

BALANCING THE PRIVACY NEEDS OF THE  
INDIVIDUAL AND THE NEEDS OF THE  
STATE:

THE CASE OF IDENTITY CARDS (ID) IN  
THE U.K.

---

## **Abstract**

The relationship between the state and the individual is dynamic and ever-changing. The balance between these relationships is also changing continuously. The current literature seems to emphasise more on the privacy needs of the individual, and place less emphasis to the information needs of the state to function effectively. To highlight these issues, the case of ID cards in U.K. is presented, which seems to present evidence of this predisposition towards the privacy needs of the individual. The issues raised in the ID cards debate are analysed in the context of academic literature on privacy. This paper suggests an alternative approach to privacy in the presence of large scale systems, which takes into account the information needs of state while also taking into account information assembly of the data. This paper provides insights of using an approach where individuals are given freedom to choose and adopt new technologies and services which they believe to be beneficial. In such an approach, those technologies which are seen as over-intrusive would have a low rate of adoption, and would be abandoned as very few individuals use them.

**Keywords:** Privacy, Identity Cards, Legal Issues, Confidentiality.

## 1 Introduction

This paper examines the debate on the changing relationship between the individual and the state. The recent example of the debate on ID cards in U.K. is used to explore whether or not this relationship is changing. A detailed account of the debate on proposed ID cards is presented in section two. The key issues raised in the ID cards debate in U.K. are then analysed within the wider academic literature on privacy. Section four analyses the debate on ID cards in relation to the academic literature on privacy, and proposes that a new balance between the information needs of the state and the privacy needs of the individual is needed. This paper suggests that such a balance can be achieved if the individual is given choice and information about any new technologies and services. Those services which are seen as more benefits than the risks they pose to their privacy would be successful, while others will be abandoned.

This paper examines the ways in which the relationship between the state and the individual is changing with the introduction of Large Scale IT Systems. This debate is examined by using the example of ID cards in U.K., to highlight issues of cost, technological knowhow, and security issues as the key drivers of this debate. However, the central issues of the needs of the state to collect information and the problems associated with information assembly were sidelined. Based on these observations, this paper suggests a model of using '*information assembly*' and looking at the needs of the state as the two key components for future analysis of similar problems. This paper also proposes possible developments to Solove's taxonomy (Solove, 2008), as a more balanced approach to examining technologies which have impact on the privacy of the individual.

## 2 Brief Account of ID Cards in UK

Britain abandoned the wartime identity paper system 50 years and since then there has been no national identity card system. By way of contrast, however at least nine of the European Union countries have some form of identity cards. The re-introduction of Identity Cards has been on the national agenda by a number of political parties (Edgar and Hosein, 2008 668-677) for a number of year. However, the first significant policy drive towards the re-introducing of identity cards came in 2002, when the Labour Government through the Home Office started a consultation which examined the issues of 'entitlement cards' for all U.K. citizens (Edgar and Hosein, 2008 668-677, Home Office, 2002). The national identity card has been an unfilled project of both the Labour and Conservative governments in the UK for more than 20 years (Jackson and Lingertwood, 2006 379-387). In the UK, ID cards have been advocated by the UK government in a report (Home-Office, 2002), as a way of combating illegal immigration, fight against ID fraud and more efficient public services. ID cards have now started to be implemented in UK since November 2008. The rationale and justifications given by the government have been challenged by a number of academic reports (Whitley et al., 2005), generating intense media (BBC, 2009a , BBC, 2009b , Guardian, 2009c) and academic interest (Horton and Wood-Harper, 2006 214-224, Lyon, 1988 , Whitley et al., 2007) in the implementation of ID cards.

Following the initial consultations, the Government introduced the Identity Cards Bill in November 2004. This legislation was debated in the House of Commons from December 2004, and was passed with a large majority in February 2005. The Bill was then presented to the House of Lords in March 2005, where it was suspended till after the general elections in May 2005. There was opposition to the bill from within the Labour Party, the Tories and the Nationals (Jackson and Lingertwood, 2006 379-387). The all-party House of Lords Constitution Committee also expressed concerns about a number of issues, such as the lack of separation and limitation of power. After the re-election of the Labour Government in 2005, the bill was re-introduced to Parliament in June 2005. It took a further nine months for the Bill to become a law. The Bill was finally passed by the House of Lords, and became The Identity Cards Act 2006 on 30 March 2006.

