Out of Reach? The troubled history of Ireland’s quest for e-government
Perry Share

On April Fool’s Day 2008 the Irish government announced the death of Reach—at barely eight years of age. On that day it was indicated that all the functions and responsibilities of this little-known Irish ‘egovernment’ agency had been ‘formally taken over by the Department of Finance, and [were] now specifically the responsibility of the Technology Policy Division’. Effectively, the initiative had been terminated. But what was Reach, where did it come from, and why did it disappear from the view of an Irish public that never really knew much about it in the first place? What is egovernment anyway and, more significantly, what broader questions does the rise and fall of the Reach initiative imply for Irish society?

In the last decade the western world, including Ireland, has seen an explosion in the technologies of governmentality and surveillance that would have impressed even Michel Foucault, whose writings have led sociologists to critically consider contemporary forms of power: including that of the ‘panoptic gaze’1. Such technologies include, amongst others, closed circuit television [CCTV], geo-tracking of mobile phones, supermarket loyalty cards, electronic passports, internet cookies, DNA databases, satellite-tracking of offenders, data-mining and data-matching and government ID cards. These technologies are linked to broader discourses of ‘security’—both personal and national— that have emerged over the last number of decades and in particular since the emergence of modern terrorist activities.2

The emergence of egovernment, like many of these technologies (some of which come within its ambit), has been welcomed by some as an enhancement of a secure and well-managed society. It has also drawn critical commentary in terms of concerns for privacy, for surveillance of everyday activities and for socially divisive impacts. Many people are just happy enough if ‘the system’ works to make their inevitably tedious and time-consuming interactions with government agencies that bit more efficient and easy. Others decry the gradual, and largely undebated, emergence of an Orwellian ‘Big Brother’ society. It is argued that our very desire for ‘security’ has the potential to contribute to feelings of greater insecurity. This chapter refers to some of these debates, but first outlines some of the key features of egovernment itself, before describing the ill-fated Reach programme and some of its allied features such as the Public Services Broker [PSB] and the PPSN (social security number).

Egovernment

E-government is a phenomenon that has emerged from the maelstrom of public sector re-engineering and technological development. Drawing on such increasingly ubiquitous technologies as the internet, digital television and mobile telephony it promises access to a panoply of public sector goods and services. The Irish government’s enthusiasm for egovernment dates from the mid-1990s—a period when,
as Fintan O’Toole has recently remarked, the Irish government (like most others in the world, it has to be said) had the habit of ‘putting e- before every noun that had the misfortune to crawl across a screen’\(^3\).

In the words of one enthusiast egovernment is no more than an extension of good government:

> from Bohola to Ballybough patient souls will happily make their way to the counter (sorry, reception facility) provided there is only one to go to, not too much of a queue, a teeny bit of privacy and a smile. That’s good government and the e-bit comes in when Máire or Seán Citizen can look things up, get them moving or even accomplish the task through the screen on the desk\(^4\).

Endorsed by governments across the developed and, increasingly, the developing world, egovernment is seen as a way to make delivery of public services more efficient and effective, in particular to allow all citizens to receive a high-quality personalised and responsive service. While the rhetoric of egovernment has yet to be met by the reality, the development of digital technology, in particular the internet, has undeniably begun to have an impact on public service delivery.

At the international level the greatest advances towards effective egovernment have been in countries such as South Korea and Taiwan, states that have made very significant investments in ICT infrastructure and which have massive electronics industries. Nevertheless, according to the Brookings Institution, Ireland is in a group of countries, including the USA, Singapore, Canada, Australia, Germany, Dominica, Brazil and Malaysia, that are the most highly-ranked in terms of egovernment. The UN is less sanguine about our performance, and has ranked Ireland at 17\(^{th}\), with the Nordic countries, US, France and South Korea topping the list\(^5\).

Egovernment can refer to either the delivery of information or of services. The first is much easier and is already widespread in the form of webpages and associated elements such as RSS feeds. Actual service delivery is a much greater challenge and remains quite limited within or across countries\(^6\). Despite the boundless aspirations of egovernment enthusiasts, there are currently few services that can be completely delivered electronically (unlike, say, iTunes or Ryanair in the private sector). Most aspects of egovernment continue to sit alongside conventionally delivered services.

