to use 'best practices'. But it is not obvious how to 'certify' best practice without distorting the very market that the measure is trying to restore. The identification of best practices and the overall move towards their adoption (and subsequent improvement) can be reinforced by standards bodies (the BSI has taken some preliminary steps in this respect). There is also clear scope for co-regulatory partnerships between government and industry; for instance, Data Protection regulators could approve industry codes of conduct – though to date only four have been approved.

[219] For example, a party processing personal data over a cloud platform may expose those data to others (if not adequately controlled by the Service Level Agreement); cloud service providers may create an ancillary privacy infringement by revealing the nature of the services requested by their clients; and social network users may allow tagging and other forms of group privacy infringement.

Recommendation 11: *A platform should be provided for joint piloting of new approaches to emergent privacy-related problems*.

The structure and the impacts of current privacy rules depend on the understanding and preferences of those involved from government, business and society. These reflect the lessons of history; in particular, large scale or highly publicised failures can inhibit the process of finding new solutions and testing them under realistic conditions to ensure that practical issues are addressed. The law proceeds as if current perceptions and preferences were permanent, despite evidence that citizens change their views of privacy in response to their own experience, public information and offers by service providers. This 'moving target' aspect is not wholly reflected in the current structure, especially as regards innovation.

The refinement and acceptance of new approaches, both of which are essential to their success, depend on experimental as well as empirical evidence. But the experiments involved must be social as well as technical and conducted as 'live pilots' in a Living Lab environment involving actual stakeholders, but surrounded by an informational firewall to prevent leakage or private information to the outside world. Such 'sandbox' arrangements have been used in exploring e.g. alternatives for reuse of public data with good success.[220]

Recommendation 12: *Undertake additional translational and policy-related research*.

There are gaps in our current knowledge that inhibit evidence-based policy; these are likely to increase as the Internet ecosystem continues to evolve. Specific areas of ongoing conceptual and practical research can be translated to improve the evidence base and inform better policies, and some issues currently beyond scope can be illuminated by additional policy-related research.

This recommendation identifies three promising areas: the economics of privacy; Framework Programme research on technical solutions; and the privacy implications of globalised economic and other activity.

As regards the economics of privacy, the literature review and the case studies identified clear examples of the use of private data and privacy rights to create, capture or contest economic value. However, they left many questions unanswered, particularly as to how well user *empowerment* (e.g. via economic privacy rights and enhanced transparency) can complement or substitute for user *protection*[221]. A related open question concerns the possible rebound effect if transparency rules provoke service providers and data collectors/processors into ceasing to collect or optimally use information. A range of other topics also need to be better understood. These include the following.

1) The nature and interrelationship of markets in private information and privacy services.

2) The potential for offering a range of (differently-priced) levels of data access, capture and reuse in Service Level Agreements, subscriptions and other Internet-related contracts between end-users and service providers; and the valuation (as well as valorisation) of individual and aggregated personal data

[220] UK Government (2007), Mayo and Steinberg (2007) and Cave and Marsden (2007).

[221] In particular, people will increasingly exchange private data in order to build trust; moreover users will increasingly collect information and may eventually become the 'eyes and ears' of the regulatory framework.

3) The economic impacts of user empowerment. Market forces will only drive privacy-enhancing innovation if customers are empowered to take control of their own data. This control will force data collectors, etc. to invest in protection in exchange for gaining access to users' data and may possibly encourage them to share the proceeds.

4) Expansion of the market for use of personal data. This implies effective solutions to informational, market power and other market failures and/or sensitisation of end-users to the costs of failing to control privacy risk that they are willing to pay to have it protected. In the latter case, the maximal value of the market is bounded above by the perceived increase in benefit through access to personalised offers or revenues from data re-use compared to opting-out by e.g. patronising Internet-based or off-line businesses that do not collect data or protecting themselves through end-user PETS. On the other side of the market, firms will only invest in PETs and related practices if the returns in terms of increased consumer demand and reduced costs associated with privacy breaches (including legal and regulatory liability) offset the opportunity costs of 'softer measures' (including non-compliance).

As regards adoption of results from current Framework Programme research, we note that the Future Internet Core Platform public-private partnership and the Future Internet Research and Experimentation expert groups are explicitly building privacy concerns into Internet innovation, and that other projects in the Trust & Security area[222] have developed a range of privacy-enhancing technologies and clarified some of the associated business and socioeconomic aspects of their wider deployment. These should be considered in relation to future regulations, which may use them as a reference standard even if their adoption is not mandated.

