The Governance of Privacy and Confidentiality[1]

Justin Keen

Leeds Institute of Health Sciences
University of Leeds

Paper prepared for IRSPM XV, Dublin, 11-13 April 2011

Abstract

This paper considers the adequacy of current governance arrangements for privacy and confidentiality in health care in the digital network era. The paper pursues two lines of argument. The first draws upon Manson and O'Neill's arguments that current data protection policies are built on shifting conceptual sands, and that confidentiality may provide a better basis for policy making. The second focuses on the privacy implications of current trends on the Internet. It is suggested that there is a need to re-think our understanding of privacy in the light of the possibilities created by 'web 2.0', and as a result we should think again about the governance of privacy online.

Introduction

Many countries have had privacy laws and regulation in place for many years now. In general, these frameworks focus on data protection: an organisation should not divulge your personal data to anyone else, unless it has your express consent to do so. It seems reasonable to say that these frameworks offer adequate protection for most of us much of the time. But there have also been heated debates in many countries about their adequacy in

[1] This paper reports on research funded by the Engineering and Physical Sciences Research Council, Award EP/F001096/1. The author is grateful to the Oxford Internet Institute for the opportunity to write, and to attend seminars, during a visit in February 2011.

particular contexts. Some debates have focused on the potential for integrating personal data, the concern being that state agencies and firms can 're-create' us in cyberspace for surveillance, marketing or other purposes.[2] Other debates have arisen from the behaviour of media organisations, which are perceived to have breached the privacy of individuals – often celebrities or politicians - by accessing their health records, tapping their phones or photographing them when, they felt, they were going about their private business.

There has been a great deal of discussion and debate about privacy in health care, and about the difficulty of balancing privacy and the need to share data to ensure continuity of care. Some of this has taken place in the general media, but there has also been discussion in some academic literatures, notably in bioethics. Are you happy if your data are used to identify you as being at risk of a major health problem, such as a stroke or heart attack? Are you still happy if your data are used for medical research, without you giving consent for that use? And are you relaxed about your data, which is out there on the Internet already, being combined and re-used by programmers working in their dorm rooms?[3]

This paper considers the adequacy of current governance arrangements for privacy and confidentiality in health care, in the context of policies advocating the creation of large scale digital networks. The paper pursues two lines of argument. The first draws upon Manson and O'Neill's[4] arguments about data protection, privacy and confidentiality. In essence they argue that current data protection policies are built on shifting conceptual sands, that confidentiality may provide a better basis for policy making, and that we need to find institutional arrangements that we – as

[2] O'Hara K, N Shadbolt (2008) The Spy In The Coffee Machine. Oxford, Oneworld.
[3] They are always in dorm rooms or garages, it seems.
[4] Manson N, O O'Neill. Rethinking Informed Consent in Bioethics. Cambridge, Cambridge University Press, 2007. Chapters 5,6 and 7.

citizens – trust to oversee the proper uses of confidential information. The second argument focuses on the privacy implications of current trends on the Internet. Following Zittrain and other authors[5], it is suggested that there is a need to re-think our understanding of privacy, particularly in the light of the possibilities created by 'web 2.0' developments, and as a result think again about the governance of privacy online.

Digital Health Policies: Integration At Any Price

Health services around the world have long been heavy users of computer systems. In England, for example, general practitioners have used computers in consultations and for administration for many years. Computerisation in hospitals is also extensive, with patient administration systems having been in place for decades, and departments having local management systems. There are a number of large datasets, collected regionally or nationally, which contain data on NHS activity, on specific topics such as deaths following surgery, and on major diseases including cancer and heart disease. Broadly, other countries have similar systems, but the details vary from place to place. Thus the USA and Canada are some way behind England in computerisation of primary care (or its equivalent). And Denmark is ahead of most countries, having had nation-wide networks for the exchange of a wide range of data for several years. The current challenge, everywhere, is to link operational systems together, so that staff in one part of a hospital, or region, can access patient data from one another, using either enterprise systems or integration engines.[6]

As we will see below, there have already been important legal judgements, and a great deal of debate, about personal data held in existing systems.

---

[5] Zittrain J (2010) The future of the Internet. London, Penguin, 2008. Chapter 9.
[6] Integration engines are used to link existing functional systems together. Enterprise systems generally offer organisations integrated suites of solutions: SAP is a well known example.

Even though some of the concerns are about proposals to integrate personal data from a number of (currently) separate databases, policy makers are pressing ahead. In many jurisdictions, including the European Union (EU) and the USA, they are advocating the development and implementation of electronic patient records. These records are pivotal technologies. They will be the source of information for a wide range of activities - not just for diagnosis and treatment, but for sharing with other agencies, for planning of services, for formal accountability purposes, and for academic and commercial research. It is already usual for doctors and other clinicians to provide data to transport and other agencies, and to employers – with our consent - to provide evidence about disability or illness, and presumably this type of sharing will continue.

Electronic records appear to be highly desirable, if the hopes that they will support high quality health care are realised, and they can also be used as a source of data for purposes that we are comfortable with. At the same time, though, our personal data may be travelling in many directions, and without us knowing or being able to control where it goes and how it is used. If the trend towards cloud computing continues, as many computing industry commentators predict it will, then large volumes of our data may be held in 'virtual' environments, far away from our homes or local surgeries. These policy developments appear to emphasise the need to find the right balance between the desirable and less desirable consequences of storing and handling our personal data electronically.

