

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

Karl Lofgren, University of Roskilde (corresponding author)

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

Dr C. William. R. Webster

School of Management

Division of Business and Organisation

University of Stirling

Stirling, FK9 4LA

Tel: 01786 467359, Fax: 01786 467329

Email: c.w.r.webster@stir.ac.uk

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

Abstract

This article examines policy activity surrounding the implementation of privacy regulations in three European countries, Denmark, Sweden and the UK, following the ratification of the 1995 European Union Directive on Data Protection. It highlights the convergence and divergence of policy embedded in the policy transfer process and stresses not only the complexity of policy transfer, but also the degree to which policy innovation is shaped by existing institutional settings and the processes associated with policy implementation. The article uses Dolowitz and Marsh's 'Policy Transfer Model' as an analytical tool to unpack the regulatory environment surrounding the governance of privacy. This illuminates the main features of the policy process in each of the three case study countries and also the tendency to focus on policy formation at the expense of policy implementation. In the case of the 1995 European Union Directive on Data Protection the three cases examined here demonstrate that multiple regulatory regimes and policy divergence are embedded in the harmonisation (or convergence) process, and that different countries approach the regulation of privacy and data protection in quite different ways.

Keywords

Data Protection, Policy Transfer Process Model, European Union Directive on Data Protection (95/46/EC), Privacy Regulation

1. Introduction

This article examines policy activity surrounding the implementation of privacy regulations in three European countries, Denmark, Sweden and the UK, following the ratification of the 1995 European Union (EU) Directive on Data Protection [26]. 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' [19]. In doing so, the article highlights limitations with the 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. We are not arguing for the rejection of the model, but a theoretical refinement which considers more explicitly policy implementation. In terms of policy innovation, we seek to perceive the policy processes surrounding the Directive as incremental 'policy-innovation processes' in which certain national institutions and normative and epistemological 'values' affect the outcome of a European policy. By including both agenda-setting and subsequent implementation processes we are able to conclude that policy innovation, in a field such as privacy regulation, highlights the sensitive nature of introducing new regulatory activity and institutions into discreet national settings.

The starting point for the article is the 1995 EU Directive on Data Protection - hereafter referred to as 'the Directive' [26]. 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 myriad diverse regulatory policy arrangements that previously existed across Europe. 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 [5, 49]. 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 [49].

This article analyses the extent to which, and in what ways, the implementation process of the Directive on data protection diverge *vis-à-vis* each other in Denmark, Sweden and the UK. There are different reasons for choosing these three countries. Firstly, they are all perceived to be 'Euro-sceptical'. While British euro-scepticism goes without saying, there is also plenty of evidence pointing to wide-spread Euro-scepticism in both Sweden and Denmark [1]. This similarity could suggest a common resistance to EU Directives and similar national implementation processes – although in this article we will demonstrate that this is not the case. Secondly, the selection of Denmark, Sweden and the UK for comparative purposes was based on the 'most-different-design' approach associated with Przeworski and Teune [46]. Sweden has a long history of privacy related legislation. It has had a Freedom of Information Act since 1766 and was an early adaptor of data protection legislation, implementing its Data Protection Act in 1973. By contrast, the UK did not develop data protection legislation until 1984 and arguably did so reluctantly [47]. In this context, Denmark represents the selection of a case somewhere between these two extremes.

The article departs from much of the established literature on privacy in three main ways. Firstly, it 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 [6].

This is achieved in this article by using Dolowitz and Marsh's Policy Transfer Model as an analytical tool to unpack and comprehend activity around the 'transfer' of Directive into national settings. The intention here is to apply a mainstream political science approach in order to take analysis of the Directive away from traditional quasi-legal analysis. Secondly, the concept of privacy is intentionally broadened to go beyond narrow quasi-legal definitions of personal data to include other aspects associated with the governance of privacy. In particular, the focus is shifted to actors and institutions influencing the provision of privacy related regulations and the handling of information. Thirdly, the paper also departs from much of the published literature by placing at the heart of its analysis international comparative case studies. The need for comparative research in this area is a point raised by both Bennett and Raab [3, 4, 5, 6]. Such an approach illuminates the processes and national settings through which privacy is regulated and the multifaceted nature of privacy governance. This is not the first study to take a comparative approach to exploring this topic area. In 1992, Bennett [3] compared data protection practices in the UK, US, Sweden and Germany, and in 1989 Flaherty [27] in his book entitled 'Protecting Privacy in Surveillance Societies' examined data protection in Germany, Sweden, France, Canada and the US. This article builds on this comparative tradition with contemporary analysis that takes into account policy developments from the mid 1990s onwards.