Finally in relation to globalisation, although international issues beyond the EU were not a central focus of this report, they are increasingly important as noted e.g. in footnote 6 (imports and exports of privacy-related innovations and privacy definitions and approaches) and at the end of Chapter 2 (discussion of Patriot Act data access provisions in relation to cloud computing). It may therefore be useful to extend the current analysis to consider global and trade-related aspects.

[222] Many of these projects are listed at: http://cordis.europa.eu/fp7/ict/security/projects_en.html. There is a particular area devoted to trust, privacy and identity in the digital economy but also a range of technological and organisational strategic research being carried out in relation to frameworks and policies to enhance trust and privacy through cooperation, clustering, etc.

REFERENCES

- Acquisti A. and Grossklags, J. (2004) “Privacy Attitudes and Privacy Behaviour: Losses, Gains, and Hyperbolic Discounting” in J. Camp and R. Lewis (eds.), "The Economics of Information Security", Kluwer.
- Acquisti, A. L. John and G. Loewenstein; (2010) "What is Privacy Worth?" Leading paper, 2010 Future of Privacy Forum's Best "Privacy Papers for Policy Makers" Competition.
- Alonso, N. (2011) “Internet: The 'right to be forgotten': its recent application in Spain” *Data Protection Law & Policy* 8(3)
- Alreck, P. & Settle, B. (2007) “Consumer reactions to online behavioural tracking and targeting” *Journal of Database Marketing & Customer Strategy Management* 15: 11–23.
- Anagnostopoulos, A. Broder A.Z.m Gabrilovich, E. Josifovski, V. Riedel, L. (2007) *Just-in-Time Contextual Advertising*, Yahoo Research.
- Article 29 Working Party (2005) “Working document on data protection issues related to RFID technology”, WP 105 , Brussels, 19 January 2005
- Article 29 Working Party (2009) “The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data” WP168 2009.
- Article 29 Working Party (2010) “Opinion 1/2010 on the concepts of ‘controller’ and ‘processor’” available from: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf (visited 12 November 2011).
- Article 29 Working Party (2011a) “Opinion 13/2011 on the current EU personal data breach framework and recommendations for future policy developments” 5th April 2011 at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf (visited 12 November 2011).
- Article 29 Working Party (2011b) “Opinion 15/2011 on the definition of consent” 15th July 2011 at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (visited 12 November 2011).
- Barcelo, R. and P. Traung (2010) "The Emerging European Union Security Breach Legal Framework: The 2002/ 58 ePrivacy Directive and Beyond" Ch. 5 in Gutwirth, S. Poullet, Y. and P. de Hert (eds.) "Data Protection in a Profiled World" Dordrecht, Heidelberg, London New York: Springer Verlag.
- Bargh, J. (2002) “Additional references: Losing Consciousness: Automatic Influences on Consumer Judgment, Behavior, and Motivation” *Journal of Consumer Research* 29(2): 280-285.
- Barth A, Datta A, Mitchell C, Nissenbaum H (2006) “Privacy and Contextual Integrity: Framework and Applications” *IEEE Symposium on Security and Privacy*, pp 198-213.
- Bäumler, H., Breinlinger, A and H-H. Schrader (1999) “Datenschutz von A-Z” (Stichwort "Informationelle Selbstbestimmung" - I300); Neuwied; Krieftel: Luchterhand).
- Bennett, C and Raab, C (2006) "The Governance of Privacy" Cambridge, MA: MIT Press.
- Berkhout G and Van der Duijn P (2007) “New ways of innovation: an application of the cyclic innovation model to the mobile telecom industry” *International Journal of Innovation Management* 40(4): 294-309.
- Body of European Regulators for Electronic Communication (BEREC) (2011) “BEREC Guidelines on Net Neutrality and Transparency: Best practices and recommended approaches” at: http://erg.ec.europa.eu/doc/berec/consultation_draft_guidelines.pdf (visited 12 November 2011).
- Boyd, D. (2010) “Risk reduction strategies on Facebook” November 8, 2010 at http://www.zephoria.org/thoughts/archives/2010/11/08/risk-reduction-strategies-on-facebook.html (visited 21 February 2011).

