Policy Innovation, Convergence and Divergence: Considering the Policy Transfer Regulating Privacy and Data Protection in Four European Countries

Karl Lofgren, University of Roskilde
C. William R Webster, University of Stirling

Contact Details:
Dr Karl Lofgren
Department of Society and Globalisation
University of Roskilde
Hus 25.2
DK-4000 Roskilde
Tel: + 45 4674 2859
E-mail: klof@ruc.dk
URL: http://forskning.ruc.dk/site/research/loefgren_karl(4737)/

Dr. C. William. R. Webster
Senior Lecturer in Public Management
School of Management
University of Stirling
Stirling, FK9 4LA
Tel: 01786 467359, Fax: 01786 467329
Email: c.w.r.webster@stir.ac.uk
URL: http://www.management.stir.ac.uk/

-- WORK IN PROGRESS --
Policy Innovation, Convergence and Divergence: Considering the Policy Transfer Regulating Privacy and Data Protection in Four European Countries

Karl Lofgren, University of Roskilde
William Webster, University of Stirling

1. Introduction
This paper examines policy activity surrounding the implementation of privacy regulations in four European Union (EU) member states, Denmark, Scotland, Sweden and the UK, following the ratification of the 1995 EU Directive on Data Protection. In particular, it highlights the convergence and divergence of policy embedded in the policy transfer process with specific reference to Dolowitz and Marsh’s ‘Policy Transfer Model’. In doing so, the paper highlights limitations with this model and stresses not only the complexity of policy transfer but also the degree to which policy formation and diffusion is shaped by existing institutional settings and the processes associated with policy implementation.

The starting point for the paper is the 1995 EU Directive on Data Protection - hereafter referred to as ‘the Directive’. The Directive signifies an important development in data protection policy for a number of reasons. Firstly, it is an EU-wide trans-national policy instrument, which is intended to ‘direct’ and guide national policy, and as such is the primary policy instrument in Europe. Secondly, it formally overrides a myriad of diverse regulatory policy arrangements that previously existed across Europe. And thirdly, it affords European citizens a degree of protection (and privacy) in the data intensive information age, at the same time as allowing private companies and public service providers to process and exchange vast quantities of information for commercial and efficiency purposes. The Directive is the central plank of modern interpretations of privacy and is regarded by many commentators and practitioners as an indication that privacy regulation in Europe is undergoing a convergence process in which the individual countries surrender their own capacity in this field, in order to fall in-line with the requirements of the Directive. In this respect a degree of convergence is the logical outcome of the Directive. However, as with other EU Directives, there is scope for the implementation of the Directive to be shaped by national settings, providing the possibility of multiple interpretations of
the Directive’s intentions. These national settings entail certain formal legal provisions, various governmental agencies, and formal legislative procedures, as well as, informal self-regulatory mechanisms, and specific discourses concerning privacy issues. Consequently, a Directive which is intended to harmonise data protection across Europe may actually facilitate the evolution of a number of different data protection landscapes, in which data protection has been implemented and is enforced differently.

This paper analyses the extent to which, and in what ways, the implementation process of the Directive on data protection privacy diverge vis-à-vis each other in Denmark, Scotland, Sweden and the UK. Based on a policy transfer approach to comprehending the policy process the argument brought forward is that certain institutional factors, such as, the national culture of self-governance, regulatory histories, and the location and capacity of the regulatory agencies (etc), has been decisive for the interpretation and implementation of the Directive in each country. Such developments raise important questions about the extent to which the Directive’s principles are being adhered to and realised.

The paper departs from much of the established literature on privacy in three main ways. Firstly, the paper examines the evolution of privacy regulations from a public policy and political perspective. This is an important development because it posits that concerns about privacy are as much political and public policy issues as they are legal and technological ones. Secondly, the concept of privacy is intentionally broadened to go beyond the narrow confines of personal data to include access to public information. Here the general principle is that privacy is about individual’s control of and access to (relevant and appropriate) information. This is an important point as the Directive has provisions for both, despite being titled the ‘Directive for Data Protection’. Thirdly, the paper also departs from much of the published literature by placing at the heart of its analysis international comparative case studies. Such an approach illuminates the processes and national settings through which privacy is regulated, and the multifaceted nature of privacy governance.

The remainder of the paper is organised into the following main sections. The next section, section 2, reviews the term privacy and how it is commonly construed and
regulated. Section 3 provides contextual information about the Directive and its implementation. Section 4 presents the main features of Dolowitz and Marsh’s ‘Policy Transfer Model’ and establishes its utility in this case. This is followed by section 5 which explores the implementation of the Directive in four case study countries. The final section, section 6, offers discussion and concluding comments.

2. The Governance of Privacy
The landscape of privacy regulation has changed dramatically since the 1980’s. Prior to the enactment of the Directive in 1995 the governance of privacy was an independent area of national policy with different regulatory measures emerging in different countries. In this period, the emergence of public policy, legislation and agencies in this field was largely a response to the pace of technological change and the increasing importance of information and data. The backdrop to contemporary concerns with privacy is therefore based on the global information revolution and the emergence of an information society with its new information and communication technologies (ICTs) at the heart of its economic, social and political reforms. Central to this revolution has been the collection and processing of vast quantities of information, including personal information, for multiple purposes and facilitated by new ICTs. These developments have brought the concept of privacy, and in particular, the right to keep personal data private, to the fore, and subsequently a major policy issue and point of debate. Consequently, over the last 30 years states have tried to regulate the collection, use, storage and dissemination of individually identifiable personal data, primarily to protect citizens from the misuse of personal information by public and private agencies. Most states now have a set of privacy principles enshrined in national legislation which provide a basic set of guidelines for every organisation that processes personal data, regardless of the technologies involved. Most laws also establish privacy or data protection agencies with a variety of advisory, regulatory, educational and complaint resolution responsibilities (Bennett, 1992; Flaherty, 1989). The patchwork of national regulatory measures that emerged across Europe in the late 1980’s was subsumed by the ratification of the Directive in 1995. This Directive set a common policy direction and afforded European Citizens with a standardised set of ‘rights’. The main features of the Directive are discussed in more detail in section 3.
For a number of commentators the information revolution poses a significant
challenge to privacy, despite the existence of regulation and legislation (Agre and
goes so far as to argue that the emergence of new surveillance technologies, based
on the capabilities of new ICTs, are going to result in the ‘end of privacy’, or in
Garfinkel’s (2000) case the ‘death’ of privacy. Here, concern is driven by the
informational capabilities of new ICTs, manifest in the existence of massive
databases containing records of information about individual financial and credit
history, medical records, purchases and telephone calls, for example. Further to
this, individuals, on the most part, do not know what information is stored about them
or who has access to it, and the ability for others to access and link databases, with
few controls on how they use, share, or exploit the information, makes individual
control over information more difficult than ever before. Alterman (2003) discusses
various privacy and ethical issues arising from expanding use of biometric
identification and recent work on privacy is examining the ways in which respect for
privacy can be balanced with justifiable uses of emerging technology (Agre and
Rotenberg, 1997; Austin, 2003; Etzioni, 2000).