Methodologically, the article derives from a combination of qualitative studies of official policy documents, informal discussions with policy officers and academics, and previously published research and media output. It is important to point out that we have gone beyond the formal and legal elements of the transfer of the Directive and have also sought to encapsulate 'policy discourse' from an interpretive policy analytical perspective [62].

The remainder of the article 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 our understanding of it in light of theories on policy innovation. This is followed by section 5 which explores the implementation of the Directive in three 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 1980s. 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. National approaches to data protection were influenced by the Organization for Economic Cooperation and Development's (OECD) guidelines for 'Governing the Protection of Privacy and Trans-Border Flows of Personal Data' [43] and the Council of Europe's 1981 Convention for the 'Protection of Individuals with Regard to the Automated Processing of Personal Data' (ETS. 108), which required signatories to apply certain principles to handling of personal data [16]. In this period, the emergence of public policy, legislation and agencies was largely a response to the pace of technological change and the increasing importance of information and data. Although the Directive signifies a common approach to European regulation, the concept of privacy has continued to be an abstract and contested notion [42] with a proliferation of different definitions [37]. 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' [6]. The combination of this sort of activity is referred to by Newman and Clarke [40, 41] 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. More specifically, and in relation to the governance of privacy, Bennett and Raab [6] 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.

++++INSERT TABLE 1 HERE++++

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 [6] argue that privacy regulation is made up of 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 Bennett and Raab the multifaceted nature of privacy regimes can be used to help explain how the divergence of data protection practices emerge in different national setting alongside broader harmonization processes [3, 6, 49].

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'. Ideas and values about how to govern privacy are consequently 'transferred' around the policy environment, between actors and nations, with a degree of regulatory conformity subsequently emerging across nation states [3, 49].

3. The 1995 EU Directive on Data Protection

The EU 1995 Directive on Data Protection, referred to as 'the Directive' in this article, was ratified by European Parliament and the Council of Europe on 24 October 1995 and came into effect in October 1998 [26]. 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)¹. 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

¹ Full text of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 can be found at, URL: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>, and http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

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 data². For some commentators these twin goals were incompatible from the outset, as the data needs of commercial companies were always going to be quite different to those of individual citizens [33].

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 [3, 5, 7]. In 1980, in an effort to encourage 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' [43]. The OECD Guidelines were not binding and data privacy laws in the 1980s varied considerably across Europe. In 1981 Council of Europe agreed its Convention for the 'Protection of Individuals with Regard to the Automated Processing of Personal Data' (ETS. 108), which as a European 'Treaty' would have binding force upon its signatories [16] and therefore encouraged a degree of standardisation. In the 1980s, 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. Initially the Commission called for member states to ratify the Council of Europe's 1981 Convention. 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 1990s two proposals for a Directive on data protection were presented, one in 1990 followed by revised proposal

² Human Rights legislation enacted by national governments and the EU include aspects of privacy protection. See for example Bygrave [15].

in 1992. 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 compromises, as well as the antagonistic positions of certain actors/nations. 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 [3]. 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 some of these policy sectors exempted from national transpositions of the Directive [25].

In line with European treaties which underpin the formation of the EU 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 [3, 5, 6]. 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 [7]. The Directive contains 33 Articles in eight chapters and contains six basic tenets: notice, choice, use, security, correction, and enforcement. These core characteristics of the Directive are summarised in table 2 (see Lloyd [33] for a more detailed review of the Directive).

+++++ INSERT TABLE 2 HERE ++++++

In addition to these overarching principles the Directive specifies the nature and function of each member states' 'supervisory authorities', which through the Directive become mandatory and which are endowed with powers to monitor the application of the Directive.

These supervisory 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 authorities 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 [6]. 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 adherence to the Directive. These authorities therefore play a critical role in national implementation of the Directive [6].

The ratification of the Directive in the mid 1990s signals the culmination of over fifteen years of policy negotiation and political manoeuvring amongst EU member states. It also signals the start of the process by which member states were obliged (legally bound) to implement, or adjust, their own legislation and practice to comply with 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 comprehended.

In terms of policy innovation, the Directive can be seen to be innovative in a number of ways. Here, policy innovation is understood to be the new aims and objectives, strategies, and underlying principles that signify an approach that is different to previous policy. Therefore, utilising the work of Hartley [28], the Directive can be seen to be both a ‘process innovation’ and a ‘governance innovation’, since it initiates the administrative reorganisation of data protection at the local (national) level while incorporating central (EU level) governance

arrangements. Hartley argues, that policy innovation is usually multidimensional in this way and it should be no surprise that different elements of an emergent policy appear innovative [28]. However, in this article, we argue that although policy innovation is multidimensional, what is perceived to be innovative in one country is not necessarily the case in another.