- Bradshaw, S. Millard C, Walden, I (2010) "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing services" Queen Mary University of London, School of Law Legal Studies Research Paper, no. 63/2010.

- Brouwer, E. and Guild, E. (2006) "The Political Life of Data: The ECJ Decision on the PNR agreement between the EU and the US" CEPS Policy Brief 109 at http://www.ceps.eu/files/book/1363.pdf (visited 12 November 2011).

- Brown, I. (2011) "Privacy Attitudes, Incentives and Behaviours" at: http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1866299_code892424.pdf?abstractid=1866299 (visited 12 November 2011).

- Capgemini (2005) "RFID and Consumers - What European Consumers Think About Radio Frequency Identification and the Implications for Business".

- Cave, J., C. Marsden and S. Simmons (2008) "Options for and Effectiveness of Internet Self- and Co-regulation" RAND TR-566-EC Santa Monica: RAND.

- Cavoukian, A. (2008) "A Privacy By Design: Take the Challenge: Information and Privacy" Commissioner of Ontario Canada.

- CEO Roundtable (2011) "Digital Agenda: second CEO Roundtable on broadband investment to sustain internet growth" http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/508&format=PDF&aged=1&language=EN&guiLanguage=en (visited 12 November 2011).

- Cohen, J. (2000) "Examined Lives: Informational Privacy and the Subject as Object" *Stanford Law Review* 52: 1373.

- Cooper, D. Tielmans, H. and Fink, D, (2010) "The Lisbon Treaty and data protection: What's next for Europe's privacy rules?" *The Privacy Advisor* at: http://www.cov.com/files/Publication/44dd09f7-3015-4b37-b02e-7fe07d1403f4/Presentation/PublicationAttachment/8a89a612-f202-410b-b0c8-8c9b34980318/The%20Lisbon%20Treaty%20and%20Data%20Protection%20What%E2%80%99s%20Next%20for%20Europe%E2%80%99s%20Privacy%20Rules.pdf (visited 12 November 2011).

- Covacio, S. (2003) "Technological Problems Associated with Subcutaneous Microchips for Human Identification (SMHId)" *Informing Science* at: http://www.proceedings.informingscience.org/IS2003Proceedings/docs/107Covac.pdf (visited 12 November 2011).

- Daily Telegraph "Facebook's Mark Zuckerberg says privacy is no longer a social norm" http://www.telegraph.co.uk/technology/facebook/6966628/Facebooks-Mark-Zuckerberg-says-privacy-is-no-longer-a-social-norm.html 11th Jan 2010 (visited 12 November 2011).

- Dijk, J. van (2009) "Users like you? Theorizing agency in user generated content" *Media, Culture & Society* 31(1): 41-58.

- Dosi, G. et al. (1988) "Technical change and economic theory" London: Pinter.

- Earp, J. et al. (2005) "Examining Internet privacy policies within the context of user privacy values" *IEEE Transactions on Engineering Management* 52(2): 227-237.

- EU Mandate 436: "Standardisation mandate to the European Standardisation Organisations CEN, CENELEC and ETSI in the field of Information and Communication Technologies Applied to Radio Frequency Identification (RFID) and Systems."

- EurActiv (2011) "Europe, US converging on Internet Privacy" http://www.euractiv.com/en/infosociety/europe-us-converging-Internet-privacy-news-503578 (visited 12 November 2011).

- European Commission (2006) "The RFID Revolution: Your voice on the Challenges, Opportunities and Threats" Online Public Consultation 16 October 2006.

- European Commission (2007) "Radio Frequency Identification (RFID) in Europe: steps towards a policy framework" COM(2007)96 final.

- European Commission (2009a) "Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification" SEC(2009) 585. SEC(2009) 586, C(2009) 3200 final, Brussels, 12.5.2009.

- European Commission (2009b) Final report 2009(COM(2010)253 final/3 - 25 August 2010 [amending COM(2010)253 - 25/5/2010]) http://ec.europa.eu/information_society/policy/ecomm/library/communications_reports/annualreports/15th/index_en.htm (visited 12 November 2011).

- European Commission (2009c) "Progress Report On The Single European Electronic Communications Market 2008" http://ec.europa.eu/information_society/policy/ecomm/doc/implementation_enforcement/annualreports/14threport/commen.pdf (visited 15 October 2011).

- European Commission (2010a) "Overview of information in the area of freedom, security and justice" COM(2010)385 final.