Although the Directive signifies a common approach to European regulation, privacy
remains an abstract and contested notion (Nissenbaum, 2004) with a proliferation of
different definitions (Margulis, 2003). It is often perceived as some sort of ‘right’
embedded in legal authority and which protects the right of the individual to be ‘left
alone’ (Warren and Brandeis, 1890). But this is problematic as it implies a legally
enforceable standard and because of the lack of clarity between the existence of
legal, moral, human and natural rights. Systematic discussion of the concept of
privacy is often said to begin with the famous essay by Warren and Brandeis titled
‘The Right to Privacy’ (1890), and is developed in the work of Westin (1969) and
Inness (1992) amongst others. Typically it is a subject area dominated by legal
definitions (for a review of definitions see; Gavison, 1980; Margulis, 2003). Clarke
suggests that:

“privacy is the interest that individuals have in sustaining a 'personal space',
free from interference by other people and organisations” (Clarke, 2006: 1),
and that the dimensions of privacy include, privacy of: the person, personal behaviour, personal communications, and of personal data. A useful distinction can also be made between privacy as an intrinsic or aesthetic value, which should be protected at all costs, and privacy as an instrumental or strategic value, where the concern should be about who uses information and for what purposes (Rule et al, 1980). An important implication of any definition of privacy is that it implies a balance between competing interests. Thus the privacy interests of one person may conflict with interests of another person, group of people, organization, or society as a whole, and the two may have to be ‘traded off’. Following on from this, ‘privacy protection’ is therefore the process of finding appropriate balances between privacy and multiple competing interests. Moreover, because there are so many dimensions of the privacy interest, and so many competing interests, at so many levels of society, the formulation of detailed, operational rules about privacy protection is a difficult exercise which ultimately involves formal authority in the form of state intervention.

The increasing importance of developments in new ICTs has meant access to, and control over, ‘information’, has been central to debates about privacy. Bennett and Raab (2006) and Clarke (2006) refer to this specific area of interest as ‘information privacy’ arguing that it is quite distinct from other types of privacy. Privacy in the information age involves the development of rules governing the capture and processing of ‘personal’ information, where such information has personal identifiers that relate it specifically to certain individuals and subsequently is seen to ‘belong’ to the individuals concerned. However, because there are so many dimensions of the privacy interest personal information can relate to individuals, organizations or society (and therefore is not always strictly speaking personal). In this respect privacy protection is about the control of information, at a personal level and across society more generally. To complicate matters, the terms ‘data’ and ‘information’ are often used interchangeably in relation to privacy, although policy instruments and legislation tend to be built around data protection and not privacy or information protection (see Margulis (2003) for an up-to-date analysis of the terms data protection and privacy). This is pragmatic on the part of policy-makers as it is much easier to legally define data than the abstract notion of privacy (Clarke, 2006).
In the information age ‘information privacy’ is therefore the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves and also the rules governing the way organizations capture, process and provide access to information. This broad approach to conceptualising privacy is useful because it goes beyond the narrow confines of legalistic definitions of an individual’s right to privacy to encapsulate broader privacy issues, like access to information and control over information, and because it emphasises policy settings and instruments. Privacy is therefore a multifaceted concept embedded in conception and practice in national and European institutional settings. It is also a concept which is multidimensional, as it encompasses personal information, data protection, and also access to information (sometimes referred to as ‘freedom of information’, or FOI). This is a much broader interpretation of privacy than just personal information and is important because it is in line with the way privacy is conceived by the 1995 Directive.

Privacy is not just a concept for definition but also a political and policy concern, and as such embodies facets of political and policy processes. Placing privacy in a broader policy perspective is enriching because it brings into focus the wide range of actors, institutions, instruments and actions in the policy environment which have a bearing on how privacy is conceived, regulated and practiced. This is significant as it provides a much deeper understanding of the societal influences that shape privacy and goes some ways to helping us understand how privacy is governed. The policy environment surrounding the governance of privacy is well established and includes a collection of laws, codes, guidelines, conventions, practices, discourses, actors and agencies, which together regulate the processing of information and which together constitute a distinct policy ‘sector’:

“characterized by a separate set of statutory instruments, regulatory bodies, a network of legal experts, a hardy bunch of journalists and activists... (and) a growing academic community with expertise in data protection and privacy” (Bennett and Raab, 2006: xxi-i).

Bennett and Raab go so far as to argue that this particular policy sector is so distinct and specialised that it is actually isolated and ‘ghettoised’.
The combination of this sort of activity is referred to by Newman and Clarke (2008) as a ‘policy assemblage’, an assemblage of apparatus, procedures and practices, as well as, institutions, discourses and strategies, into a coherent entity that functions as ways of governing, rather than temporally separated elements of a cycle of action and effect. For Newman and Clarke, this is especially important in a networked era where co-regulation and self-governance are perceived to be the order of the day following the ‘hollowing out’ of the state. Building on ideas associated with Actor-Network Theory (Latour, 2005) the assemblage highlights the importance of particular kinds of ‘agents’ (translators, mediators and transactors) and the interchange of ideas, discourse and beliefs.

More specifically, and in relation to the governance of privacy, Bennett and Raab (2006) bring forward the concept of ‘regimes’ of privacy protection, which consist of multiple actors, structures and tools, which together help us comprehend the intricate complex processes through which privacy protection is provided. For Bennett and Raab, privacy protection is a subtle process of negotiation, debate and interaction between stakeholders, and not just the imposition of policy instruments. In other words, it is a political process. Nevertheless, an approach based on regimes highlights the significant role played by certain actors, agencies and instruments, in the provision and implementation of privacy protection. Table 1 summarises the main features of a privacy regime.

Table 1. Core Features of Bennett and Raab’s Privacy Regimes

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Community</td>
<td>Actors and agencies active in the privacy domain: international legal experts, policy administrators and public service practitioners, politicians (elected representatives), privacy advocates, data controllers, government policy-makers, regulatory agencies (Information Commissioners), the media, private companies and technology developers and suppliers.</td>
</tr>
<tr>
<td>Privacy Discourse</td>
<td>Prevailing attitudes and debate in society and within policy community</td>
</tr>
</tbody>
</table>

(Source: adapted from Bennett and Raab, 2006.)
Central to the conception of a regime is the interaction and intertwined relationships between all the elements of a regime. Such an approach to understanding the governance of privacy is beneficial, not just because it emphasises underlying policy processes, but because it recognises the fragmented nature of modern governance and the emergence of self-governance and co-regulation within the regime. Here Bennett and Raab argue that privacy regulation is made up of legally enforceable legislation as well as voluntary codes of behaviour and negotiated commitments – so, a greater emphasis on the use of authority, rules and standard setting, as opposed to state ownership, direct control and delivery – and that these instruments emerge from and are embedded within their institutional and policy settings.

For this paper, the privacy regime approach is important for two main reasons. Firstly, it demonstrates, beyond doubt, that privacy is a policy issue and subsequently subject to complex policy processes. Secondly, it emphasises the complexity of the privacy policy environment and the multitude of actors and instruments that exist with this environment. Both suggest that the formation and implementation of a European Directive in the privacy area would be an inherently complex negotiated process. Also, these two points suggest that it is not unreasonable to assume that ‘best practice’ in privacy protection and governance is likely to emerge from within the regime as a sort of ‘negotiated order’, and that ideas about how to govern privacy are ‘transferred’ around the policy environment, between actors and nations, with a degree of regulatory conformity emerging across nation states.

3. The 1995 EU Directive on Data Protection

The European Union 1995 Directive on Data Protection, referred to as ‘the Directive’ in this paper, was ratified by European Parliament and the Council of Europe on 24 October 1995 and came into effect in October 1998 (European Union, 1995). It directs EU member states policy and practice in relation to ‘the protection of individuals with regard to the processing of personal data and on the free movement of such data’ (Directive 95/46/EC). The Directive was established to provide a

---

regulatory framework to guarantee secure and free movement of personal data across the national borders of the EU member countries, in addition to setting a baseline of security around personal information wherever it is stored, transmitted or processed. So, the essence of the Directive was twofold, to secure a commercial market for data processing at the same time as securing the protection of personal data. For some commentators these twin goals were incompatible from the outset, as the data needs of commercial companies was always going to be quite different to those of individual citizens (Lloyd, 1996).