The progression of the Identity Cards Bill was followed by a number of key interventions during its passage through Parliament. There were increasing concerns within business, academic and civil liberties groups about the distinct lack of a public debate regarding the Identity Cards. A key intervention was taken in January 2005, when a group of academics and practitioners initiated a project to examine the details to the potential impacts and benefits of Identity Cards Bill, which became known as 'The Identity Project' (LSE, 2005, Whitley and Hosein, 2008 668-677). The LSE team released its interim report in March 2005, which coincided with the Bill's first presentation to the House of Lords. The report examined the key aspects of Identity Card Scheme, and one of the key concerns highlighted was regarding the privacy of the individual. This report highlighted the concern of the public about a lack of trust and uncertainty about the collection and management of information both in the private and the public sectors. This initial report also pointed out that there was a dichotomy in the relationship between an individual's stated attitudes towards privacy and the actual behaviour of actors. It found that while individuals claim to be concerned about protecting their privacy individuals consistently sacrifice privacy for small benefits. Also, those who say they do not require privacy, routinely attempt to protect their personal information without realising their actions (LSE Interim Report, 2005).

The LSE report (LSE, 2005), was critical of the Identity Cards scheme on a number of grounds. The report concluded that the proposal for a national identity system was '*too complex, technically unsafe, overly prescriptive and lack a foundation of public trust and confidence*' (LSE, 2005: 5). The report also concluded that the proposals would be very expensive, and that it would alter the nature of society. The LSE report also estimated that the cost of a 10 year rollout of the identity card scheme would be between £10.6 billion and £19.2 billion, which were significantly higher than the £5.8 billion estimated of the Government (LSE, 2005). One of the key concerns of the LSE report was the perceived benefits of an identity card scheme (such as prevention of identity fraud), would not materialise, as there are much better means of giving control to citizens of their sensitive information. The LSE report also included an alternative blue print for a National Identity Scheme, with slightly lower cost estimates.

The LSE report proved to be controversial (Whitley and Hosein, 2008 668-677), and was disputed by the Labour Government even before it was formally released. The major controversy surrounding the report was around the cost estimates. Charles Clarke, the then

Home Secretary went on leading radio news programme and dismissed the LSE report's cost findings as wholly inaccurate and as 'simply mad' (BBC News, 2005). The other issue hotly debated by the LSE academics and the Labour Government was regarding the Government's claims about the technological design and specifications. Whitley and Hosein (2008 668-677) noted that there was a tendency for the Government to use 'contentions technological statements as statements of fact to further their own political cause' (Whitley and Hosein, 2008 668-677: 670). This debate, however failed to address many of the issues of privacy which were highlighted in the LSE report, as the focus of the debate remained focused on costs and technological aspects of the proposal.

Another key intervention in the debate on Identity Cards was by the Information Commissioner's Office (ICO, 2005), which was of the view that the information collected by the Government may not be fair and proportionate to the public interest. The information commissioner also called on the Government to be clear about the purpose behind the proposed ID card system. The Information Commissioner also pointed out that there may be other ways to run identification systems, which would avoid the intrusive central register of personal information (ICO, 2005). The creation of detailed data trails of individual's activities is seen as particularly worrying, especially since this cannot be seen in isolation. Other initiatives such as CCTV surveillance and automatic number plate recognition systems, place another component in the infrastructure of a surveillance society. The ICO (2005) was of the view that it is important that each component limits to the minimum the recording of information about individuals to avoid unwanted intrusions into individual lives. The Royal Academy of Engineering also published a report in March 2007 dealing with the dilemmas of privacy and surveillance (Royal Academy of Engineering, 2007), which explored the possible forms that ID cards could take. It explored the ways in which an ID card could be seen as a token, which could take any form such as a phone, watch or a piece of jewellery. The report, rather oddly, suggests that ID tokens should be used instead of ID cards and the major advantage would be 'a person's PC would be more secure' (2007: 41).

A number of other debates, which have similar issues to the I.D cards have also been continuing in Britain. These have included other policy initiatives such as the DNA Databank, Child Protection system (ContactPoint), CCTV. The debate for and against the DNA database has focused on the costs and benefits of the DNA database to society. O'Hara and Shadbolt explain that there are clear privacy concerns with the DNA database in UK (tens of thousands of children who have never been charged with an offence are on the database), on the other hand there is a clear value of the database, which it is claimed helps in matching 166 crimes scenes and criminals (O'Hara and Shadbolt, 2008). Similarly, the mass retention and distribution of data of children through ContactPoint and other children's databases has created the prospect of privacy intrusion of children and their families (Crossman et al., 2007). Although there is little dispute over the appropriateness of information sharing between appropriate bodies (Crossman et al., 2007) however concerns were raised about the sheer volume of data that was retained, and the ways in which the private data of children could be available to a large number of people (Crossman et al., 2007).