The features of egovernment can be placed along a continuum, with static information provision at one end, and fully interactive service delivery at the other. At its simplest, egovernment is about the basic provision of information, perhaps a web page outlining

---


available benefits: the electronic equivalent of a brochure. Such information might formerly have been disseminated as a newspaper advertisement, pamphlet, on the telephone or face-to-face at a public office. Further along, we come to services that allow for some interaction with the information provided: perhaps we can download a form to print off and fill in. In the past we may have had to attend at a public office to complete such a form, or have had to have one posted out to us for completion and return. With egovernment we can print the form at home, but still must submit in person or by mail, especially if a handwritten signature is required. The third level of service is 2-way interaction. Here the user might not need to print out a form, but could fill it in online and submit the information through the site. It is here that egovernment services really begin to become useful: all provision of information can be done at the computer. The ultimate level of egovernment is transactional capability. Here the user can carry out a transaction that may involve case handling, decision-making and service delivery – all online. They can put data into an electronic form, transfer funds through an electronic funds transfer system and receive a service as a result: for example print out a license or document they have paid for.

A good egovernment service will allow users to operate at the level at which they are most comfortable. Ideally all services would be available at the top level, but even the most advanced generally fail to achieve this. For example, the Irish government’s motor tax online service allows you to fill in your details online and pay for your tax disc without having to use the mail or to attend at the local tax office. But as yet it is not possible to print out your own disc, presumably for security purposes. Such a development would mean that the whole process could be transacted by computer, as is the case now with airline tickets and boarding passes.

Security and confidentiality of information are big issues for many people. We might be happy enough to enter details about our car, or even our passport number, online to a computer. But we may feel a lot more circumspect about submitting sensitive personal details related to our health or income. Thus services such as applications for state benefits, or for medical services, are much less likely to be fully-delivered electronically at this stage. This may change as people become more familiar with using computer technology, especially e-commerce, and as more people have access to computers. It may also be supported by ways of storing and making easily available our personal information, as was envisaged by Reach, and as will be discussed below.

The delivery of egovernment raises other important issues in relation to data security and accessibility. One 2008 study\(^7\) has found internationally that egovernment websites did not tend to have clear policy statements about privacy and security, were not accessible to all, and did not support e-commerce. In addition many suffered from lack of maintenance and poor information design. The study concluded that at this stage, ‘in general, e-government is not radically transforming the public sector’. In other words, the overall level of service is poor.

The most radical form of egovernment, and one that we perhaps glimpsed in the hi-tech campaigning of Barack Obama, lies in the area of e-participation. This is the process whereby the one-way information flows of egovernment can become two-way. Through e-participation the citizen can become involved in government, through voicing their

\(^7\) West, op cit.
opinions and having them taken seriously. The UN measures e-participation through an assessment of a government’s institutional capacity, leadership role and willingness to engage their citizens in participatory decision-making for public policy. By these measurements Ireland, perhaps not surprisingly, did not perform at all well, with a ranking of 49th. The leading countries were the USA, Denmark, South Korea and France.

Nevertheless, the Irish Government has until recently expressed considerable enthusiasm for egovernment. It has been seen as a key element in making Ireland more competitive in the global information economy. The government sees a highly developed public service capable of delivering e-services to customers and businesses as an essential part of that strategy. It has also squarely set the egovernment strategy in the context of the reorganisation of the public sector (the ‘Delivering Better Government’ initiative). Egovernment is directly linked to the desire to bring about major changes to the organisational structures, cultures and working processes of the Irish public service. The grandly-titled ‘Information Society Action Plan’ set out a framework for egovernment initiatives, a number of which were established and pursued in the early to mid-2000s, the most ambitious of which was Reach.

Reach, the PSB and the PPSN

Reach was established in 1999, as an initiative of the Department of the Taoiseach related to the technologically and managerially-driven Information Society programme. Its task was to develop a strategy for the integration of public services and to develop and implement the framework for egovernment. Given the centrality of egovernment to the future development of government as a whole, Reach was seen as a very important initiative, despite having a negligible public profile. During its short lifetime (2000-2007) it also consumed a not insignificant amount of taxpayers’ money (€37m) though it never gained the notoriety of the doomed HSE computer project PPARS (cost €182m) or electronic voting machines (cost €52m), despite some belated media attempts to lump it in with these other failed e-projects.