- European Commission (2010b) "The economic benefits of privacy-enhancing technologies (PETs)" Final report to the European Commission, DG Justice, Freedom and Security. Brussels, EC.

- European Commission (2011a) "Public consultation on personal data breach notifications under ePrivacy Directive" at: http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/data_breach/index_en.htm (visited 12 November 2011).

- European Commission (2011b) "The open internet and net neutrality in Europe" COM(2011) 222 final at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/communications_reports/netneutrality/comm-19042011.pdf (visited 12 November 2011).

- European Data Protection Supervisor (2008) "Opinion of the European Data Protection Supervisor on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on "Radio Frequency Identification (RFID) in Europe: steps towards a policy framework" COM(2007) 96, 2008/C 101/01.

- European Data Protection Supervisor (2010) "Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy" http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-03-19_Trust_Information_Society_EN.pdf (visited 3 July 2011)

- European Data Protection Supervisor (2011), "Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data" at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-10-07_Net_neutrality_EN.pdf (visited 12 November 2011).

- European Telecommunications Standards Institute (2011) ETSI TR 187 020 - Radio Frequency Identification (RFID); Coordinated ESO response to Phase 1 of EU Mandate M436 at: http://www.etsi.org/deliver/etsi_tr/187000_187099/187020/01.01.01_60/tr_187020v010101p.pdf (visited 12 November 2011).

- Federal Trade Commission (Bureau of Consumer Protection) (2010) "A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" (Dec. 1, 2010) available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (visited 12 November 2011).

- Fitzpatrick B.W., Lueck, J.J. (2010) "The Case Against Data Lock-In" *Communications of the ACM*.

- Fransman, M. (2010) "The new ICT Eco-system – Implications for policy and regulation" Cambridge: Cambridge University Press.

- Gadzheva, M. (2008) "Legal Issues in Wireless Building Automation: an EU Perspective" *International Journal of Law and Information Technology* 16(2).
- Garza G (2011) "The History of Biometrics and Biometric Devices" http://www.brighthub.com/computing/enterprise-security/articles/106926.aspx (visited April 6, 2011).
- Goldfarb, A. and Tucker C. (2011) "Online Advertising, Behavioral Targeting and Privacy" *Communications of the ACM* 5 May 2011.
- Grossklags, J. Acquisti, A. (2007) "When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information" Sixth Workshop on the Economics of Information Security available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.137.696&rep=rep1&type=pdf (visited 12 November 2011).
- Hogben (ed) et al: (2011) "European Network Information Security Agency: Botnets: Detection, Measurement, Disinfection & Defence Report" available at: http://www.enisa.europa.eu/act/res/botnets/botnets-measurement-detection-disinfection-and-defence?searchterm=botnets (visited 12 November 2011).
- Hoh, B. Gruteser, M. Herring, R. *et al.* (2008) "Virtual Trip Lines for Distributed Privacy-Preserving Traffic Monitoring" in MobiSys '08 Proceeding of the 6th international conference on Mobile systems, applications, and services.
- Huijboom, N. (2010) "Joined-up ICT-innovation in government – An analysis of the creation of eIDM systems from an Advocacy Coalition and Social Capital perspective" PhD-thesis, Erasmus University Rotterdam.
- Hustinx, P. (2009) Speech at the European Conference of Privacy and Data Protection Commissioners, Edinburgh, 23-24 April 2009 http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/PressNews/Newsletters/Newsletter_18_EN.pdf (visited 12 November 2011).
- Hustinx, P. (2010) Presentation given to ENISA-FORTH Network and Information Security summer school, 13th September 2010 available at http://www.nis-summer-school.eu/nis10/presentations/hustinx.pdf (visited 12 November 2011).
- ICO (1999) "Privacy and biometrics" Privacy Commissioner, Ontario, Canada.
- Juels, A. (2006) "*R*FID Security and Privacy – A Research Survey" RSA Laboratories.
- Katz, M. and C. Shapiro (1985) "Network Externalities, Competition, and Compatibility" *The American Economic Review* 75(3): 424-440.
- Kool L. Plas, van der A., Eijk, N. van , Helberger, Nl. and Sloot, B. van der (2011) "A bite too big: Dilemmas bij de implementatie van de Cookiewet in Nederland" Delft: TNO-IvIR-rapport 35473.
- Kroes, N. (2011a) "Online privacy – reinforcing trust and confidence" SPEECH/11/461, Online Tracking Protection & Browsers Workshop, Brussels, 22 June 2011.
- Kroes, N. (2011b) "Smart tags - working together to protect privacy" Privacy and Data Protection Impact Assessment Framework Signing Ceremony Brussels, 6th April 2011, Press releases RAPID.
- Lace, S (ed) (2005) "The Glass Consumer: Life in a surveillance society" Bristol: The Policy Press.
- Langheinrich M. and G. Karjoth (2010) "Social networking and the risk to companies and institutions" *Information Security Technical Report* 15(2): 51-56.
- Leathers, D. (2009) "Giving Bite to the EU-U.S. Data Privacy Safe Harbor: Model Solutions for Effective Enforcement " Case *W. Res. J. Int'l L.* 41(193).
- Leichtenstern, K., Bee, N. André, E., Berkmüller U. and J. Wagner (2011) "An Empirical Evaluation of the Compliance of Game-Network Providers with Data-Protection Law " TRUST MANAGEMENT V IFIP *Advances in Information and Communication Technology* 358/2011: 149-164.