4. The Policy Transfer Process

While policy transfer between nations is not a new phenomenon, there is reason to believe that the increased internationalisation of trade and increased communication between governments, has resulted in knowledge about other nations' policies (including ideas and values), instruments and institutional arrangements has resulted in copying, lesson-drawing and adaptation, including across EU member states [13]. 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, [20]). Although there seems to be several competing perspectives, for example, 'policy diffusion' [51], 'policy convergence' [4], and not at least the burgeoning 'Europeanization literature' [50], one should probably not exaggerate the differences between these perspectives. In terms of this article, 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 to which EU member states are legally obliged to respond. In relation to data protection, a previous study, by Bennett [3, 5] examined policy convergence in four countries (UK, US, Sweden and Germany). It highlights four different convergence processes: 'determinism', the identification of similar problems, 'emulation', 'harmonisation', and finally 'penetration', as levels of policy convergence. Although the comparative empirical analysis in this work is useful, it is not able to account for recent developments in the role and function of the EU, the pace of technological change or new data protection initiatives, including the Directive itself. Following Dolowitz and Marsh's 'Policy Transfer Model' [19, 20], 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 would benefit from insights from theories of policy implementation and innovation. Policy transfer is not solely a process of the trans-national diffusion of ideas, but is also a factor that fosters policy innovation and development. For example Berry [8] argues, that policy innovation cannot be assumed to derive directly from a central agency, as the flow of ideas can transfer between agencies at the local or service delivery level and ultimately these 'local' organisations adopt new policies for a local reasons as well as centralised national reasons. The latter is a significant point, as an underlying theme of this article 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, and with a less distinct understanding that policy innovations are often incremental in nature. 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 with the stages blurring and overlapping [39].

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 [20]. 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 EU, imposes new supra-national legislation which forces member states to amend their national legislation. However, as described in studies examining the ratification of the Directive, there is evidence to suggest that the final 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 [7, 52]. 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 [52]. In this perspective, there is reason to question the description of this specific policy transfer process as the pure imposition of new legislation. Also, a coercive transfer would suggest the implementation of unambiguous policy regulation, but the case studies presented in this article show this not to be the case.

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 [50]. 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. Moreover, in relation to policy innovation, we can ask the question of whether the Directive represents an improvement in a nation’s data protection policy and practice?

4.2 Transfer participants: who is involved?

In their original article Dolowitz and Marsh list nine main categories of political actor involved in the policy transfer process: elected politicians, political parties, bureaucrats/civil servants, pressure groups, policy entrepreneurs and experts, trans-national corporations, think tanks, supra-national governmental and nongovernmental institutions and consultants [20]. It is important to make a distinction between those actors involved in the agenda setting process leading to the transfer and those who took part in transferring the policy to implementation in national member states. Dolowitz and Marsh do not really make this distinction, even though contemporary governance perspectives stress the blurred boundaries between agenda setting and implementation [41]. At the very least, one should not take for granted that the categories and the actors are the same. Nevertheless, from the outset it is evident that despite national differences the Commission, national regulators and the community of national legal experts on privacy have been involved in the transfer. For example, The Article 29 Working Party Clause, creates a body, made up of national Data Protection Authorities, which is responsible for overseeing national implementation (transfer) of the Directive. 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 different countries [3]. 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: policy goals, policy content, policy instruments, policy programs, institutions, ideologies, ideas and attitudes and negative lessons [19]. However, as Dolowitz and March stress, it is important to distinguish between 'policies' and 'programmes' in which the latter is a complete course of action [51]. In this respect 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 initiating and delivering legislation does not also provide a budget for its administration, this is done at the national level. Moreover, one should bear in mind that the Directive *per se* is a patchwork of various national discourses on privacy as well as national administrative practices, which indirectly have been transferred from one nation to another. 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.

4.4 Transfer extent: degrees of transfer?

Dolowitz and Marsh distinguish between four different degrees of transfer: 'copying', the direct transfer, 'emulation', in which the ideas of a policy are transferred, 'combinations', which involve the blending of different policies, and '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 [19, 51]. As already mentioned in 'why transfer?' the degree of transfer in terms of the Directive is likely to become a combination of what Dolowitz and Marsh refer to as: '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, under coercive and voluntarily forces, have adopted elements of the Directive [7], especially those countries seeking membership of the EU. In terms of our approach, we are studying the balance between copying and emulation in the three 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 factors which influence the actual impact of the transfer. Dolowitz and Marsh distinguish between three different factors

which have a significant effect on policy failure [19]. First, the borrowing country may have insufficient information about the policy/institution and its contextual circumstances, what they refer to as 'uninformed transfer'. Second, 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 or 'borrowing' country, something that Dolowitz and Marsh call 'inappropriate transfer'. 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. This may be the case for voluntarily policy transfer, but cannot be taken for granted in cases of coercive transfer. Given what we have already said about the Directive there is reason to believe that at least some member states assumed the Directive would not be a policy success. Rather, it could be argued that some states felt reluctantly obliged to comply with the Directive, albeit only to a certain minimum level.