The Identity Card Scheme in UK started with a number of trial roll-outs and pilot schemes. Initially, non-EU students and marriage visa holders were required to apply for a ID from

November 2008 (Home Office, 2009a). A planned scheme for pilots and airport workers, which was due to be launched has now been cancelled due to opposition from a number of quarters (Guardian, 2009d). Similarly, it was reported in the press in 2009 that the Conservative Party has warned the leading identity card suppliers that their contracts would be cancelled if the Conservatives won the next general election (Guardian, 2009a), expected in 2010. However, another concern has been that although the Government has now made ID cards optional for everyone in UK, anyone applying for or renewing their passports will be put on the National Identity Register (Guardian, 2009b), which is seen by the media as having the same negative effects as the ID cards.

### **3 A Taxonomy of Privacy for ID Cards:**

Much of the debate on ID cards confuses the issues surrounding privacy of the individual with other issues such as costs (LSE, 2005, LSE Interim Report, 2005) and technological debate (Whitley and Hosein, 2008 668-677). A comprehensive grounding of the ID card debate in the domain of privacy is needed, to enable the debate to be meaningful. There have been a number of attempts to explain the meaning of 'privacy' in a comprehensive and concrete manner. One of the earlier famous attempts was by William Prosser in 1960. According to Prosser (1960) there could be four different types of activities deemed as harmful which are covered by the privacy debate, which include intrusion into a person's seclusion, public disclosure about a person's private facts, publicity about a person which places them in a false light and appropriation of a person's name or likeness by others. Solove (Solove, 2008) is of the view that privacy is too complicated a concept to be boiled down to a single essence, and therefore a more detailed taxonomy for examining privacy.

Although Prosser's (1960) taxonomy is valid in most cases even today, other commentators such as Solove (2008) have argued that in the advent of Information Technology (IT), this taxonomy is no longer complete. Solove has derived a more modern taxonomy of privacy, which takes into account broader issues of cultural analysis, sociological theory and legal sources. According to Solove (2008), there are four basic groups of harmful activities which can be harmful to an individual's privacy. This taxonomy (Solove, 2008) has been used to analyse the debate surrounding ID cards within the parameters of privacy.

#### **3.1 Information Collection**

According to Solove, one of the key concerns for organisations when dealing with issues of ID cards is information collection. Two main forms of data collection have been identified in the literature; *surveillance* and *interrogation*. Surveillance has been viewed as problematic for a long time, with examples from the Jewish law prohibiting building windows that could peer or look into other people's homes, as long ago as the twelfth century (Hofstadter, 1954). More recently, surveillance has been categorised both as visual and audio surveillance. In the US, electronic eavesdropping was prohibited in most of the US states, and was deemed to be illegal (Kerr, 2004). Solove (2008) is of the view that in certain manners, continuous surveillance can be very problematic for the society. A constant feeling of being looked over or gawked at can create feelings of anxiety or discomfort. The discussion on ID cards has an underlying theme on surveillance as an important issue of contention. The Information Commissioner told The Times newspaper in August 2004 that there was a con-

cern that the society may 'sleepwalk' into a surveillance society, and where much more information is collected and distributed than anyone is comfortable with.

Similarly, the LSE report (LSE, 2005) pointed out a number of issues of surveillance that are pertinent to the ID card debate. One of the opinion groups served in the report found that surveillance was one of the key negatives for those who are concerned about technologies such as ID cards. Other concerns highlighted by the report were based on the issue of a lack of audit trails of access to the National Identity Register. These can be perceived by the individual as using identity card as a tool of surveillance by the state. The current system of identifying individuals is by a series of local identities in disparate systems, which are only relied on by a few local providers. The major concern of privacy rights activists has been the perceived ability of the State to increase the surveillance by the having universal identifiers brought about by the national ID card system. The combining of individual identifier information into a single database has the potential for hackers, or rogue system administrators to falsify private information leading to harm.

There have been concerns within academia about the way in which ID cards are perceived by the public. Similarly privacy rights activists see ID cards as a tool by which the government can infringe on the privacy rights of the individual. ID cards are an example of the complex interactions between the state, citizen, outside world, technology and political forces (O'Hara and Shadbolt, 2008). Opponents of ID cards commonly cite Bentham's 'Panopticon' and Orwell's 'Big Brother' as examples of totalitarianism in society (Froomkin, 2009). There are genuine grounds for such stereotypes, with many examples of repressive regimes using ID cards as programmes with which to control and oppress societies (Froomkin, 2009). For example, the Information Commissioner's Office published a report in September 2006 by the Surveillance Studies Network (ICO, 2006). In this report, the phrase 'surveillance society' was officially coined instead of 'big brother' being used in the media in a different way (Whitley, 2008). Shortly afterwards, the Royal Academy of Engineering (RAE) also published a report entitled 'Dilemmas of Privacy and Surveillance: Challenges of Technological Change (RAE, 2007).