The final content of the Directive can be best understood as compromise following lengthy negotiations between national governments and the European Commission. Prior to the Directive, data protection had been a European policy concern for quite some time. In 1980, in an effort to create a comprehensive data protection system throughout Europe, the Organization for Economic Cooperation and Development (OECD) issued its ‘Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data’ (OECD, 1999). The OECD’s recommendations were organized around the ‘seven principles’ for protection of personal data, namely: (1) notice, (2) purpose, (3) consent, (4) security, (5) disclosure, (6) access, and (7) accountability (for a full description of these principles see OECD, 1999). Interestingly, all seven principles were later included in the Directive. The OECD Guidelines, however, were not binding and data privacy laws in the 1980’s varied considerably across Europe. Moreover, the European Commission realised that diverging data protection legislation in EU member states would impede the free flow of data within the EU ‘zone’ and provide European citizens with differentiated levels of data protection. It therefore set out to harmonise regulation and practice. Simitis argues, that the European Parliament struggled to get data protection onto the political agenda in the 1980’s, primarily because the European Commission was pursuing a market-


\(^2\) Human Rights legislation enacted by national governments and the EU include aspects of privacy protection. See for example Bygrave (1998).
orientated approach to the development of ICT’s in Europe, especially in the area of telecommunications liberation and in relation to the prospects for the commercialisation of personal data (Simitis, 1995). Initially the Commission called for member states to ratify the European Council 1981 Data Protection Act, a much softer set of guidelines. However, in the transition period from a European Community (an economic union) to a European Union (a more political union) in the late 1980s, and the subsequent commitment to certain European fundamental citizen rights, the position of the Commission changed, and in the early 1990’s two proposals for a Directive on data protection were presented, one in 1990 followed by revised proposal in 1992 (European Commission, 1990/277; European Commission, 1992/310). The content of both proposals was familiar to policy-makers in the data protection field and the development of these proposals over time signifies the importance of combining existing national policy and legislation, as opposed to presenting radical new alternatives. The struggle to reach a settlement between the Commission and the national member state governments took five years to resolve and demonstrates the problems of finding comprises, as well as the antagonistic positions of certain actors. Existing regulative frameworks and the underlying national law systems and traditions proved to be a challenge for the Commission, who hitherto had been focused on pure market relationships and had little experience of regulating public sector activity. Also, it became clear at a relatively early stage that the Commission’s proposals had the potential to interfere with data protection at all levels of government, including the politically sensitive areas of taxation, policing and national security. Some member states, principally France and the UK, succeeded in getting these policy sectors exempted from the Directive. And at the very final stage of the ratification process, Greece, which also happened to hold the European Presidency at the time, strongly argued that the proposal grossly violated the Greek constitution. Nevertheless, the Directive was finally adopted by the Council of Ministers in July 1995.

In line with European treaties which underpin the formation of the European Union the Directive asserts a strong influence over national decisions to legislate in the field of data protection, and also to legislate according to the specific requirements (principles) set out in the Directive. So what is the main content of the Directive? Although there is not enough room here for a full length account of the Directive, it is
possible to deduce some overall principles. The Directive contains 33 Articles in 8 Chapters and contains six basic tenants; (1) notice, (2) choice, (3) use, (4) security, (5) correction, and (6) enforcement. These core characteristics of the Directive are summarised in table 2 (see Lloyd (1996) for an overview of the Directive).

Table 2. Basic Tenants of the 1995 EU Directive on Data Protection

<table>
<thead>
<tr>
<th>Tenant</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice</td>
<td>An individual has the right to know that the collection of personal data exists. The personal data must be ‘collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes’.</td>
</tr>
<tr>
<td>Choice</td>
<td>An individual has the right to choose not to have the personal data collected.</td>
</tr>
<tr>
<td>Use</td>
<td>An individual has the right to know how personal data will be used and to restrict its use. Personal data may only be used for ‘legitimate processing’ as described by the Directive details.</td>
</tr>
<tr>
<td>Security</td>
<td>An individual has the right to know the extent to which the personal data will be protected. Organizations must implement appropriate technical and organizational measures to protect personal data. The measures must be ‘appropriate to the risks represented by the processing and the nature of the data be protected’.</td>
</tr>
<tr>
<td>Correction</td>
<td>An individual has the right to challenge the accuracy of the data and to provide corrected information. Personal data collected and maintained by organizations must be up to date and reasonable steps must be taken to ensure that inaccurate or incomplete data is corrected.</td>
</tr>
<tr>
<td>Enforcement</td>
<td>An individual has the right to seek legal relief through appropriate channels to protect privacy rights.</td>
</tr>
</tbody>
</table>

Following analysis provided by Bennett and Raab (1997) these basic tenants can be seen to provide a set of underlying principles. First, the principle of ‘fair information and openness’ in terms of the ‘data controller’ notifying the supervisory authority prior to carrying out any (wholly or partly) ‘automatic processing operation or set of set of such operations’ (Article 18 [1]). The notification process should include providing the supervisory authority with information about the data controller, the purpose for the data processing, the recipients of such data (etc), regardless of whether the data is collected directly from the citizens or from a third party (Article 11). Second, the principle of ‘access and correction’, under which individuals have the right (‘without constraint’) to know the nature of the data gathered and also that they should be allowed to rectify inaccurate data (Article 12). Thirdly, the Directive specifies the ‘limitations of collection and the finality principle’, basically, this means that data once processed cannot be arbitrary reused by the data collector or any
third party. Whereas some previous national data protection regulatory frameworks made distinctions between retrieval, use and disclosure of data, this distinction does not exist in the Directive. Additionally, the Directive uses a general definition of data protection, where data protection is defined as ‘any operation or set of operations which is performed upon personal data, whether or not by automatic means’ (Article 2(b)). In this respect the Directive can be said to have been proactive and flexible as it is not constrained by the technology or method used for data processing. Fourth, the Directive sets out member states’ obligations in securing that personal data is ‘processed lawfully’ (Article 6 [1a]) with alternative legal remedies. Finally, the Directive stipulates the principle of security whereas the data controllers must apply necessary measures to protect personal data against either destruction or loss, and against ‘unauthorised alteration, disclosure or access’ (Article 17 [1]). This also refers to all involved parties.

In addition to these overarching principles the Directive specifies the nature and function of each member states’ ‘supervisory agents’ which through the Directive becomes mandatory (for all the member states), and which are endowed with powers to monitor the application of the Directive (Article 28[1]). These supervisory agents (or authorities) are typically data protection, privacy or information ‘commissioners’ and are important because the data protection principles promoted by the Directive are not self-enforcing and a culture of privacy and respect of personal data cannot emerge without suitable actors/agencies responsible for their promotion. The responsibilities of the supervisory agents vary from nation to nation, but typically include: oversight, auditing, monitoring and evaluation, expert knowledge, mediation and dispute resolution, and the balancing of competing interests. For Bennett and Raab (2006) these ‘agents’ act as; auditors, ombudsmen, consultants, educators, policy advisors, negotiators and enforcers. Amongst other duties these authorities must act with ‘complete independence’, mainly vis-à-vis other parts of government, and have effective powers for investigating violations and to engage in legal proceedings concerning the Directive. In addition to national supervisory agents, the Directive established a ‘Working Party’ composed of national representatives from each national supervisory agency together with members from the Commission and other EU institutions. This institution was responsible for overseeing and reviewing the implementation of the Directive. However, it only had
advisory status, with ‘real’ executive power residing with the EU and individual national governments.

The ratification of the Directive in the mid 1990’s signals the culmination of over fifteen years of policy negotiation and political manoeuvring amongst EU member states. It also signals the start of a process by which member states were obliged (legally bound) to implement, or adjust, their own national legislation and practice to complement the legally enforceable measures enshrined in the Directive. In this respect, the transfer of privacy policy occurred, firstly, to inform the content of the Directive, and secondly, once the Directive was adopted, to inform the direction of subsequent national legislation and practice. The importance of the transfer of policy pre and post Directive leads us to look more closely at the transfer process, and how this process should be best comprehended. This is achieved, in the paper, with reference to the ‘Policy Transfer Model’ developed by Dolowitz and Marsh (1996, 2000).