- Lieshout, M. van et al. (2007) "RFID Technologies: Emerging issues, Challenges and Policy Options" Delft: Report 22770 EN Sevilla: JRC-IPTS. http://ipts.jrc.ec.europa.eu/publications/pub.cfm?id=1476 (visited 10 July 2011).

- Loewenstein, G. and E. Haisley (2008) "The economist as therapist: Methodological issues raised by light paternalism" In S. A. Caplin A. (Ed.), *Perspectives on the Future of Economics: Positive and Normative Foundations*.

- London Economics (2010) "Study on the economic benefits of privacy-enhancing technologies (PETs)". Report to European Commission, DG Justice, Freedom and Security: http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf (visited 12 November 2011).

- Lundvall, B.-A. (ed.) (1992) "National Innovation Systems: Towards a Theory of Innovation and Interactive Learning", London: Pinter

- MacKenzie, P. (2011) "Weapons of Mass Assignment" *Communications of the ACM* May 2011.

- Marsden, C., J. Cave, et al. (October 2006) "Better re-use of public sector information: evaluating the proposal for a government data mashing lab" Santa Monica: Rand Corporation.

- Mayer, J (2011) 'Do Not Track Is No Threat to Ad-Supported Businesses'. Stanford Law School blog post at http://cyberlaw.stanford.edu/node/6592 (visited 12 November 2011).

- Mayo, E. and Steinberg, T. (2007) "The Power of Information: An independent review" at: http://www.opsi.gov.uk/advice/poi/power-of-information-review.pdf (visited 12 November 2011).

- McDonald, A. and Cranor L.F. (2008) "The Cost of Reading Privacy Policies" *I/S: A Journal of Law and Policy for the Information Society* 2008 Privacy Year in Review issue.

- McDonald, A. and Cranor, L. (2009) "An Empirical Study of How People Perceive Online Behavioral Advertising" Carnegie Mellon University.

- McDonald, A. and Cranor, L. (2010) "Americans' Attitudes About Internet Behavioral Advertising Practices" Carnegie Mellon University.

- Odlyzko, A. (2003) "Privacy, Economics and Price Discrimination on the Internet" in "ICEC2003: Fifth Int'l Conf. on Elec. Comm". N.Sadeh (ed.) available at http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf (visited 12 November 2011).

- OECD (1997) "National Innovation Systems" Paris: OECD Publications.

- OECD (2005) "Oslo Manual: Guidelines for collecting and interpreting innovation data; 3rd edition". Paris: OECD Publications

- OECD (2010) "Joint WPISP-WPIE Roundtable The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines" OECD Conference Centre 1 December 2010 http://www.oecd.org/dataoecd/22/26/47690650.pdf (visited 12 November 2011).

- Oudshoorn N. and Pinch T (eds) (2003) "How users matter. The co-construction of users and technology" Cambridge, MA: MIT press.

- Oudshoorn N. and Pinch T. 2007. "User-Technology relationships: Some Recent Developments" in "The Handbook of Science and Technology Studies" Hackett, E.J., Amsterdamska, O., Lynch M., and Wajcman, J. (eds) Cambridge, MA: MIT Press.

- Penn J (2010) "Security and the Cloud. Looking at the Opportunity behind the obstacle" Forrester Research.

- Pigou (1920) "Economics of Welfare", London: MacMillan.