Another issue which relates to privacy is interrogation. In US, the Fifth Amendment provides the legal basis for an individual to not implicate himself in self-incrimination. Interrogation has been defined as the pressing of individuals to divulge information. Solove (2008) is of the view that asking too many questions from individuals can be a coercive exercise. People can feel that not answering a question may be taken as a negative implication, and have a number of negative consequences. The privacy law's theory of interrogation is incoherent; however it has far reaching implications on the debate on ID cards. BT, which was to be one of the key suppliers of ID cards technologies, warned the Home Affairs Committee that the storage and interrogation of data would be heavily reliant on the design of the database, which would require a high performance system. Such a system may be seen as too intrusive by the individual, as it would have power to collect and correlate data about individuals. Another issue with the ID cards is the perceived inability of the individual to refuse ID card. Although it has been claimed that ID cards will no longer be compulsory for UK citizens, many do not take this claim seriously. Popular media has reported that although ID cards have now been made non-compulsory, however all the information collected on the

ID cards will now be stored on the National Identity Register whenever a UK national applies for a new or a renewal of their passports. This is seen by privacy rights activists as individuals being pressed for information and the storage of this information on centralised database.

### **3.2 Information processing**

A major concern regarding the implementation of ID cards has been opposition to the aggregation of data and personal information by the State. There are a number of issues relating to how information is processed, and one of the first issues is aggregation. Aggregation is the gathering of information about a person, which when combined, begins to form a portrait of the person (Nock, 1993). Aggregation is not a new phenomenon, but the power of and scope have changed in the information age, where the data is now very extensive and the process of combining it increasingly easier (Solove, 2008). Although aggregation can have a number of benefits such as in credit reporting companies (Nock, 1993), however it can however cause harm by unsettling expectations. Aggregation reveals facts and information about an individual in many ways far beyond what the person imagined. People provide information about their daily activities in small snippets, which they do not expect to be collected and correlated, and a change in this relationship disturbs the trust between the Public and the Government.

The debate on ID card however only focuses on the negative aspects of aggregation. For example, the LSE report (2005) has failed to mention the positive aspects of aggregation. Aggregation has been extensively used to combat benefits fraud, and there is some evidence that security agencies have used evidence gathered through aggregation for anti-terrorist operations. However, the main concern with ID cards is not just aggregation, but a lack of a clear explanation of what data will be gathered and how it will be used. This lack of clarity about the reasons for aggregating data and personal information has led to a lack of trust by the public in the intentions of the governments for bringing in an ID cards system in UK. Others have argued that within the context of a national ID card infrastructure, if your personal data is secure, then your privacy is protected (Whitley et al., 2005) The ID card scheme, even if all the political, cost and other problems are overcomes, has a potential for massive privacy implications going beyond what the original Identity Card Act had envisioned (Crossman et al., 2007). It is likely that the National Identity Register will become a hub for all public sector databases (Crossman et al., 2007).

Another major concern highlighted in the literature is the security aspects of a proposed ID card in UK. The LSE report highlighted that the ID Card Bill was silent on the ways in which data will be kept secure according to the 7<sup>th</sup> data protection principle, which protects against unauthorised access, use and disclosure of personal information. A key privacy related concern for organisations is identity theft of customer and employees. Identity theft is the theft of extensive personal information that is maintained by various companies and institutions. Identity theft is today a key concern for individuals, as victims find it difficult to get jobs, loans and mortgages as long as their identity remains contaminated or in question (Solove, 2004). These identity thefts cause what is known in the literature as insecurity. Security lapses, abuses and illicit use of personal information fall into this category, and is a key concern for organisations handling personal data (Solove, 2008). O'Hara and Shadbolt

(2008) also argue a security dimension affecting the private lives of the individual in the ID card case. They argue that although the current system of loosely-coordinated cluster of identities associated with a person is not very secure, however, the new ID card is 'an all-eggs-in-one-basket' approach, making it a one-stop shop for identity thieves. At times, the debate surrounding ID cards have been surrounded by political spin and perceptions, rather than a debate on the real issues (O'Hara and Shadbolt, 2008).