The central element of Reach was the development of the ‘Public Services Broker’ (PSB): an ‘integrated set of processes, systems and procedures designed to provide a standard means of access to public services’. In particular the PSB was to help Reach to: connect services through a virtual ‘one-stop-shop’; personalise services towards the individual needs and preferences of the customer; provide choice and convenience over time and place; reduce the need for repeated form-filling and provision of basic personal data; and simplify access to services and information by allowing self-service over the Internet.

The development of the PSB is partly technological and partly administrative. The technological side involves the development of ‘interoperability’ standards so that the many different data systems used by the state can talk to each other. It also involves the development of secure networks that can identify individuals and link them to

---

8 UN, op cit
9 Department of the Taoiseach, New connections: A strategy to realise the potential of the Information Society. 2002
centralised data. All of these process raise complex technical and ethical challenges, as we will see.

Generally everyday access to government services requires us to provide personal data about ourselves, for example name and address, date of birth, PPSN (Personal Public Services Number), car registration, bank account number, and so on. Sometimes, as in applying for a financial benefit, much more detailed and sensitive information is sought. Often the provision of such information has to be backed up with one or more types of documentary ‘proof’, such as a birth certificate, driving license, marriage certificate, passport or utility bill. Having to provide such information, often repeatedly, to different state agencies, can be tedious and time-consuming.

The aim of Reach was to make such information more easily available to agencies. It was argued that this would prevent the citizen (or ‘customer’ in Reach language) from having to prove their identity and supply the same personal details over and over again. Reach thus sought to give public service agencies controlled access to an accurate set of customer data, thereby speeding up the application and reducing the amount of forms that have to be filled in.

In the new egovernment system, the citizen/customer would be able to deposit their personal data with the PSB and later choose to release it when applying for a service. Thus, rather than having to produce a document such as a passport or driving license, the citizen/customer would be able to easily prove their identity using information already deposited with the PSB. When seeking to establish their entitlement to services, instead of having to undergo several means tests by different agencies the customer could release previously stored data relating to income and means. With egovernment, these tasks could be completed from home or workplace without having to attend at any government office or post office.

A crucial aspect of the PSB would be secure personal data vaults. These would be set up for customers as services are developed and on request of the individual. In addition to the normal basic set of personal data required for most services (date of birth, address) customers could store additional data in these vaults to be released at their discretion to aid or assist in gaining access to a service or to enhance service levels. Examples of such data would be birth and marriage certificates, details of income or other means, digital photographs, credit card details, passport details, car registration and insurance details. Data could be updated directly by the customer or by an agent acting on their behalf. Access would be strictly limited to the individual customer or to public servants and agents authorised to access the data in the context of a specific transaction. In effect, for the citizen the government becomes a single unit, rather than a collection of individual departments, agencies and services. As you can imagine, data security would be a major issue here; you wouldn’t want someone finding all this information on a stolen laptop or discarded hard-drive!

A key aspect of the PSB is that information can be shared across different government agencies. In fact such information sharing has been quietly taking place in Ireland over the last decade. For example, the interagency messaging service [IAMS] allows the exchange of data between the General Register Office and the Department of Social and Family Affairs [DSFA]. When a baby is born and registered, data is transferred from the
GRO to the DFSA, meaning less paperwork and delay in setting up a new PPSN and ensuring the payment of relevant benefits\textsuperscript{10}. This service will eventually be extended to allow for the capture and dissemination of other registry data, such as marriages and deaths, to a variety of government agencies. Similarly, DSFA currently provides data to the National Breast Screening and Irish Cervical Screening Programmes to allow them to invite women for screening.