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 are not featured in their framework. This is a shortcoming, as it is at the policy implementation stage that important decisions are made regarding policy innovation, that is, the actual institutional division of labour between domestic actors, the design of the national legislation, and the resources allocated to monitor and safeguard the principles of the Directive. It is 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 also important to 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. Nevertheless it offers a useful starting point and by 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 range 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 article.

+++ INSERT TABLE 3 HERE [in LANDSCAPE] ++++

5. Policy Transfer or Evolution? Implementing the Directive in Three EU Countries: Denmark, Sweden, and the UK

The deadline for implementing national data protection legislation complying 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, Germany and the UK, had still not fulfilled their obligations under the Directive. In relation to the three 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 [23]. The rate of transfer suggests that either existing legislation was entirely compliant with the Directive, or possibly that member states did not readily acknowledge, or were resisting, 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)³ was established to oversee implementation and transfer. The Article 29 Working Party is made up of the data protection authorities of member states and is serviced by the European Commission. It is also charged with producing annual reports about the development of data protection in member states. The most recent was published in 2007 and provides interesting reading [24]. In the opening statement Peter Schaar, the Chairman of the Article 29 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"* [24: 8]. Implicit in this statement is a recognition that data protection laws remain different across EU member states, despite adoption of the Directive some ten years earlier,

³ EU Data Protection Working Party (Article 29) website, URL: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm

and also that certain member states were introducing measures to combat terrorism and ensure national security which 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. With this in mind it is important to note that the Directive is currently being reviewed and is the subject of a wide-ranging consultation exercise⁴ [18].

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 [25]. Much of this consultation was with national governments, data protection authorities, and data controllers and subjects. According to Bygrave [14], two underlying themes that emerged from this consultation were the lack of harmonisation of member states' respective data protection regimes and the ambiguity of many of the terms and rules in the Directive. He argues, that one problem with existing data protection law, including the Directive and national legislation, is that many of the terms and legal concepts are ambiguous, their intentions not always clear, and sometimes there are different meanings and interpretations in different national jurisdictions [14].

5.1 Denmark

Prior to the adoption of the Directive in 1995 Denmark opposed the imposition of data protection legislation by the EU. This is expressed in the first governmental report on the 'information society' in 1994 [38, 12] 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 Directive within the specified time frame

⁴ European Commission, Justice and Home Affairs, consultation on the legal framework for the fundamental right to protection of personal data. Consultation period: 09.07.2009 to 31.12.2009. Available at, URL: http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm

[9]. According to Blume [10], the committee was working under the understanding that the Directive set tight premises for the implementation process which could not be deviated from. The final act, the 'Act on Processing of Personal Data' [45], which entered into force on 1 July 2000 contained several deviations from the EU Directive, and according to Blume, verges on violating the Directive [10].

There are notable differences between prior legislation in Denmark and the new legislation deriving from adoption of the principles of the Directive. One difference is that prior to the new Act Denmark had different regulation for the public and private sectors: the 'Public Authorities Registers Act' [36] and the 'Private Registers Act' [35]. 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 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 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 [11].

The Register Law Committee played a vital role in the national implementation process in Denmark. The committee was composed of a number of stakeholders, including representatives from relevant ministries, local and regional authorities, legal societies and industry. Other interests, such as, the Danish association of journalists were consulted. During the legislative process the first Act proposed was criticised by the Standing Judicial Committee in Parliament which issued 139 formal questions, many of which related to unclear or ambiguous wording. In practice, limitations in the new legislation were addressed by a series of amendments and revisions initiated by the newly created 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 employed communicative instruments to ensure a better appreciation of data protection principles across Danish society and industry. The main implementation problems in Denmark were 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.

5.2 Sweden

Sweden's Data Protection Act of 1973 was the first comprehensive data protection legislation at a national level in Europe [56]. 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 [44, 58]. In relation to the Directive, the Commission did not interpret the Directive as a 'minimum standard' and instead proposed the introduction of more stringent privacy regulations [44, 54]. The new Swedish legislation, the Swedish Data Protection Act (1998) [57], deviated from the existing Data Protection Act in a number of ways [32]. For example, the new Swedish law incorporated exemptions in 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.

Beyond the implementation of new legislation it is also apparent that a range of actors were involved in the 'domestication' 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 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 the implementation of the Directive the Ministry of Justice collected 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 [21]. 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 new legislation, the implementation of the Directive in Sweden resulted in the establishment of new regulatory measures and instruments. The Swedish 'supervisory authority', the Data Inspection Board, which existed prior to the transfer of the Directive, has legal instruments at its disposal, it may prohibit any data controller from processing personal information and can apply to the County Administrative Court for the erasure of data that has been processed in an unlawful manner. Apart from these pure legal instruments, the supervisory authority has mainly communicative instruments to employ in order to secure the compliance of the Directive, such as, establishing information channels and the cooperation of other actors through networks [17].