Another issue with the implementation of a proposed ID cards system in UK is the extent to which data will be used for other purposes. One of the key provisions of the National Identity Register will be that data will be shared between public bodies. The EU Data Protection Directive stipulates that personal data must be collected for a specified purpose and should not be further processed in a way which is incompatible with the original purpose (EU, 1995). Similarly, the OECD privacy guidelines and APEC Privacy framework also contain a number of restrictions on the secondary use of personal information. The secondary use of information causes a number of problems. Firstly, the person does not expect the information to be used in this particular manner. Secondly, the potential for secondary use generates fear and uncertainty in the mind of the individual about the possible use of information. In these ways, secondary use resembles the harm that is created by insecurity. Similarly, secondary use of information can create problems because this information may not fit well with the new use (Solove, 2008). The removal of data from the original context may also make it easy to misunderstand the original data, a danger of decontextualisation. However, the UK Identity Card Scheme provides few of these obligations and may allow for the access of data to a broad range of third parties, with no limits on retention and no rights of access by the individual (Jackson and Ligertwood, 2006 , Whitley, 2008 , Whitley et al., 2005).

The existence of a National Identity Register will create problems of access and control of personal information. Another privacy issue raised by the ID cards is that of the right to access personal information. The failure to provide individuals with notice and input about their records is called an 'exclusion' by Solove (Solove, 2008) in his taxonomy of privacy. This exclusion leads a reduction in the accountability of the organisations which maintain records about an individual. The harm to the individual is created when the individual is kept away from participating in the use of his personal data, and not being informed about how the data is being used.

### **3.3 Information Dissemination**

The Identity Cards Law is unclear about how it will deal with cases of breach of confidentiality. The existence of a single large and centralised database will make it a prime target for fraudsters, viruses and criminal elements. Protection against the breach of confidentiality helps to promote certain relationships which are based on trust (Solove, 2008). In the United States, tort law recognises breach of confidentiality as a distinct harm. The breach of confidentiality tort applies to the patient-physician relationship and to a number of other relationships too. In a number of judgements in the US, other courts have agreed that banks and other organisations must not divulge the personal information of customers to other parties. In England, a breach of confidence tort applies, which is applied more generally.

Disclosure occurs when certain true information about a person is revealed to others. Davies argues that the protection from disclosure is important as it prevents people from engaging in activities that further their self-development (Solove, 2004). Disclosure can also inhibit people from associating with others, which will impinge on the freedom of association and can destroy anonymity. Similarly, data protection principles are based on a premise that only personal information needed for a specific purpose and a defined purpose will be collected by organisations (Jackson and Ligertwood, 2006), in a study of Australian law. Similarly, the European Data Protection law also defines a set of principles which stipulate that the information should only be collected for a specific and declared purpose (Beynon-Davies, 2006). This information will be retained for a limited time and should be destroyed when the purpose has been fulfilled.

### **3.4 Invasion**

Identity cards systems can also be categorised as a nationalised system of intrusion by the State in the daily lives of the citizen. The Information Commissioner's key concerns in this regard were that the combination of data from a variety of sources in a National Identity Register could be considered a gross intrusion into people's private lives (ICO, 2005). There can be ways in which the government can achieve aims similar to the ID cards, but are less intrusive for the individual's privacy. Protection against intrusion exists around the world. The constitutions of many countries protect their citizens against unreasonable search and seizure by the Government (Bradley, 1993). Intrusion is close to disclosure, as it is often made possible by intrusive information gathering activities. According to some academics, intrusion in the modern organisation is not only concerned with the presence of spatial incursions. Other artefacts such as spam, junk email, junk faxes and telemarketing are also forms of intrusion which affects the privacy of the employees and customers. In particular, intrusion often interferes with solitude, a state of being alone or able to retreat from the presence of others.

Protecting a zone of autonomy is the responsibility of the state towards the individual (Solove, 2008). However, the State should not be seen as taking a decision to interfere in the personal and private lives of the individuals. The ID Cards Scheme in UK can be categorised as a case of '*decisional interference*' by the state in the private matters of the citizen. In the US, the Supreme Court explained in *Whalen v. Roe* (1977 599) that a 'zone of privacy' extends not only to the interest in independence in making certain kinds of important decisions, but also included the individual's interest in avoiding disclosure of personal matters. Similarly, within the literature on privacy and data protection, the option of choice for the citizen is critical (Culnan and Armstrong, 1999). The UK Data Protection Act requires that the data subjects are informed that a particular data set is collected, and that they are given the choice whether or not to provide this information Culnan and Armstrong (Culnan and Armstrong, 1999) reported that the privacy policies should incorporate informed consent of the data subjects. However, the interaction between the government and the citizen in relation to the issues of choice are controversial (Joinson, 2009 1-10). In many cases, the state may require information from the individual and may punish those who do not comply with the requirements.