4. The Policy Transfer Process

While policy transfer between (in particular industrialised) nations is not a new phenomenon, there is reason to believe that the increased internationalisation of trade (sometimes wrongly called ‘globalisation’) and increased communication between governments, has resulted in knowledge about other nations’ policies (including ideas and values), instruments and institutional arrangements which, in turn, has resulted in copying, lesson-drawing and adaptation. This development has also resulted in a mushrooming body of literature within comparative political science, public administration, and traditional international politics subject areas (for a review, see Dolowitz and Marsh, 1996). Although there seems to be several competing perspectives, for example, ‘policy diffusion’ (Rose, 1993) and ‘policy convergence’ (Bennett, 1991), one should probably not exaggerate the differences. Ultimately, the literature concurs with Dolowitz and Marsh’s baseline definition in which we study:

“[the] process in which knowledge about policies, administrative arrangements, institutions and ideas in one political setting (past or present) is used in the
development of policies, administrative arrangements, institutions and ideas in another political setting” (Dolowitz and Marsh, 2000: 5).

In terms of this paper, there is reason to apply a policy transfer perspective since the Directive is undoubtedly an (external) institutional pressure which embodies ideas about values and administrative arrangements that EU member states are legally obliged to respond to. Following Dolowitz and Marsh’s ‘Policy Transfer Model’ (1996, 2000), our comprehension of policy transfer is organised around an analytical framework of core questions:

- Why undertake policy transfer?
- Who is involved in the policy transfer process?
- What is transferred (and what is not transferred) in the policy transfer process?
- What are the different degrees of policy transfer?
- What are the restraints (or facilitators) of the policy transfer process?

Although these questions are both transparent and easily applicable to our case, we argue that the complexity of the actual process points to some weaknesses in the framework, and in particular, that the process fails to fully take into account the policy implementation side of the transfer process. The latter is a significant point, as an underlying theme of this paper, is that, whilst considerable attention, in Dolowitz and Marsh’s model, has been paid to the making of policy relatively little has been paid to its implementation – with the policy process perceived to be a linear process with formation and implementation as separate stages in a process characterised by rational instrumentalism. This is a major shortcoming, as public policy rarely proceeds in such an orderly fashion and readily identifiable stages, instead it is usually more fluid and overlapping with the stages blurring and overlapping (Nakamura, 1987). Next we will briefly discuss how the questions at the heart of Dolowitz and Marsh’s Policy Transfer Model relate to the case of the EU Data Protection Directive.
4.1 Transfer motivations: why transfer?
Dolowitz and Marsh argue that the answer to the question ‘why transfer’ can be located in a continuum between voluntary and coercive forces, or between lesson-drawing and imposition (Dolowitz and Marsh, 1996: 248-249). Seemingly, the Directive is an example of what Dolowitz and Marsh would call ‘direct coercive transfer’ in which one supra-national institution, i.e. the European Union, imposes new supra-national legislation which forces the member states to amend their national legislation. However, as described in studies of the process, there is much evidence to suggest that the actual Directive was the outcome of a lengthy process (between 1990 and 1995), based on compromise and negotiation between member states, rather than a coercive top-down process (Simitis, 1995; Bennett and Raab, 1997). Simitis argues, that the final Directive is actually a patch-work of existing national legislation and not an entirely new regulatory regime. This he argues, is because some member states were not willing to replace existing national legislation and instruments:

“the endless debates in the Council of Ministers have shown too well that while Member States welcome concessions, they are not ready to accept sacrifices” (Simitis, 1995: 450).

In this perspective, there is reason to question the description of this specific policy transfer process as a pure imposition of new legislation. Also, a coercive transfer presumes unambiguous policy regulation which is hardly the case with the final Directive. As Bennett and Raab observe:

“many of its [the Directive's] provisions can be interpreted in different ways, and no doubt will be in the course of implementation. Much of its meaning is concealed within complicated wordings or within lengthy recitals” (Bennett and Raab, 1997: 252).

Policy-making in the EU is non-hierarchical, and there is no central body which can mastermind the whole process, although the Commission holds a pivotal role as an active ‘bourse’ of interests and ideas (Radelli, 2000). So we can, perhaps unsurprisingly, conclude that it is difficult to label the process as direct coercive
transfer. Instead, the policy transfer of EU data protection policy as embedded in the Directive is both coercive and voluntary at the same time. So, although it is ultimately implemented as an EU-wide instrument which member states are obliged to adhere to, its content is actually the result of a negotiated order and is shaped prior to and during implementation.

4.2 Transfer participants: who is involved?
In their original article, Dolowitz and Marsh mention nine main categories of political actors involved in the policy transfer process: (1) elected politicians, (2) political parties, (3) bureaucrats/civil servants, (4) pressure groups, (5) policy entrepreneurs and experts, (6) transnational corporations, (7) think tanks, (8) supra-national governmental and nongovernmental institutions and (9) consultants (Dolowitz and Marsh, 2000: 10). It is here important to make a distinction between on the hand those actors who were involved in the agenda-setting process leading to the transfer, and those, on the other hand, who de facto took part in transferring the policy, i.e. the Directive, to implementation in the national member states. Dolowitz and Marsh are not really concise in their presentations, and even though analyses of ‘governance’ usually stress that the boundary between policy (agenda-setting) and implementation is fluid, and is open for feed-back and learning (Newman, 2001), one should at least not analytically, and a priori, take for granted that the categories are the same. Even though there are national differences, we can already at this stage conclude that at least the Commission, the national regulatory agencies (which are given a prominent role through the Working Party clause (Article 28) in the Directive) and the community of national legal experts on privacy have been involved in the transfer. Also, there is evidence that not only the EU, but also other international organisations (such as the Council of Europe and their ‘Convention 108’) have been important players in transferring data protection policies to a number of nations (Bennett, 1988). Moreover, the Commission is given a role in the policy implementation of the Directive (Articles 25-27, 30). For our study, it is important to identify those actors involved in the implementation of the transfer and the degree to which these actors differed from those involved in policy formation.
4.3 Transfer content: what is transferred?

Dolowitz and Marsh identify eight different categories which can be transferred: (1) policy goals, (2) policy content, (3) policy instruments, (4) policy programs, (5) institutions, (6) ideologies, (7) ideas and attitudes and (8) negative lessons (Dolowitz and Marsh, 2000: 12). However, and as Dolowitz and Marsh stress, it is important to distinguish between policies and programs in which the latter is a complete course of action. In terms of what constitutes a program we can use the extensive definition provided by Rose:

“a programme is a creation of public law; a statue identifies its purposes and the conditions under which it operates. Money to finance the programme is appropriated in the budget. A specific public agency and employees are responsible for administering the programme [...]. A programme is an instrument of public policy, because it is a necessary means of achieving policy intentions” (Rose, 1993: 6).

Following this definition, the Directive is not easily defined. It is clearly more than just a policy and resembles a programme in that legislation is enacted and institutions and actors undertake administration, although the body responsible for delivering legislation does not also provide a budget for its administration, this is done at a national level. Following Bennett, the focus in this paper is what is transferred in terms of the choice of policy instruments between voluntary control, subject control, licensing, a data commissioner and registration (Bennett, 1992: 154) and whether this has changed as a result of the Directive. In his study, Bennett identifies notable differences in the selection of policy instruments in the US, Britain, Germany and Sweden. Moreover, one should bear in mind that the Directive per se is (as mentioned above) a patchwork of various national discourses on privacy, as well as national administrative practices, which indirectly have been transferred from one nation to another. Simitis mentions, for example, Article 18 of the Directive, on the obligation to notify the supervisory authority, which appears as an exceedingly bureaucratic exercise, but makes sense if one takes into account existing French law (Simitis, 1995: 451). Consequently, it is important to ask not only what is transferred directly from the EU to the respective member states, but also what national legacies have been adopted and transferred through the Directive. Therefore it also makes
sense to describe the policy transfer as a process of ‘isomorphism’ in which the forces for the change of national institutional set up can be the result of coercive, mimetic or normative sources (DiMaggio and Powell, 1991).