During the Parliamentary committee process several points of criticism were brought forward. One issue that emerged during the transfer process was whether the constitutional principle of public access to official documents in Sweden was going to be overridden by the implementation of the Directive [55]. A strict interpretation of the Directive could have meant the end of a 200 year-old legal principle allowing the public access to all official information, including personal information. At the time, this principle was unique to Sweden and Finland and the general view was that there was little chance of concessions or even understanding from the EU. However, in the process of ratifying national legislation this principle was upheld despite contradicting the Directive. This was achieved by omitting all references to the principle of public access in the drafting the Act. The issue that this course of behaviour contravened the Directive was dealt

with by another committee which in their final report suggested maintaining the public access principle, a view later ratified by Parliament [53]. A further criticism was 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 [21] and included several critical voices, particularly from public agencies. According to this study the main problem appears to be the unclear definitions of personal data, as well as, the situations in which 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 principle of '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 1960s. The Younger Report on Privacy [30] and the Lindop Report on Data Protection [29] 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 [61], passed the Data Protection Act [60]. The Act was the first British legislation concerning data protection and only applied to data stored on a computer. It was primarily concerned with the free flow of information and not the protection of privacy. The 1984 Act 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.

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. 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 [47, 48]. 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. A new Data Protection Act (1998) implementing the Directive [59] 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.

The UK Data Protection Act of 1998 was more explicit in setting out individuals' rights 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 Act gives individuals certain rights regarding personal information held about them and places certain obligations on those who process personal information. It covers eight 'Data Protection Principles', which are essentially the core principles promoted by the Directive. 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. The role of the Information Commissioner is perceived to be further strengthened by the Human Rights Act 1998 [31].

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 [6]. Currently the European Commission is investigating whether eleven of the Directive's thirty four Articles, 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 [22]. 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 is occasionally referred to as toothless⁵ 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 came into effect on 1 March 2000 there had been (just) twenty six successful prosecutions for non compliance under the Data Protection Act [2]. Moreover, the penalties imposed for these prosecutions included: a conditional discharge, 150 hours of community service and twenty four fines totalling £22,250 - hardly a deterrent to further infringement [2]. This situation is currently changing. Following numerous high profile losses of personal data the ICO has gained more effective powers to investigate and prosecute organisations for data breaches [34], this may lead to a more effective data protection regime. In the UK it is clear that the transfer of privacy regulation via the Directive is an ongoing process with both coercive and voluntary forces at play.

⁵ See for example Sixsmith, M. (2009) The information watchdog without any teeth. The Times, 14 July. Available at, URL: http://www.timesonline.co.uk/tol/comment/columnists/guest_contributors/article6702869.ece

6. Concluding Discussion

This article 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 cases of Denmark, Sweden and the UK. Consequently, extended discussion could cover a range of topics, including: the nature of privacy regulation in Europe, policy innovation and 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 three 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, this is because they are entrenched and shaped by existing legal and political processes in each national setting. Importantly, this article demonstrates that policy innovation does not take place in a vacuum and is shaped and determined by a range of institutional processes and actors. In this respect, harmonisation is not about uniformity in policy and practice, but the provision of 'agreed' 'principles' (set out in Table 2), shaped by discreet national settings and circumstances, and coercive and voluntary forces. So, convergence, divergence, harmonisation, coercion (etc.) all take place at the same time.

Table 4 presents a comparative overview of the emergent privacy regimes at the EU level and in the three case study countries considered here. From this table it is evident that there is a degree of convergence, via the enactment of national legislation which appears to be compatible with the Directive, but that this takes place in a context of differentiated national policy communities and approaches to privacy. The extent to which this convergence is compliant with the Directive is open to debate, as demonstrated by the UK case presented here. Implicit in the table is the national trajectory of data protection implementation guided by the Directive.

+++ INSERT TABLE 4 HERE [in LANDSCAPE] ++++

Additionally, the case studies show that different aspects of the Directive are problematic in different countries and that the new supervisory authorities are given different levels of legal authority and competence in each country. For example, Sweden has developed ‘higher’ standards of privacy protection than the UK [6]. In this respect, the case of the EU Directive is not a ‘true’ case of direct policy transfer, but of policy evolution and innovation, 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, it appears that convergence is occurring around the core data protection principles and that divergence exists in implementation. 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 subscribe to here. Instead we would argue that the EU and its policy instruments, such as the Directive, are also part of the institutional framework of each member state, and consequently a force, along with many others, influencing behaviour and change – they should not be seen as simple external forces impacting upon national policy as they themselves are often the product of national

policy. Policy and practice 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 adjustment as the various actors 'muddle through' the process. The EU Directive considered here is therefore both coercive and voluntary at the same time.