#### 4 Analysis: Beyond the ID Cards:

This paper seeks to extend and adapt the model presented by Solove (Solove, 2008), in light of the analysis conducted from the ID cards debate in U.K. The approach used by Solove (Solove, 2008) for presenting a taxonomy of privacy can also be expanded to include wider issues of the relationship between the individual and the state. One of the main assumptions of Solove is that information collection creates disruption through the process of data gathering. However, evidence from the ID cards debate shows that this may not be the primary concern. Governments and private organisations have gathered data on citizens and consumers for a very long time, controversial. For example, Passports have been implemented in U.K as 'safe conduct' documents since medieval times. The process of information collection has not been controversial, it is the ways in which this information is assembled which creates difficulties. We could call this process '*information assembly*', where data is gathered from a variety of sources build an in-depth picture of a citizen, and infringes on the right to privacy. The debate on ID cards in U.K., if examined from an information assembly perspective would not only examine ID cards, but would also look into other technologies such as Automatic Number Plate Recognition, DNA database and National Identity Register. It can be argued that the right to privacy of an individual is affected if information about him or her is assembled from these databases different by service providers, which would then adequately affect the privacy of the individual, not just by one technology such as the ID cards.

Solove has also argued that surveillance as an issue of concern. However, the evidence from academic literature and practise seems to contradict some of this argument. For example, passports in different forms have been issued in U.K as early as 1414, and in their current form from 1915 onwards (Home Office, 2009b). However, the use of these passports did not face any major resistance, especially within the realm of surveillance. On the other hand, the debate on ID cards in U.K. indicated that surveillance is one of the key problems (ICO, 2005 , ICO, 2006 , LSE, 2005 , LSE Interim Report, 2005). The main opposition to ID cards is not because they provide surveillance tool for the government, but the underlying argument is that ability of increasingly connected large scale databases and systems to drill down and link data across systems would create an intrusion into the private lives of the individual. ID cards in themselves are not this enabling technology, rather it is these other systems such as the DNA database, Police National Database and other upcoming systems which are seen as threat by the privacy rights activists.

It also appears that Solove's (Solove, 2008) use of *information assembly* is an effective approach to examine the debate on the changing relationship of the state and the individual especially within the realm of privacy. We believe one key mean for extending Solove's arguments on privacy is to examine issues of balance of the needs of the state and individual depending on the situation. The various reports by academics and privacy rights organisations have been critical of the U.K government in relation to its attempt to collect information which is critical to the smooth functioning of the government's key tasks. However, governments around the world need to collect and assemble more data on their citizens for a variety of reasons. These included border protection, crime prevention, anti-terrorism initiatives, fraud detection and a host of other applications.

One dimension of future analysis of the changing relationship between the state and the individual, and the impact of this process on privacy would be include a stand on research on the ways in which the state can function more effectively while also collecting the necessary information. The focus of the various reports on ID cards and academic literature on privacy has been of the view that governments should not need much information on citizen. However, governments increasingly need to collect more information for service improvements, combating crimes and terrorism, and providing basic civil facilities to the population. An improved approach would be recognising that governments have legitimate concerns and needs to collect, assemble and analyse data. The debate should then focus on the kinds of 'needs' and the justification for particular types of data which can be collected within the realm of these needs.

Using a framework of '*information assembly*' while also taking into consideration the needs of the state to function effectively, will enable future debates on those technologies which affect the privacy of the individual to be shaped more positively. There would be a number of advantages of using such a framework. Firstly, a clear discussion on how a particular technology can be used to assemble a complete picture of the individuals can be presented. This discussion would also involve the information needs of the government for functioning in an effective manner. If the ID cards debate was to be analysed within this framework, one of the first issues would be to examine the ways in which the government proposed to assemble and gather data about the individual. Another positive aspect of this approach would be that this debate would also examine in detail, the changing perceptions of the individuals towards privacy in a world changing swiftly with the advent of new technologies and technology led services.