4.4 Transfer extent: degrees of transfer?
Dolowitz and Marsh distinguish between four different gradations, or degrees, of transfer: (1) copying, the direct transfer, (2) emulation, in which the ideas of a given policy are transferred, (3) combinations, which involve blending of different policies, and finally (4) inspiration, where policy in another (national) setting may be a vehicle for policy change, but where the actual change does not draw upon the original (Dolowitz and Marsh, 2000: 13; Rose, 1993). As already mentioned in ‘why transfer’ the degree of transfer in terms of the directive is likely to become a combination of copying and emulation. It can be considered ‘copying’ in so far that certain parts of the Directive have been directly implemented into national legislation, and ‘emulation’ in that there have been domestic variations in the implementation process. While the category of inspiration is not relevant in a study of EU member states, one should bear in mind that the Directive has been relevant in non-EU countries which, more or less voluntarily, have adopted elements of the Directive (cf. Bennett and Raab, 1997), especially those countries seeking membership of the EU. In terms of our approach, we are studying the balance between copying and emulation in the four case countries.

4.5 Transfer constraints: restraints or facilitators of transfer?
Whereas the other questions posed by Dolowitz and Marsh are not concerned with whether policy transfer is successful or not, this question touches upon the factors which influence the actual impact of the transfer, and hence determine its success or otherwise. Dolowitz and Marsh distinguish between three different factors which have a significant effect on policy failure (Dolowitz and Marsh, 2000:17). First, that the borrowing country may have insufficient information about the policy/institution and its contextual circumstances, what they refer to as ‘uninformed transfer’. Second, that a certain element of a policy, or an institution, gets lost during the transfer making the transfer an ‘incomplete transfer’. Third, are cases where little attention is paid to the political, economic, social and ideological contexts in the transferring and ‘borrowing’ country, something that Dolowitz and Marsh call
‘inappropriate transfer’. In the context of our specific case, there is, however, reason to be sceptical about the Dolowitz and Marsh framework. The underlying idea about failure in policy transfer rests on the assumption that the borrowing countries believe that the transfer will lead to success rather than failure (although this is not always the case in practice). This may be the case for voluntarily policy transfer, but cannot be taken for granted in cases of coercive transfer. Given what we already have said about the Directive there is reason to believe that at least some member states assumed that the Directive would not be a policy success. Instead, some states felt that they had to comply with the Directive, albeit only to a certain minimum level during the implementation process. Moreover, although Dolowitz and Marsh acknowledge that there can be other explanatory variables in the policy transfer process, the policy implementation process seems to be a secondary concern and issues about the actual implementation is not featured in their framework. This is a short coming, as it is at the policy implementation stage that important decisions are made regarding the actual institutional division of labour between domestic actors, the design of the national legislation, and the resources allocated to monitor and vanguard the principles of the Directive. It is also only by examining policy implementation that we can identify whether an actual transfer has taken place and also the outcome of the process, and therefore make judgements about whether transfer has been successful or not. Here, the Dolowitz and Marsh model does not really connect to the policy implementation discussion, despite their assertions that their framework can expand our understanding of the policy-making process. For our purposes, it is important discuss those elements of the transfer that have been perceived to constrain implementation, especially those elements which have led to domestic variations in policy and practice.

This discussion highlights the benefits and pitfalls of the Policy Transfer Model, on the one hand it is a useful simple heuristic device to highlight main elements of the transfer process, and on the other its over simplicity is its undoing. By examining the model’s core questions in light of the development of the Directive it is clear that the complexity of contemporary policy processes cannot be accounted for in a simple model, especially one that pays so little attention to the implementation side of transfer.
## Emergent From the Policy Transfer Model

<table>
<thead>
<tr>
<th>Policy Transfer Features</th>
<th>Emergent Empirical Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuum between voluntary and coercive forces, between lesson-drawing and imposition.</td>
<td>What are the key motivating forces that ensure implementation of the directive? To what extent has the Directive been appreciated / understood as coercive? To what extent did the Directive make a difference to existing legislation?</td>
</tr>
<tr>
<td>Actors: elected politicians, political parties, bureaucrats/civil servants, pressure groups, policy entrepreneurs and experts, transnational corporations, think tanks, supra-national governmental and nongovernmental institutions and consultants.</td>
<td>Who has been involved in the formation of the Directive and who have been involved in its national implementation? To what extent are the same actors involved in policy formation and implementation?</td>
</tr>
<tr>
<td>Content of transfer: policy goals, policy content, policy instruments, policy programs, institutions, ideologies, ideas and attitudes and negative lessons.</td>
<td>Which policy instruments have been applied to ensure implementation of the Directive? Has implementation of the Directive resulted in the enactment of new national legislation and the creation of new regulatory agencies? What national legacies (i.e. pre-Directive instruments) remain? Are all elements of the Directive compulsory or is there an element of choice?</td>
</tr>
<tr>
<td>Type of transfer: copying, emulation, combinations, and inspiration.</td>
<td>Is policy transfer similar across all EU member states? Is implementation of the Directive primarily copying or emulation? Does new national legislation compliment the Directive?</td>
</tr>
<tr>
<td>Extent of transfer: uninformed transfer, incomplete transfer and inappropriate transfer’</td>
<td>What constraints have there been in implementing the Directive? Have there been problems in interpreting the intentions of the Directive? Has public debate influenced the implementation process? Has implementation of the Directive been successful? How is the success measured? Has the Directive subsequently been amended or adjusted?</td>
</tr>
</tbody>
</table>

(Adapted from Dolowitz and Marsh, 2000.)
Using the core questions at the heart of the Policy Transfer Model it is possible to raise a further set of questions which relate specifically to the implementation of the Directive, or its transfer into national settings. These questions, presented in table 3, stress the myriad of relationships, institutions, actors and activities involved in implementation, as opposed, or in addition to policy formation. They include important questions about whether the Directive has initiated new policy instruments, about whether the Directive is perceived to be coercive or advisory, about whether national pre-Directive legacies remain, and about whether the Directive is seen to be successful, and if so how this is determined. Table 3 sets out the Policy Transfer Model’s core questions, the features underpinning each question, and the questions/issues raised in relation to the implementation of the Directive. By approaching policy transfer from this direction (policy implementation), the interrelated linkages and differences between policy formation and implementation become more transparent, as do the important roles played by national institutions. These questions are utilised to guide our empirical observations in the next section of the paper. Not all questions are applied to each case, instead they are discussed as appropriate.

5. Policy Transfer or Evolution? Implementing the Directive in Four EU Member States: Denmark, Sweden, the UK and Scotland

The deadline for implementing national data protection legislation complimentary with the Directive by EU member states was October 1998. By this time only four countries, Greece, Italy, Portugal and Sweden, had adopted the Directive in their national legislation. Even by 2002 several countries, including France and Germany, had still not fulfilled their obligations under the Directive. In relation to the four case studies explored here a number of pieces of national legislation were enacted or amended by the October 1998 deadline. In Denmark six ‘national execution measures’ were adopted, in Sweden twelve and in the UK just one (European Commission, 2008). The rate of transfer suggests that either existing legislation was entirely complementary with the Directive, or possibly that member states did not readily acknowledge the coercive requirement to fulfil the obligations of the Directive.
To ensure that member states complied with the obligations and intentions of the Directive an EU Working Party (under Article 29) was established and charged with producing annual reports about the development of data protection in member countries. The most recent was published in 2007 and provides interesting reading (European Commission, 2007). In the opening statement Peter Schar, the Chairman of the Article 28 Data Protection Working Party, states:

“for the future it remains important that, in the interests of all data subjects, further legal and practical steps are taken in order to achieve a high-level harmonisation of data protection, and, in particular, governmental responses to security threats should not result in unacceptable restrictions in civil liberties or infringements of established data protection legislation” (European Commission, 2007: 8).