The policy transfer process is therefore a continually evolving process, 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, and because of the number of countries involved in adopting the Directive, multiple transfers are occurring simultaneously. Moreover, because different countries have different histories of legislation and practice in the data protection area, they offer different levels of personal privacy. Some offer minimum standards, such as the UK, whilst others, such as Sweden, offer much higher levels (the question of what is the most appropriate 'level' is explored by Bennett and Raab [6]). 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, 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, in that the Directive itself is a manifestation of national policy activity and interests. So, policy transfer is arguably better described as policy

evolution. Also, it is 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 light of these arguments, our intention is not to dismiss the model, but to suggest theoretical refinement which explicitly accommodates aspects of policy innovation and implementation, whilst at the same time retaining the overall simplicity of the approach.

In summary, this paper makes a number of 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 (and any subsequent Directives), though the policy processes leading to this convergence are likely to be messy and complicated and the result of a negotiated order. A final point which emerges from this article is the need for further detailed comparative research, including empirical studies, exploring the emerging policy environment surrounding privacy and data protection governance in Europe and beyond. In particular, further work exploring implementation processes would be very valuable and would give greater insights into the nature of relationships surrounding the transfer of the Directive into national settings.

7. References

- [1] Archer, C. (2000) 'Euro-Scepticism in the Nordic Region', Journal of European Integration, 22, 1: 87-114.

- [2] Baird, V. (2007) 'Data Protection Prosecutions', House of Commons Written Answer, 25 June. Available at, URL: <http://www.parliament.the-stationery-office.co.uk/pa/cm200607/cmhansrd/cm070625/text/70625w0075.htm> Accessed on 23 August 2008.
- [3] Bennett, C. (1992) Regulating Privacy: Data Protection and Public Policy in Europe and the United States. Ithaca: Cornell University Press.
- [4] Bennett, C. (1991) 'Computers, Personal Data, and Theories of Technology: Comparative Approaches to Privacy Protection in the 1990s', Science, Technology & Human Values, 16, 1: 51-69.
- [5] Bennett, C. (1988) 'Different Processes, One Result: The Convergence of Data Protection Policy in Europe and the United States', Governance: An International Journal of Policy and Administration, 1, 4: 415-441.
- [6] Bennett, C. and Raab, C. (2006) The Governance of Privacy: Policy Instruments in Global Perspective. Cambridge: MIT Press.
- [7] Bennett, C. and Raab, C. (1997) 'The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response', The Information Society, 13, 3: 245-264.
- [8] Berry, F.C. (1994) 'Sizing up State Policy Innovation Research', Policy Studies Journal, 22, 3: 442-456.
- [9] Betænkning 1345/1997. Behandling af Personoplysninger. Betænkning afgivet af udvalget om registerlovgivningen.
- [10] Blume, P. (2003) Behandling af Persondata – en kritisk kommentar, DJØF: Publishing: Copenhagen.
- [11] Blume, P. (2002) Protection of Informational Privacy, DJØF Publishing: Copenhagen.
- [12] Blume, P. (1996) 'Information Infrastructure and Data Protection. The Danish Perspective', International Journal of Law and Information Technology, 4, 2:1-18.
- [13] Bulmer, S. and Padgett, S. (2004) 'Policy Transfer in the European Union: An Institutional Perspective', British Journal of Political Science, 35, 2: 103-126.
- [14] Bygrave, L. (2002) 'The 1995 EC Directive on Data Protection Under Official Review – Feedback so Far', Privacy Law and Policy Reporter, 9: 126-129.
- [15] Bygrave, L. (1998) 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties', International Journal of Law and Information Technology, 6: 247-284.
- [16] Council of Europe (1981) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. European Treaty Series, No.108.
- [17] (Swedish) Data Inspection Board (2008) Annual Report, Stockholm.