Another key aspect absent from the debate on the changing relation between the state and the individual was the ways in which privacy needs of the individual is a concept, which has continued to evolve over time. In many scenarios, the individual is happy for his privacy to be compromised to a certain level if the individual expects to receive a benefit which outweighs the costs. A classic case of such examples is the phenomenal growth of blogs and social networking websites. However, in the case of ID cards in U.K., this benefit was not seen and neither perceived by both, the privacy activists and the individuals. This also increased the resistance to the proposed implementation of ID cards by the U.K. government. One way of balancing the privacy needs of the individual with the information needs of the state is for the state to provide a clear map of the benefits that individuals receive when a new technology such as the ID cards is introduced. Individuals could then be given the choice to choose or reject any new technologies. Such a mechanism of individuals '*self-selecting*' new initiatives should work on similar principles as a market driven mechanism. New technological initiatives, which are seen by individuals as presenting acceptable risks to their privacy, yet providing benefits which outweigh these risks will be adapted. This adaptation will also follow the traditional adaptation patterns of a commercially available product, with technological savvy individuals adapting these services initially, and others joining in as they are convinced that the new technology or service is at acceptable levels of benefits and risks.

## 5 Conclusion

This paper has analysed the debate on ID Cards in U.K, with an aim to investigate the changing nature of the debate on the needs of the state to conduct its affairs and the needs of the individual to protect their privacy. The debate on the case of ID card was considered in light of academic literature on privacy, and it was established that current methods for examining the needs for privacy of the individual against the needs of the state need to be developed further. A model for using '*information assembly*' and the needs of the state was discussed. Using this method could be more constructive, as it would not only examine the needs of privacy of the individual, but also examine the various needs of the state to function successfully, and could lead to more constructive and meaningful discussions. Finally, it was suggested that a self-selecting mechanism for uptake of new technologies and services may be a reasonable approach for negotiating this balance between the state and the individual.

If we were to consider the case of ID cards in U.K. in a hypothetical scenario, where this initiative had been presented by the government as non-mandatory, the results today may have been different. The government in U.K. would in this case have presented a more comprehensive case for the benefits that citizens get from the adoption of ID cards. These could be benefits such as ease of opening bank accounts or faster processing of services such as issuing of passports. However, some may argue that critical services such as ID cards may have to be mandatory, as they are essential to the functioning of the state. The use of this approach, it can be argued may lead to individuals never choosing to adopt core services, thereby making this approach unfeasible. However, we believe that on the contrary, an approach where individuals are given the freedom to pick and choose services they feel comfortable with would provide incentives for the government to improve non-functioning services. If the government is investing huge sums into the implementation of ID cards, and it appears that the public is not choosing to use this service, then the project would either have to be shelved or radical improvements would be needed. This would lead to reaching a reasonable settlement where individuals start to believe that they will receive benefits from adopting new technology such as the ID card, and that these benefits outweigh the costs of intrusion to privacy.

## 6 References

1977. Whalen v. Roe. US Supreme Court.
- BBC. (2009a) *Blunkett seeks 'end to id cards'* [Online]. Available: <http://news.bbc.co.uk/1/hi/technology/8022791.stm> [Accessed 16 May 2009 2009].
- BBC. (2009b) *Id card 'flash and dash' warning* [Online]. Available: [http://news.bbc.co.uk/1/hi/uk\\_politics/7925779.stm](http://news.bbc.co.uk/1/hi/uk_politics/7925779.stm) [Accessed 17 May 2009 2009].
- BBC News. 2005. *£300 price tag on id cards 'mad'* Available: [http://news.bbc.co.uk/1/hi/uk\\_politics/4099356.stm](http://news.bbc.co.uk/1/hi/uk_politics/4099356.stm).
- Beynon-Davies, P. (2006) Personal identity management in the information polity: The case of the uk national identity card. *Information Polity*, 11(
- Bradley, C. (1993) *The failure of criminal procedure revolution*, Philadelphia, University of Pennsylvania Press.
- Crossman, G., Kitchin, H., Kuna, R., Skrein, M. & J., R. 2007. *Overlooked: Surveillance and personal privacy in modern Britain*. London: Liberty.
- Culnan, M. & Armstrong, P. (1999) *Information privacy concerns, procedural fairness and impersonal trust: An empirical investigation*. *Organization Sciences*, 10(1).
- Edgar, W. & Hosein, I. (2008) Doing the politics of technological decision making: Due process and the debate about the identity cards in the U.K. *European Journal of Information Systems*, 17(668-677).
- EU 1995. *Eu data protection directive*. European Union.
- Froomkin, A. 2009. Identity cards and identity romanticism. In: KERR, I. (ed.) *Lessons from the identity trail: Anonymity, privacy and identity in a networked society*. New York: Oxford University Press.
- Guardian. (2009a) *Conservatives warn firms not to sign long-term id card contracts* [Online]. Available: <http://www.guardian.co.uk/politics/2009/jun/17/chris-grayling-id-cards> [Accessed].
- Guardian. (2009b) *Gordon brown's back door to compulsory id cards* [Online]. Available: <http://www.guardian.co.uk/politics/2009/sep/29/id-cards-gordon-brown-speech> [Accessed].
- Guardian. (2009c) *Id cards scheme in terminal decay* [Online]. Available: <http://www.guardian.co.uk/commentisfree/libertycentral/2009/may/06/id-cards> [Accessed].
- Guardian. (2009d) *Identity card trial for air industry staff dropped* [Online]. Guardian. Available: <http://www.guardian.co.uk/politics/2009/jun/30/identity-cards-pilots-airports> [Accessed].
- Hofstadter, S. (1954) *The development of the right of privacy in New York*, New York, Grosby Press.
- Home-Office 2002. *Entitlement cards and identity cards: A consultation paper*. In: OFFICE, H. (ed.).
- Home Office 2002. *Entitlement cards and identity fraud: A consultation paper*.