Implicit in this statement is recognition that data protection laws remain different across EU member states, despite adoption of the Directive some ten years earlier, and also that certain member states were introducing measures to combat terrorism and ensure national security which actually contradicted fundamental principles enshrined in the Directive. Such a statement points to the implementation of the Directive as being less coercive and more a process of constant negotiation renegotiation and revision.

The first official report on how the Directive was being applied, as mandated by Article 33 of the Directive, reported on the results of consultation with the various parties affected by the Directive. Much of this consultation was with the national government and data protection authorities in member states, as well as data controllers and data subjects. According to Bygrave (2002), two underlying themes that emerged from this consultation was the lack of harmonisation of EU Member States' respective data protection regimes and the ambiguity of many of the terms and rules in the Directive, with the latter possibly resulting in the former? Data protection laws are expected to establish a climate of certainty, for both data controllers and data subjects, who need to be clear on their rights and responsibilities. This depends on the clarity of legal definitions. One problem with existing data protection law, including the Directive and national legislation, is that
many of the terms are ambiguous, their intentions not always clear, and sometimes there are different meanings (and interpretations) in different national jurisdictions. This results in a climate of uncertainty and potentially the imposition of contradictory instruments.

5.1 Denmark
Prior to the adoption of the Directive in 1995 by the Council of Ministries Denmark was one of the countries which was opposed to the imposition of data protection legislation. This is expressed, for example, in the first governmental report on the ‘information society’ in 1994 (Ministry of Research, 1994; Blume 1995) in which the proposals for a new Directive were described as hampering the development of new ICT services across Europe. Nevertheless, the Danish implementation process under the ‘the Register Law Committee’ was given the clear objective of implementing the EU Directive within the specified time frame. The committee, composed of members from both the public and private sectors, presented their final report in December 1997 (Betænkning1345/1997). According to Blume (2003: 27) the committee was working under the premise (or understanding) that the EU Directive set tight premises for the implementation process which could not be ignored or deviated from. The final act, the Act on Processing of Personal Data (Act No. 429 of 31 May 2000), which entered into force on 1 July 2000 contained several deviations from the EU Directive, and is, according to Blume, on the edge of violating the Directive (Blume, 2003).

There are a number of notable differences between existing legislation in Denmark and the legislation deriving from adoption of the principles of the Directive. One difference is that prior to the Act on Processing of Personal Data Denmark had different regulation for the private and public sectors - ‘The Public Authorities’ Registers Act’ and ‘The Private Registers Act’. More significantly, the public sector’s use of personal data was heavily regulated by four different pieces of legislation. At the time the Register Law Committee merely advised that revisions of the public sector legislation in terms of personal registers was all that was required to fulfil the needs of the Directive. This caused problems at a later date in the parliamentary process when it became clear that simple revisions would not suffice. A second important issue which also caused problems at a later date was in relation to the
protection of personal data on the internet. On this issue the Committee chose not to take a position, instead assuming protection would be provided by general principles. A further difference, according to Blume, was that the old legislation did not provide citizens with sufficient protection for personal data protection, whereas the implementation of Directive secured much higher levels of personal data protection (Blume, 2002:83).

The Register Law Committee played a vital role in the national implementation process in Denmark with the composition of the committee made up of the usual Danish stakeholders, including representatives from; the relevant ministries, local and regional authorities, legal societies and industry. Other interests, such as, the Danish associations of journalists were also consulted. Several other interested parties voiced their concerns about the new legislation after the publication of the committee report. Additionally, political parties played an important role during the legislative process in Parliament. During the legislative process the first governmental act proposal was not appreciated by the Standing Judicial Committee in Parliament which issued no less than 139 formal questions, many of which related to unclear or ambiguous wording. According to Blume (2003: 29) the process was characterised by a ‘nostalgia and a somehow illusory belief’ that the register laws were clear and understandable to everyone. In practice, limitations in the new legislation were addressed by a series of amendments and revisions initiated by the new Danish Data Protection Agency. The Danish Data Protection Agency has been the driving force in maintaining up to date data protection legislation and also in making administrative decisions on how to interpret the legislation and the Directive. The agency also makes inspections and since 2000 has begun to employ communicative instruments to ensure a better appreciation of data protection principles across Danish society and industry.

The main implementation problems in Denmark were, according to our sources, problems with understanding the terminology and principles of the new Directive, especially amongst parliamentarians, and issues associated with the desire to retain existing national legislation. However, and unlike in Sweden, the process of implementing the Directive in Denmark, via new legislation and regulatory agencies,
did not provoke extensive public debate and discussion was kept within the realms of parliament and government.

5.2 Sweden

Sweden’s Data Protection Act of 1973 was the first comprehensive data protection legislation at a national level in Europe. However, in June 1995, shortly after the Council’s adoption of the Directive, the Swedish government instigated a parliamentary commission of inquiry to implement the new Directive and also to propose a complete and thorough revision of the existing regulatory Data Protection Act (Terms of Reference: 1995/91). Although this commission was allocated resources and expertise (mainly legal experts), there are some commentators who argued that the short time-frame (15 months) and contradictory aims (see below) made it extremely difficult to deliver the inquire’s core objectives (Ilshammar, 2002: 170; Olsson, 1996: 33). In terms of the EU Directive, it is apparent that the commission, as noted in the final commission report (SOU 1997:39), did not interpret the Directive as a ‘minimum directive’ (ibid. 108). Consequently, different stipulations on data protection were implemented in accordance with the Directive.

The new Swedish legislation deviated from the old Data Protection Act (1973) in five important respects (according to Ilshammar, 2002: 175). Firstly, the new act included all personal data, including paper based data, which is a significant difference to previous legislation which only included computerised personal data. Secondly, the new act prohibits, in principle, all registration of personal data (with lots of exceptions) whilst the old legislation was based on permissions following individual applications to the agency. Thirdly, while the old legislation stipulated that individual consent was a ‘praxis’, the new legislation demanded ‘unambiguous informed consent’ from each individual. Fourthly, the new act made exemptions from consent for journalistic, literary and artistic work. And finally, the act introduced a ban against export of personal data to third countries. The one major difference between the Directive and the new Swedish law was the exemptions in the new act with respect to the Swedish constitutional principle of public access to official documents (which is part of the Freedom of the Press Act) and through which citizens can get access to public information and records. The final legislative act,
the Personal Data Act is perceived by some as a ‘copy’ of the Directive with alternative interpretations of the Directive discarded (Ilshammar, 2003).

Beyond the implementation of new legislation it is also apparent that a range of actors were involved in the ‘domstification’ process. The commission was put under auspices of the Ministry of Justice with the original commission of inquiry composed mainly of parliamentarians from the Swedish ‘Riksdag’ and some senior civil servants. They were, however, assisted by a wider group of legal experts and practitioners, as well as actors from the courts (on different levels), public agencies, private trade associations and the mass media, some of which presented critical comments about the implementation of the Directive in Sweden. During an assessment of the bill a couple of years later the Ministry of Justice asked for a broader set of opinions from society. Among those making presentations were several public agencies, courts, trade associations and individuals, the views of which were collected in an internal report (Ds 2001:27). In this respect the implementation process has been relatively ‘open’ with possibilities for a range of different actors to get involved.

In addition to the provision of legislation, the implementation of the Directive in Sweden resulted in the establishment of other regulatory measures and instruments. These too were enshrined in new legislation. The Swedish ‘supervisory agent’ – the Data Inspection Board – has got some legal instruments at their disposal and may prohibit any data controller (on pain of a fine). The Board may also apply to the County Administrative Court of the erasure of data that has been processed in an unlawful manner. Apart from these pure legal instruments, the supervisory agent has mainly communicative instruments to employ in their efforts to secure the compliance of the Directive, such as, for example, establishing information channels and the cooperation with other actors through networks (Data Inspection Board, 2008).