- [18] Data Protection Working Party (Article 29). (2009) Press Release. Brussels, 13 October 2009. Available at, URL: http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_13_10_09_en.pdf
- [19] Dolowitz, D. and Marsh, D. (2000) 'Learning from Abroad: The Role of Policy Transfer in Contemporary Policy-Making', Governance, 13, 1: 5-23.
- [20] Dolowitz, D. and Marsh, D. (1996) 'Who Learns What from Whom: a Review of the Policy Transfer Literature', Political Studies, 44, 2: 343-357.
- [21] Ds 2001: 27 Problem Med EG Direktivet om Personuppgifter, Internal memorandum from the Swedish Ministry of Justice.
- [22] Dyer, C. (2007) 'Europe's Concern Over UK Data Protection 'Defects' Revealed', The Guardian, 1 October.
- [23] European Commission. (2008) Status of implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data. European Commission. Available at, URL: http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm#ukingdom
Accessed on 26 August 2008.
- [24] European Commission. (2007) Tenth Annual Report of the Article 29 Working Party on Data Protection. No.1830-6446, adopted June 2007. EU: Brussels.
- [25] European Commission. (1997) First Annual Report of the Article 29 Working Party on Data Protection. No.XV/5025/97, adopted June 1997. EU: Brussels.
- [26] European Union (EU). (1995) Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal data and the Free Movement of Such Data. Brussels, OJ No. L281 (the EU Data Protection Directive), 24 October 1995.
- [27] Flaherty, D. (1989) Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States. University of North Carolina Press.
- [28] Hartley, J. (2005) 'Innovation in Governance and Public Services: Past and Present', Public Money and Management, 25, 1: 27-34.
- [29] HMSO (1978) Report of the Committee on Data Protection. Cmnd 7341 (The Lindop Report).
- [30] HMSO (1972) Report of the Committee on Privacy. Cmnd 5012 (The Younger Report).
- [31] (UK) House of Lords. (2008) House of Lords, House of Commons, Joint Committee on Human Rights. Data Protections and Human Rights. 14th Report of the Session 2007-08. HL72, HC132.

- [32] Ilshammar, L. (2002) Offentlighetens nya Rum – Teknik och Politik I Sverige 1969-1999, PhD thesis, Örebro Studies in History 2: Örebro.
- [33] Lloyd, I. (1996) 'An Outline of the European Data Protection', Journal of Information, Law and Technology, 1.
- [34] Information Commissioners Office (ICO). (2008) ICO Welcomes New Powers. Press Release, 9 May, ICO.
- [35] Lov nr. 293 af 8. juni 1978 om private register m.v. (Danish Private Registers Act) Lovtidende.
- [36] Lov nr. 294 af 8. juni 1978 om offentlige myndigheders registre. (Danish Public Authorities Registers Act) Lovtidende.
- [37] Margulis, S. (2003) 'Contemporary Perspective on Privacy: Social, Psychological and Political', Journal of Social Issues, 59, 2.
- [38] (Danish) Ministry of Research (1994) Info-society 2000. Schultz forlag: Copenhagen
- [39] Nakamura, R. (1987) The Textbook Policy Process and Implementation Research. Policy Studies Review, 7: 142-154.
- [40] Newman, J. and Clarke, J. (2008) Boundary Troubles: Governance Theory, Politics, Policy and Practice. Stirling Keyword Session on Governance. May 28th, University of Stirling, Stirling, Scotland, UK.
- [41] Newman, J. (2001) Modernizing Governance: New Labour, Policy and Society. London: Sage.
- [42] Nissenbaum, H. (2004) 'Privacy as Contextual Integrity', Washington Law Review, 79: 119-158.
- [43] Organization for Economic Co-Operation and Development (OECD) (1999), Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available at, URL: http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (last modified Jan. 5, 1999), accessed on 25 August 2008.
- [44] Olsson, A. (1996) IT Och Det Fria Ordet – Myten om Storebror. Juridik och samhälle: Stockholm.
- [45] The (Danish) Act on Processing of Personal Data (2000) Act No. 429 of 31 May.
- [46] Przeworski, A. and Teune, H. (1970) The Logic of Social Inquiry. New York: John Wiley.
- [47] Raab, C. (1996) 'Implementing Data Protection in Britain', International Review of Administrative Sciences, 62: 493-511.
- [48] Raab, C. (1993) 'Data Protection in Britain: Governance and Learning', Governance, 6, 1: 43-66.

- [49] Raab, C. and Bennett, C. (1994) 'Protecting Privacy Across Boundaries: European Policies and Prospects', Public Administration, 72, 1: 95-112.
- [50] Radaelli, C. (2000) 'Policy Transfer in the European Union: Institutional Isomorphism as a Source of Legitimacy', Governance, 13, 1: 25-43.
- [51] Rose, R. (1993) Lesson-Drawing in Public Policy: A Guide to Learning Across Time and Space, Chatham House: Chatham, NJ.
- [52] Simitis, S. (1995) 'From the Market to the Polls: The EU Directive on the Protection of Personal Data', Iowa Law Review, 80, 3: 445-469.
- [53] SOU 2001: 3 Offentlighetsprincipen och den nya Tekniken. Betänkande av Offentlighets- och Sekretesskommittén. Fritzes förlag: Stockholm.
- [54] SOU 1997:39 Integritet – Offentlighet – Informationsteknik. Betänkande av Datalagskommittén. Fritzes förlag: Stockholm.
- [55] Steele, J. (2002) Data Protection: An Opening Door. The Relationship between Accessibility and Privacy in Sweden in an EU Perspective, Liverpool Law Review, 24, 1:19-39.
- [56] The Swedish Computer Act (1973), SFS 1973:289.
- [57] The Swedish Data Protection Act (1998), SFS 1998:204.
- [58] Terms of Reference 1995/91 for the Inquiry committee on a new Personal Data Act (Sweden).
- [59] UK Data Protection Act 1998. Available at URL: http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1 Accessed on 20 August 2008.
- [60] UK Data Protection Act 1984.
- [61] Warren, A. and Dearnley, J. (2005) 'Data Protection Legislation in the United Kingdom', Information, Communication and Society, 8, 2: 238-263.
- [62] Yanow, D. (2000) Conducting Interpretive Policy Analysis, Sage University Papers Series on Qualitative Research Method Series, Vol.47. Thousand Oaks, CA: Sage.