- Home Office. (2009a) *Identity cards* [Online]. Available: <http://www.homeoffice.gov.uk/passports-and-immigration/id-cards/> [Accessed 15 November 2009].
- Home Office. (2009b) *Passport history timeline* [Online]. Available: [http://www.ips.gov.uk/cps/rde/xchg/ips\\_live/hs.xsl/1080.htm](http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/1080.htm) [Accessed].
- Horton, K. & Wood-Harper, W. (2006) The shaping of i.T. Trajectories: Evidence from the u.K. Public sector. *European Journal of Information Systems*, 15(2), 214-224.
- ICO. 2005. The identity cards bill- the information commissioner's concerns. Available: [http://www.ico.gov.uk/upload/documents/library/corporate/detailed\\_special\\_guides/id\\_cards\\_bill\\_-\\_ico\\_concerns\\_october\\_2005.pdf](http://www.ico.gov.uk/upload/documents/library/corporate/detailed_special_guides/id_cards_bill_-_ico_concerns_october_2005.pdf).
- ICO 2006. A report on the surveillance society. Surveillance Studies Network.
- Jackson, M. & Ligertwood, J. (2006) Identity management: Is an identity card the solution for australia? *Prometheus*, 24(4).
- Jackson, M. & Lingertwood, J. (2006) Identity management: Is an identity card the solution for australia? *Prometheus*, 24(2), 379-387.
- Joinson, A. 2009. Privacy concerns, trust in government and attitudes to identity cards in the united kingdom *2nd Hawaii International Conference on System Sciences*, Hawaii.
- Kerr, O. (2004) The fourth ammendment and new technologies: Constitutional myths and the case for caution. *Michigan Law Review*, 102(
- LSE 2005. The identity project: An assesment of the uk identity cards bill and its implications. London: London School of Economics and Political Science.
- LSE Interim Report. 2005. The identity project: An assesment of the uk identity cards bill & its implication. Available: <http://identityproject.lse.ac.uk/InterimReport.pdf>.
- Lyon, D. (1988) British identity cards: The unpalatable logic of european membership. *Political Quarterly*, 62(3).
- Nock, S. (1993) *The costs of privacy: Surveillance and reputation in america*, New York, Walter De Gruyter.
- O'Hara, K. & Shadbolt, N. (2008) *The spy in the coffee machine: The end of privacy as we know it*, Oxford, Oneworld Publication.
- Prosser, W. (1960) Privacy. *California Law Review*, 48(
- RAE 2007. Dilemmas of privacy and surveillance: Challenges of technological change. In: GILBERT, N. (ed.). The Royal Academy of Engineering.
- Royal Academy of Engineering 2007. Dilemmas of privacy and surveillance: Challenges of technological change. London.
- Solove, D. (2004) *The digital person: Technology and privacy in the digital age*, New York, New York Univeristy Press.
- Solove, D. (2008) *Understanding privacy*, London, Harvard University Press.
- Whitley, E. 2008. Preceptions of government technology, surveillance and privacy: The uk identity cards scheme. In: NEYLAND, D. & BENJAMIN, G. (eds.) *New directions in privacy and surveillance*. Cullompton: Willan.
- Whitley, E., Hosein, G., Angell, I. & Davies, S. (2007) Reflections on the academic policy analysis process and the uk identity cards scheme. *The Information Society*, 23(1).

- Whitley, E., Hosein, G. & Davies, S. 2005. The identity project: An assessment of uk identity card bill and its implications. London: LSE.
- Whitley, E. & Hosein, I. (2008) Doing the politics of technological decision making: Due process and the debate about the identity cards in the u.K. *European Journal of Information Systems*, 17(668-677).