The use of the existing Personal Public Services Number [PPSN] as the common unique identifier is an important element of the delivery of government services through the \textit{Reach} model. The aim was to use the PPSN as the customer’s unique ‘key’ to help the development of personalised services and minimise the risks of error and inaccuracies in personal records. Legislation had already prepared the way for the development of such a unique identity. The Social Welfare (Miscellaneous Provisions) Act 2002 provides for the new ‘Public Service Identity’ - a secure and unique identifier for customers of public services. The Act defines the elements of the Public Service Identity, including name, address, date of birth, gender, nationality and PPS number. It also provides that where specified bodies collect relevant information then it also feeds into the Public Service Identity. Personal data collected at registration of birth will also be collected for the purpose of establishing a person’s Public Service Identity. The DFSA is responsible for maintaining and managing the Public Service Identity database.

\textit{Reach} aimed to develop the Public Services Card (PSC) as the key for access to services. This card would identify and authenticate individuals. Based on the existing PPSN card it would display the cardholder’s name, PPS number and signature. Every citizen would also have a PIN number. More sophisticated versions of the card were being planned, to contain a variety of types of stored information, including an ‘electronic signature’ that could be legally used to claim benefits or other services. In many respects the PSC was effectively a national identity or ID card.

**ID cards, surveillance and the privacy debate**

Governments across the world have long sought to introduce ID cards for their citizens. They have been extensively used in times of war and for colonial administration, and have also accompanied the development of the welfare state with its conceptions of ‘entitlement’ and, more recently, of ‘risk’\textsuperscript{11}. In Continental Europe and Southeast Asia there has been widespread adoption of such cards and they appear to be well accepted. Germany has had them for over 50 years and Belgium has introduced an electronic ID card that is mandatory for all those aged 12+ and that can be used for both public and private (eg banking) transactions\textsuperscript{12}. In English-speaking countries there has been much greater debate over their adoption. For example, in Australia a proposal to introduce a national identity card (the ‘Australia Card’) was rejected after vigorous public debate as long ago as 1987.


\textsuperscript{11} For example, by the Belgian administration in Rwanda, see Lyon, D. ‘Identification practices: state formation, crime control, colonialism and war’ in Aas et al (eds) \textit{op cit}.

Notwithstanding the hesitancy over the adoption of ID cards, other ‘smart’ cards are of course very much a part of our everyday life. As well as long-established credit and debit cards many of us now carry supermarket loyalty cards – Tesco has been an international leader in this area. These allow private firms to gather considerable amounts of data about our purchasing activities, and the scope of such cards is increasing. There are concerns about information privacy, accuracy, sharing of commercial data with state bodies (as is already occurring in the UK) and the potential to exacerbate social exclusion through the ‘social sorting’ and categorisation of specific population groups.

There are also concerns about the potential for surveillance, especially as the technology now exists, for example, to link loyalty card data to that gathered by global positioning systems (GPS) and RFID (radio frequency identification) tags. These are tiny tags, attached or embedded into goods, set to eventually replace barcodes. They emit a radio signal that enables data to be remotely collected. It has been suggested that RFID tags could be linked with smart cards in a number of ways, for example they:

- could become an alternative to biometric recognition because the tagged clothes of a consumer could help a retailer, as the consumer enters the store, to identify from where the clothes were purchased and the personal details of the consumer.  

Does this possibility of being tracked every minute of the day via the items we carry or wear, represent an unjustified invasion of personal privacy, or is it a price we are prepared to pay for ‘better customer service’?

In Britain there has been, for a number of years, a robust debate over the adoption of national ID cards. The UK Information Commissioner has gone so far as to describe the proposed introduction of such cards as ‘a sea change in the relationship between the State and the Citizen’. Indeed he used the emotive phrase ‘sleep-walking into a Surveillance Society’ to express his concern about this and related developments. Key concerns relate to issues such as ‘data mining’ and consequent ‘data matching’ – the ability to bring together disparate pieces of information about a person. As technology writer Elizabeth Dyson suggests:

The user wants a seamless experience as he (sic) explores the Web, but he wants to appear as a discrete entity to each place he visits with a legitimate identity revealed as appropriate – a credit rating, an employment record, a bank account, or a medical history. Indeed a person’s identity gets splashed all over the Net in little fragments – no problem. But then someone in particular – anyone from a benign marketer only after the customer’s business, to an employer, a stalker, or a blackmailer – can start collecting...
those fragments. One version of the problem is when the data are incorrect (and the user is the last to know); another version is when they are true.\footnote{Release 2.1: A design for living in the Digital Age. Harmondsworth: Penguin. 1998, p. 247}

The use of a single identifier – such as the PPSN number - at least potentially allows for such activities to take place.