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

Feature	Description
Policy Instruments	The tools of privacy regulation: trans-national and international legislation, national legislation, self-regulation, codes of practice, standards and guidelines.
Policy Community	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.
Privacy Discourse	Prevailing attitudes and debate in society and within policy community.

(Source: adapted from Bennett and Raab [6])

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

Tenant	Description
Notice	An individual has the right to know that the collection of personal data has taken place. The personal data must be 'collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes'.
Choice	An individual has the right to choose not to have the personal data collected.
Use	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's details.
Security	An individual has the right to know the extent to which the personal data will be protected. Organisations must 'implement appropriate technical and organisational 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'.
Correction	An individual has the right to challenge the accuracy of the data and to provide corrected information. Personal data collected and maintained by organisations must be up to date and reasonable steps must be taken to ensure that inaccurate or incomplete data is corrected.
Enforcement	An individual has the right to seek legal relief through appropriate channels to protect privacy rights.
Adequacy	The transfer of personal data to third countries is prohibited unless they provide adequate levels of data protection (Articles 25/26)

Table 3. Empirical Questions Emerging From the Policy Transfer Model

Core Policy Transfer Questions	Policy Transfer Features	Emergent Empirical Questions
Why undertake policy transfer?	Continuum between voluntary and coercive forces, or between lesson-drawing and imposition.	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?
Who is involved in the policy transfer process?	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.	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?
What is transferred (and what is not transferred) in the policy transfer process?	Content of transfer: policy goals, policy content, policy instruments, policy programs, institutions, ideologies, ideas and attitudes and negative lessons.	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?
What are the different degrees of policy transfer?	Type of transfer: copying, emulation, combinations, and inspiration.	Is policy transfer similar across all EU member states? Is implementation of the Directive primarily copying or emulation? Does new national legislation complement the Directive?
What are the restraints (or facilitators) of the policy transfer process?	Extent of transfer: uninformed transfer, incomplete transfer and inappropriate transfer'.	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? Is the Directive likely to be revised in the future (bearing in mind the current consultation)?

(Source: adapted from Dolowitz and Marsh [18])

Table 4. European Privacy Regimes in Comparison: Denmark, Sweden and the UK

	Policy Instruments	Policy Community	Privacy Discourse
EU	1995 EU Directive on Data Protection (Directive 95/46/EC); creation of independent national 'supervisory authorities' (typically Information Commissioners and/or data Protection Agencies) in EU member states.	National Governments, European Commission/Union, supervisory authorities, Data Protection Working Party (Article 29) to oversee and review implementation of the Directive.	Establishment of data protection 'principles' to govern processes of data handling <u>and</u> the creation of an EU-wide data market. Perceived need to balance individual data protection with market forces. Significance of convergence of data protection regulations across EU member states to eradicate diverging levels of privacy protection.
Denmark	Public/Private Registers Acts (1978) replaced by Processing of Personal Data Act (2000); Danish Data Protection Agency.	Register Law Committee; Danish Data Protection Agency; policy community consists primarily of key interest groups.	Initial opposition to Directive based on assumption that adoption prescriptive; disputes about terminology and definitions of data protection principles; a desire to retain existing legislation; extensive Parliamentary debate but limited public debate.
Sweden	Data Protection Act (1973) replaced by Personal Data Act (1998); Data Inspection Board.	Ministry of Justice, Data Inspection Board, policy community open to media and public involvement.	Directive perceived to be a minimum standard; a strong desire to retain long standing principle of public access to official documents; considerable Parliamentary and public debate; public concern about curbs on internet use and freedom of speech.
UK	Data Protection Act (1984) replaced by Data Protection Act (1998); Information Commissioners Office.	Government; Parliament; the Information Commissioners Office; other key interest groups.	No real desire within government to adopt Directive; key concern is to create a commercial data market as opposed to protecting individuals privacy; current legislation complies with theoretical minimum standards but is perceived to be in conflict with Directive; limited public debate and awareness of privacy issues.