- Png, I. And D. Lehman (2002) "Managerial Economics" London: Blackwell.

- Poel, M., Kool, L. and van der Giessen, A. (2010) "How to decide on the priorities and coordination of Information Society Policies – Analytical framework and three case-studies" *INFO* 12(6): 21-39.
- RACE Network (2011)"RFID, Guidelines on the Use of the Common European RFID sign" , Draft Version 1, July 2011.
- Rafaeli, S. and D. R. Raban (2003) "Experimental investigation of the subjective value of information in trading" *Journal of AIS* 4 (1).
- Reding, V. (2011) "Your data, your rights: Safeguarding your privacy in a connected world" Privacy Platform "The Review of the EU Data Protection Framework" speech by the Vice-President of the European Commission and EU Justice Commissioner Brussels, 16 March 2011 http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/183 (visited 12 November 2011).
- Reding, V. (2011a) "Statement by Vice-President Reding on the European Parliament's vote on the Voss report" at: http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/489&format=PDF&aged=1&language=EN&guiLanguage=en (visited 12 November 2011).
- Robinson N. Valeri, L. Cave J. *et al.* (2010) "Review of the Strengths and Weaknesses of the EU Data Protection Directive 95/46/EC" RAND Santa Monica TR-710-ICO.
- Robinson, N. Valeri, L. Cave, J. *et al.* (2011) "The Cloud Understanding the Security, Privacy and Trust Challenges" RAND Santa Monica TR-933-EC.
- Roco, M. C. and Bainbridge, W.S. (eds) (2003) "Converging Technologies for Improving Human Performance – Nanotechnology, Biotechnology, Information Technology and Cognitive Science" Dordrecht: Kluwer.
- Rubinstein, I. (2011) "Regulating Privacy by Design" Working Paper available as SSRN-id1837862-1.pdf.
- Ryan M (2011) "Cloud Computing Privacy Concerns on our Doorstep" *Communications of the ACM* 54(1): 36-38.
- Schmierer (2011) "Better late than never: How the online advertising industry's response to proposed privacy legislation eliminates the need for regulation" *Rich. J.L. & Tech*. 17(13).
- Schriver, R. (2002) "You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission" *Fordham Law Review* 70(6): 2777-2818.
- Shao, J and Smith, R. (2007) "Privacy and e-commerce: a consumer-centric perspective" *Electronic Commerce Resources* 7: 89-116.
- SIENA consortium (2011) "SIENA European Roadmap on Grid and Cloud Standards for e-Science and Beyond" http://www.sienainitiative.eu/Repository/Filescaricati/8ee3587a-f255-4e5c-aed4-9c2dc7b626f6.pdf (visited 12 November 2011).
- Soghoian, C. (2010) "An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government" Paper presented at TPRC, available at: http://tprcweb.com/images/stories/2010%20papers/soghoian_2010.pdf.pdf (visited 12 November 2011).
- Solove, D. (2002) "Conceptualizing Privacy" *California Law Review* 90(4): 1087-1155.
- Soltani, A. (2011) "Identifiers and online tracking" Submitted to W3C Workshop on Web Tracking and User privacy, April 28-29, Princeton, USA.
- Spiekermann, S. (forthcoming), "The RFID PIA – developed by industry, accepted by regulators" in Wright, D. and de Hert, P. (Eds.) "Privacy Impact Assessment – Engaging Stakeholders in Protecting Privacy". Dordrecht: Springer.
- Thaler, R. (2008) "Nudge: Improving Decisions About Health, Wealth and Happiness" New Haven: Yale University Press.
- Thomson, J. (1975) "The Right to Privacy" *Philosophy & Public Affairs* 295 (4)

- Tirtea R. et al. (2010) "Bittersweet Cookies: Some Security and Privacy Considerations" ENISA (European Network and Information Security Agency).

- Tsai, J., S. Egelman, L. Cranor and A. Acquisti (2007) "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study" Workshop on the Economics of Information Security, Pittsburgh at: http://weis2007.econinfosec.org/papers/57.pdf (visited 12 November 2011).

- Turow, J., King, J., Hoofnagle, C., Bleakley, A. and Hennessy, M. (2009) "Americans Reject Tailored Advertising and Three Activities that Enable It" University of California, Berkeley, School of Law.