Several points of criticism were brought forward, both during the committee process and afterwards prior to the adoption of the new act in Parliament. One unexpected area of conflict was the concession of the abuse centred principle, which also existed in the old Swedish Data Protection Act (1973), in favour of the Directive’s
requirement in which all data processed information is encompassed by the legislation. Whether Sweden actually could retain this element of the old model became an issue even after the adoption of the new act. Most of the actors involved in the remit process were in favour of an abuse centred principle. However, based on Illshammer’s (2002) review of the responses it is possible to conclude that there is was clear pattern of positive and negative responses based on, for example, private – public actors. Even legal opinion was divided on whether Sweden could maintain their old computer law principles.

A second substantial issue that emerged during the transfer process was whether the constitutional principle of public access to official documents in Sweden was about to be overruled by the implementation of the Directive. A strict interpretation of the Directive could have resulted in the end of a 200 year legal principle allowing the public access to all official information (including personal information). This was a principle that was unique to Sweden (and Finland), at the time, and the general view was that there was little chance of concessions, or even understanding from the rest of the EU. However, in the process of ratifying national legislation this principle was upheld, despite contradicting the Directive. This was achieved by omitted all references to the principle of public access when drafting the Act. The issue that this course of behaviour contravened the Directive was dealt with by another committee which in the final report suggested maintaining the public access principle. A view which was later ratified by Parliament (SOU 2001: 3). In addition to these two main points of criticism, several of the actors who were consulted during the remit circulation, prior to the government’s final proposal, expressed minor concerns regarding economic consequences of the proposal, especially in relation to the ban on export of personal data to third countries, and that the proposal represented a threat to the freedom of speech. These voices did not affect the final proposal of the act.

A more interesting criticism is the one expressed in a second public hearing (through a web based survey) in which the Ministry of Justice asked for opinions about the new Directive. The result was presented as a Ministerial Memorandum (Ds 2001:27) which presented several critical voices, in particular from public
agencies. According to this study the main problem seemed to be the unclear definitions of personal data, as well as, in which situations the legislation was applicable. In terms of public debate, the actual law proposed in the autumn of 1998 did cause some turmoil, especially the assertion that the law would mean a ban on publishing individual names on the Internet and that the freedom of speech was at stake. However, this public debate only lasted a week on the front pages of the main Swedish newspapers.

5.3 United Kingdom
Data protection has been a policy issue in the UK since the late 1960’s and was initially the subject of UK Parliamentary Private Members Bills and Committee Reports calling for varying degrees of privacy legislation. The Younger Report on Privacy (HMSO, 1972) and the Lindop Report on Data Protection (HMSO, 1978) established broad principles for regulating data processing and privacy. Both recommended a flexible legal approach but neither was legally binding or taken up in legislation. In 1984, and to ensure British companies were not disadvantaged against their European competitors, the UK Government, begrudgingly according to Warren and Dearnley (2005), passed the Data Protection Act (see Warren and Dearnley (2005) for a review of data protection in the UK in the period preceding the enactment of the 1984 Data Protection Act). By that time, the UK had lost its lead in defining data protection policy, established by the Reports of Younger and Lindop, and was coming under increasing international pressure from the EEC (Council of Europe, 1981), OECD (OECD, 1999) and other nation states to adopt privacy and data protection practices. The Data Protection Act of 1984 was the first British legislation concerning data protection. It only applied to data stored on a computer and was primarily concerned with the free flow of information and not the protection of privacy. The 1984 Act adopted the general principles of the OECD Guidelines (1999). It created a public register of those organisations in both the public and private sectors that processed personal data, administered by an official known as the ‘Data Protection Registrar’, who was given powers of enforcement. The Act established new rights for individuals, the most important of which were the right to know if an organisation was processing personal data about them and the right to have a copy of the information (the right of subject access). Individuals also had a right to complain to the Registrar. The 1984 Act was limited in its effect, its
The enforcement regime was cumbersome and linked too closely to the register, and there was no recognition of Data Protection as a privacy matter. Nevertheless, the Registrar gradually established a jurisprudence that significantly improved standards associated with the processing of personal data (Raab, 1996).

At this time the Conservative led government in the UK was unconvinced that separate legislation was required to protect personal data and privacy, and consequently unreceptive to the idea of a Europe-wide data protection Directive. As a result of this standpoint UK policy-makers and politicians had very little influence on the shaping and emergence of the EU Directive on Data Protection. During this period it is clear that the motivating forces shaping the emergence of data protection practices in the UK were commercially driven and were not associated with a desire to protect personal privacy. Following the election of the New Labour government in 1997 this position altered with data protection seen as part of a broader concern with citizens' human rights. The Data Protection Act 1998, implementing Directive 95/46/EC, was passed on 16 July 1998 and came into force in 1 March 2000. The Act transposes the provisions of the Directive into UK law, although much of the detail was left to secondary legislation, with 17 Statutory Instruments required before commencement (more have been introduced subsequently). Other relevant legislation which make a significant contribution to the framework within which data protection is interpreted and applied in the UK includes the Human Rights Act 1998 and the Freedom of Information Act 2000.

The UK Data Protection Act of 1998 was more explicit in recognizing individual's right to privacy, especially in relation to the processing of personal data. It specified conditions for the processing of data, tightened restrictions on the use of particularly sensitive information and broadened the definition of data to include some details held on paper. The purpose of the Act is to protect the rights and privacy of individuals and to ensure that data about them is processed only with their knowledge and consent. For this, the Act gives individuals certain rights regarding personal information held about them and places certain obligations (in the form of eight principles) on those who process the personal information. The act covers eight 'Data Protection Principles', which are essentially the core principles promoted by the EU Directive. These state that all data must be: (1) processed fairly and
lawfully, (2) obtained and used only for specified and lawful purposes, (3) adequate, relevant and not excessive, (4) accurate, and where necessary, kept up to date, (5) kept for no longer than necessary, (6) processed in accordance with the individuals rights (as defined), (7) kept secure, and (8) transferred only to countries that offer adequate data protection.

The 1998 Act also separated the functions of registration and enforcement and increased the powers of what is now known as the Information Commissioner (previously the Data protection Registrar), and the Information Commissioners Office (ICO). The functions of the independent Commissioner are set out in section 51 of the Act. Section 51(1) states that the Commissioner should promote good practice by data controllers, and promote the observance of the Act. 51(2) states that the Commissioner should advise the public about the operation of the Act and 51(3) states that the Commissioner should prepare and disseminate codes of practice. The Commissioner also assesses the observance of data controllers to the Act, and can order compliance and undertake prosecutions. If a data subject feels that a data controller has not complied with the Act then the data subject has: the right to complain to the ICO who will then investigate and if needed serve an ‘information notice’ or an ‘enforcement notice’ in case of non-compliance, and the right to sue the data controller. The Act also treats it as a criminal offence if a data controller: having received a subject access request destroys the data rather than disclose it or discloses personal data without the authority to do so. It is also a criminal offence if a data subject: does not comply with an enforcement notice or knowingly or recklessly obtains, discloses or procures the disclosure of personal information without the consent of the data controller. In addition to its UK responsibilities, the ICO has an international role including cooperation with similar organisations in the rest of Europe and with the European Union. Non-legislative instruments deployed by the Information Commissioner include the publication and promotion of standards in the form of Codes of Practice, for example the CCTV Code of Practice (ICO, 2008), and a ‘DPA Toolkit’, a downloadable set of MS-Word (and PDF) documents intended to guide individual and organisation through the act and the compliance process.
The adoption of the Directive embodied in 1998 Data Protection Act suggests that privacy regulation in the UK has converged with other EU nations. However, unlike other European legislation the Act only enforces the theoretical minimum standards required by the Directive. Moreover, there is evidence to suggest that the transfer of the Directive into UK law has been superficial and that privacy regulation in the UK is not actually compatible with the Directive or other European national legislation. Currently the European Commission is investigating whether eleven of the Directive’s thirty four Articles, so about a third of the entire Directive, have actually been implemented in the UK. The Commission has initiated negotiations to resolve this matter and have threatened proceedings before the European Court of Justice if negotiations with the UK stall (Dyer, 2007). Further concerns about the enforcement capacity of the Data Protection Act and the Information Commissioner also point to serious limitations to privacy protection in the UK. The Data Protection Act has become known as ‘the toothless act’ because there is relatively little the new regulatory instruments can do to ensure compliance with the Act (or the Directive), despite the principles of data protection now having the force of law behind them. In a written answer to a parliamentary question in 2007, Vera Baird the Justice Minister, stated that since the Data Protection Act 1998 can into effect on 1 March 2000 there had been (just) twenty six successful prosecutions for non compliance under the Data Protection Act (Baird, 2007). Moreover, the penalties imposed for these prosecutions included; a conditional discharge, 150 hours of community service and twenty four fines totaling £22,250 - hardly a deterrent to further infringements (Baird, 2007). In the UK it is clear that the transfer of privacy regulation via the Directive is an ongoing process involving both coercive and voluntary forces.