Thus we can see that initiatives such as Reach and its associated features raise fundamental questions about privacy, data confidentiality and surveillance. On one side there is the potential for increased convenience for both citizens and government. It would be great to be able to pay all your bills and order a health promotion brochure all from the one government website. On the other hand, do we want a single government agency to have linked information about the car we drive, what we spend on electricity, whether we have paid our tax, and that we have just sought out information on sexually-transmitted diseases?

The Irish government has said it wants to achieve an ‘appropriate balance’ between the personal privacy rights of individuals and the benefits that integrated online services can bring for individuals and society as a whole. But, unlike elsewhere\footnote{See for a good discussion: Edwards, C. & C. Fieschi (eds) UK confidential. London: Demos. 2008.}, we have had virtually no public debate over Reach and associated developments in data-gathering and sharing across government agencies, such as the development of the PPSN itself. Indeed the only significant public criticism of Reach related to the cost of the exercise. The principles of privacy and security, of personal rights and public good, have hardly been addressed, except by public advocacy organisations such as the Irish Council for Civil Liberties and Digital Rights Ireland. On the other hand according to a survey carried out for the Data Protection Commissioner\footnote{Public awareness of data protection and privacy issues. [Survey carried out by Lansdowne Market Research]. Dublin: Office of the Data Protection Commissioner. 2006} up to 90% of Irish people claim that ‘privacy of personal information continues to be of utmost importance’ to them personally. There is obviously a contradiction at work here.

It has been suggested that the fragmented and haphazard nature of Irish government has been a key factor in this mismatch. Ironically this was one of the specific barriers confronted, not altogether successfully, by the Reach project itself. The digital rights activist Cian Murphy suggests that the state’s failure to systematically address the issue of identity management and government services has the capacity to stifle discussion of the issues:

there is no clear debate on the overall Government policy to expand the use of the PPSN. Each expansion can be introduced as merely a small step further than the status quo, just as the present status quo was once a mere incremental advance. There is a process of function creep underway, the PPSN has not yet reached the boundaries of its functionality, especially when one considers the intentions of those now authorised to use it.\footnote{‘From RSI to national identity number? Tracking the development of the Personal Public Service Number.’ Irish Association of Law Teachers Annual Conference, Cork, 10 April 2006, p. 7. ‘Function creep’ refers to how a technology that is introduced for a specific purpose (eg DNA databases to detect}
In other words, the lack of debate on privacy and information policy in Ireland means that significant developments are more likely to occur ‘by stealth’. It is for this reason, I believe, that we need to inform ourselves about the government’s information management policies and their benefits and drawbacks, particularly at a time when radical changes to the public sector and its activities are being mooted.

For the moment, at least, the public face of egovernment has receded even further from view. In an evaluation of Reach carried out in 2004, Dr Joe McDonagh of Trinity College suggested there had been too much emphasis on the technological side of the project, without sufficient attention to the types of organisational changes that would help to make egovernment a reality. In 2007 the government’s financial watchdog, the Comptroller and Auditor General, carried out a broader review of egovernment in Ireland. It was highly critical of the lack of progress and the poor return on an investment of €420m. It called for a much stronger system of monitoring and control of costs and outcomes. Subsequently the Reach website has been discontinued and offers no more than the phone number of an unnamed person in the Department of Finance. The initiative has been buried in Finance’s Centre for Management Organisation and Development, which is the training arm of the civil service.

But the important questions about privacy, data and surveillance remain. At a time of increased pressure on public service accountability, targeting of benefits, cutbacks to services and mounting moral panic over crime, immigration and social welfare fraud, it is even more important to be aware of the data-gathering, sharing and matching activities of government. At least while the Reach initiative was (relatively) out in the open, there was some possibility of keeping an eye on what was going on. Now that the information management processes of the state have been reabsorbed into the heart of the civil service, effectively hidden from view, such practices are dangerously out of reach.

---

serious crime) can, over time, be expanded into new and originally unintended areas (eg DNA databases to clear up burglaries or ‘street crime’).