- UK Government (2007) "Information matters: building government's capability in managing knowledge and information" available at: http://www.nationalarchives.gov.uk/documents/information-management/information-matters-strategy.pdf (visited 12 November 2011).

- UNISYS (2007) "Biometrics in Europe – Trend Report 2007" European Biometrics Portal, available from http://www.scribd.com/doc/11770142/Bio-Metrics-in-Europe-Trend-Report (visited 28 November 2011).

- US Senate (2011) Committee on Commerce, Science and Transportation Press Release: "Rockefeller Announces Do-Not-Track Legislation to Protect Consumers When They Are Online" (May 6th 2011) available at: http://commerce.senate.gov/public/index.cfm?p=PressReleases&ContentRecord_id=12fed3f7-22c7-49b6-bafe-111998a3d6d9 (visited 12 November 2011).

- Van Oranje-Nassau C. Schindler R., Vilamovska, A., Botterman (2010) "Policy options for Radio Frequency Identification (RFID) application in healthcare; a prospective view", Final report (D5), RAND, TR767, available at: http://www.rand.org/pubs/technical_reports/TR767-1.html (visited 12 November 2011).

- Warren, S. and L. Brandeis (1890) "The Right to Privacy" Harvard Law Review IV(5).

- Westin, A. F. (2008) "How Online Users Feel About Behavioral Marketing and How Adoption of Privacy and Security Policies Could Affect Their Feelings: Results of a Harris Interactive / Westin Survey March 10-17, 2008" Report to the Federal Trade Commission March 2008 available at: http://www.ftc.gov/os/comments/privacyroundtable/544506-00052.pdf (visited 12 November 2011).

- Yang Z, Rothkranz L (2010) "Automatic aggression detection in trains" *IEEE*, pp2364-2373.

ANNEX - INTERVIEWEES

Table 6: List of interviewees

Name	Organisation / sector
Alejandro Becerra Gonzalez	Telefonica
Alma Witten	Google
Anne Toth	Yahoo
Anthony House	Google
Brian Pickering	IT Innovation Centre, University of Southhampton
Caspar Bowden	Microsoft
Didier Bourse	Alcatel Lucent
Elwyn Brian Davies	Folly Consulting / IETF Internet Architecture Board
Gerd Wolfram	Metro Group Future Store
Gert Wabeke	KPN Security
Gus Hosein	London School of Economics
Ian Brown	Oxford Internet Institute
Jean Jacques Sahel	Skype
Jose E Garcia	Telefonica
Kirsten Bock	EuroPriSe
Kostas Kossoglu	BEUC
Lee Bygrave	Olso University
Marisa Jimenez	Google
Massimilio Minisci	EPCglobal
Max Snijder	European Biometrics Forum
Mikko Niva	Nokia

Name	Organisation / sector
Nick Wainwright	HP Labs Bristol
Nick Wiggin	Ericcson
Pat Walshe	GSMA
Raphael Sofar	Diaspora / Clique (social network)
Robert Beens	Ixquick
Tony Fish	AMF Ventures (IT VC)
William Dutton	Oxford Internet Institute
Yaymeen Patel	GSMA, O2

Source: Study Team

CONSULTATION MEETING

As part of this study, a one-day consultation meeting was held on June, 30th 2011 at the Netherlands house for Education and Research (Neth-ER) in Brussels. The parties whom we invited include the following organisations:

Table 7: List of organisations participating in consultation

Organisation	
Agnitio	Amazon
BEUC	Biometrics Group
BPR attorneys	BSA
Cabinet Gelly (TBC)	Diaspora
ECP.NL	ECTA
Ericcson	ETNO
EuroISPA	European Interactive Advertising Association
European Privacy Association	EuroPriSe
Google	GS1
GSMA	IBM
IWIW	Ixquick
KPN Security	KU Leuven
La Quadrature	London School of Economics (LSE)
Microsoft	Nokia
Oslo University	Privacy International (TBC)
PrivaSense	SAP
Skype	Telefonica
Tuenti	Vodafone (TBC)
Yahoo	

Source: Study Team

EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A
ECONOMIC AND SCIENTIFIC POLICY

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Economic and Monetary Affairs
- Employment and Social Affairs
- Environment, Public Health and Food Safety
- Industry, Research and Energy
- Internal Market and Consumer Protection

Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**

PHOTO CREDIT: iStock International Inc.

Does it help or hinder? Promotion of Innovation on the Internet and Citizens' Right to Privacy