5.4 Scotland

Of the four case studies considered here Scotland is unique in that it is under no obligation to adopt the data protection principles of the Directive. This is primarily because Scotland is not a member state of the European Union but a devolved regional administration within the UK, and as such, it is the UK government (as an EU member state), and not the Scottish Government, that is obliged to harmonise its legislation with the Directive. So, despite having its own legislative and legal systems Scotland has not instigated any data protection legislation. This can further be explained by the remit of the Scottish Government (formally the Scottish
Executive) and Parliament, as set out in the Scotland Act 1998, and under which matters relating to EU Directives including data protection are ‘reserved’ for the sovereign Parliament at Westminster. And in any event, the Directive came in force before devolution in Scotland.

Despite this, it is apparent that a regulatory regime around privacy has started to emerge in Scotland. Scotland has its own Information Commissioner, a regulatory agency, also called ‘The Scottish Information Commissioner’ and has initiated new Freedom of Information legislation (the Freedom of Information (Scotland) Act 2002). This legislation has a bearing on the flow of information and data in that it governs access to public information and records. It also places on public authorities a range of duties in respect to how they retain records and process requests for information. The result of these developments is that the UK now has a dual access regime, one specifically for Scotland and one for the UK (the UK Freedom of Information Act 2000). This organisational arrangement could result in overlapping or conflicting responsibilities, for example where requests for access involve personal information and could be demanded under either the UK Data Protection Act 1998 or the Freedom of Information Act (Scotland) 2002. Interestingly then, the transfer of data protection principles into Scottish legislation and other regulatory instruments has occurred voluntarily. This may not involve the full transfer of the Directive into Scottish legislation, but certainly some of the intentions of the Directive are being transferred into the newly emerging devolved regulatory regime.

6. Concluding Discussion
This paper has covered a lot of ground around the transfer and implementation of the EU Directive on Data Protection into national settings, especially in relation to the 4 cases of Denmark, Sweden, the UK and Scotland. Consequently, extended discussion could cover a range of topics, including; the nature of privacy regulation in Europe, the characteristics of the transfer process surrounding the Directive, and a critique of the utility of the theoretical approach adopted by the Policy Transfer Model. We will touch briefly on all three.

In essence the emergence of data protection legislation, at both the national and EU level, is an exercise of the power of the state in regulating the processing of personal
data. As such, it is a manifestation of policy and political processes which encapsulate a range of vested interests and which could, and does, lead to non-legislative regulatory outcomes as well, for example in the form of non-legislative policy instruments. These policy processes also determine the scope of data protection and its purpose. Despite the notion of convergence embedded in EU policy, and manifest in the Directive, the extent of harmonisation, or rather the lack of harmonisation, as illustrated by the 4 cases considered here, highlight the plurality of regulatory regimes and multiplicity of regulatory practices. So, although there is an illusion of harmonisation, through the adoption of new data protection legislation and regulatory agencies, national legal systems dealing with privacy issues are not uniform, with the administration of the new data protection apparatus (legislation and agencies, etc) varying considerably. Primarily, because they are entrenched and shaped by existing legally and political processes in each national setting. Additionally, the case studies show that different aspects of the Directive are problematic in different countries and that the new supervisory agents are given different levels of legal authority and competence in each different country. In this respect, the case of the EU Directive on data Protection is not a ‘true’ case of direct policy transfer, but of policy evolution, in which policy convergence and divergence is happening simultaneously in multiple countries and is best understood by taking into account the powerful vested institutional interests that shape policy development in each discreet national setting. On the face of it, this perspective suggests a very bleak outlook for the development of EU policy, as it suggests that member states will bend proposals and Directives to fit neatly with existing national arrangements, at the expense of broader harmonised policy. This, however, is not the view we ascribe to here. Instead we would argue that the EU and its policy instruments, such as the Directive discussed in this paper, are also part of the institutional framework of each member state, and consequently a force, along with many others, influencing behaviour and change. Policy therefore evolves from an environment containing a range of intertwined relationships and the development of policy and its implementation is subject to revision, amendment and adjustments as the various actors ‘muddle through’ the process. The EU Directive considered here is therefore both coercive and voluntary at the same time.
From this discussion it is clear that the policy transfer process is not static but a continually evolving process. This is a significant point, especially in the field of new ICTs, where technological advances are rapid and regulatory arrangements, if they are to be effective, need to keep pace with the technology. Further to this, because of the number of counties involved in adopting the Directive, multiple transfers are occurring simultaneously. Moreover, because different counties have different histories of legislation and practice in the data protection area, they offer different levels of personal privacy. Some comply with the minimum standards enshrined in the Directive, such as the UK, whilst others, such as Sweden, offer much higher levels. This again highlights the importance of the national settings encompassing privacy regimes and also illustrates the different privacy ‘trajectories’ in each member state.

Turning to the Policy Transfer Model, a further set of observations can be made. Primarily that the simplicity of the model demonstrates both its utility and its deficiency. So, although it is extremely useful in highlighting the main elements of the transfer process it barely scratches the surface of the complexity of these processes. Also, that the model by seeing policy transfer as a top-down process fails to recognise the extent to which policy implementation has a bearing on the transfer process. In analysing the policy transfer surrounding the adoption of the EU Directive on Data Protection we have argued that transfer does not occur in a vacuum and is instead shaped by historical national settings, and that these settings are reflected in the policy being transferred and its implementation in practice. In this respect, and in the case of the Directive, the policy being transferred cannot be separated from its environment. So, policy transfer is arguably better described as policy evolution. Also, it’s worth bearing in mind that the transfer of the Directive into divergent national practice is not a manifestation of the failure of policy transfer, as the Policy Transfer Model would suggest, but a reflection of the forces that shape and determine implementation. So, policy transfer (or evolution) takes place, but it is different in different national settings as different interpretations of the Directive emerge.

In summary, this paper makes a number of useful observations about the policy transfer processes surrounding the adoption of the EU Directive on Data Protection.
Policy transfer is an evolutionary process which is both simultaneously coercive and voluntary. It is a complex process involving multiple transfers, a range of actors, agencies and instruments, which are shaped by powerful vested interests, and which are far from uniform in practice. Moreover, embedded in the transfer process are forces resistant to change. Nevertheless, a degree of convergence is the logical long-term outcome of the Directive, though the policy processes leading to this convergence are likely to be messy and complicated and the result of a negotiated order.

Bibliography


European Commission. (2008) **Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data.**


The (Danish) Act on Processing of Personal Data (Act No. 429 of 31 May 2000).


Terms of Reference 1995/91 for the Inquiry committee on a new Personal Data Act (Sweden).