Problems With Privacy

Academic discussions of privacy often refer back to an article published in the USA in the late nineteenth century, by Warren and Brandeis[7], but current debates are framed by laws and regulations developed over the last twenty

[7] http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

years or so. At least in part, they seek to take into account the capacity of computers to hold, move and combine personal data items. The details of the legislation vary, reflecting important differences in legal traditions in different countries, but in general laws and regulations are designed to control the use of personal data. Individuals have the right to know what data are held about them by any organisation, from a badminton club to a bank , and those organisations can not release personal data to anyone without the individual's consent.

Two discussion strands are of interest here, one concerned with practices, particularly with perceived or actual invasions of privacy, and the other with the idea, the concept, of privacy. Taking practices first, there has been a great deal of media coverage of, and commentary on, the uses and perceived abuses of personal health data. These are typically are reported as breaching individuals' privacy in some way. (The term 'information privacy' is often used, to distinguish this use of the term from others, such as 'private space' or 'private life'.) Sometimes the story involves a disk, or laptop, containing sensitive data which is left on a train or in another public place. At other times the problem is more complicated – but still newsworthy – as it involves the 'secondary use' of peoples' health care data for research purposes. We will return to this issue below. A third type of story involves legislation, which is either criticised or directly challenged in the courts. Some examples, such as journalists hacking into mobile phones, lie outside the scope of this paper. But others are relevant. Three examples are sketched out here, to illustrate issues and problems that are discussed later.

S and Marper 2008

The *S. and Marper* case was considered by the European Court of Human Rights in 2008. The case concerned two English individuals whose DNA data were held on a database, the National DNA Database, used for criminal

identification. They had not been convicted of any crime, and asked for their fingerprints, cell samples and DNA profiles to be destroyed. They were not successful in the English courts, and went to Europe.[8]

In its ruling the Court established that it is contrary to the requirements of the European Convention of Human Rights (ECHR) to store personal information relating to innocent people for unlimited periods of time. It concluded that the powers granted to UK authorities, by the UK Parliament, constituted a disproportionate interference with the applicants' right to respect for private life, and could not be considered as necessary in a democratic society. It was, therefore, to a violation of Article 8 of the Convention. The UK Government has now introduced rules limiting the storage periods for DNA data.

For our purposes, the key point is the judgement that the mere storage of DNA information runs the risk of stigmatization. As Fuster and colleagues put it, shadows of suspicion are projected onto people whose data are stored in a database dedicated to criminal identification.[9] Therefore, the storage of such data, when related to non-convicted individuals, has to be somehow limited. But what should the limit be? The Court argued that DNA data could be collected and held for a reasonable period, consistent with the main use of that data. So, it might be reasonable to hold the data for a year, because people might be charged some time after their DNA sample was taken, but it could not be held indefinitely, if there was no conviction.

Section 60

One of the debates in health care circles over the last decade has focused on the risk that an individual's data will be used without her knowledge or

[8] http://bit.ly/fzbvFm

[9] Fuster G, P de Hert, E Ellyne, S Gutwirth. *Huber, Marper* and Others: Throwing new light on the shadows of suspicion. INEX Policy Brief #11, June 2010.

consent, and constitute an intrusion, a breach of that individual's right to privacy. The UK Data Protection Act 1998 states clearly that personal data can only be used for the purposes for which it is collected. Put in more academic language, the Act gives you a privacy right: you have the right to control the use of your data, wherever it is held. In the case of health care, then, any data collected can only be used for your care. But, as already noted, there are many datasets in the NHS which pre-date the Act, which are used for research, and consent for this 'secondary use' was not obtained. There are typically details of thousands of patients in these databases, and it is not practicable to obtain consent retrospectively. An attempt was made to solve the problem – and keep the datasets – in Section 60 of the Health and Social Care Act 2001. The Act effectively made the datasets an exception to the 1998 Act, and set out arrangements for researchers to obtain approval for their work from an oversight body, the Patient Information Advisory Group. Subsequent legislation has led to changes in the details, but not the general principles governing, the secondary use of data.[10]

The debate has been lengthy, and complicated. The central problem seems to be that data protection legislation requires consent for different uses of an individual's information. But medical researchers have argued that there are no implications for individuals: that is, their work does not involve any invasion of individual's privacy. The data protection argument needs to be balanced against the social value of medical research using the datasets, but is not. Some researchers argue that valuable research is impractical or impossible to conduct.[11] What is more, they argue, most of us agree with

[10] New governance arrangements are now in place, following the NHS Act 2006 and the Health and Social Care Act 2008, but the procedure for researchers is essentially unchanged.
[11] Iversen A, K Liddell, N Fear, M Hotopf, S Wessely. Consent, confidentiality and the Data Protection Act. BMJ 332;165-9:2006.

them.[12] In line with the *Marper* case, then, one side argues that holding data without consent over long periods is acceptable, and the other does not. The twist here is that – in the view of some, anyway – most people do not object to the data being held, and research is a legitimate secondary use of the data.

The Celebrity Photograph

The third example is different in kind, but is included here because it draws our attention to the point that health-related information is not the preserve of health care systems or of computers. In 2004 a celebrity was photographed near a rehabilitation centre in London, the implication being that she had an addiction problem. A national newspaper published the photograph, alongside a story about her addiction.[13]

The celebrity took the newspaper to court, claiming a breach of confidence (not privacy). The case went to the House of Lords, where key arguments balanced two rights enshrined in the UK Human Rights Act. The celebrity's right to privacy was balanced against the newspaper's right to publish – what used to be termed, 'publish and be damned'. In the House of Lords there was a majority decision in favour of the newspaper.

These brief accounts illustrate some general points about privacy, which will be pursued below. Information privacy debates often revolve around data held in computers. Data are deemed to be concrete, objects that can be preserved or deleted. And, even if we choose to focus on informational privacy, and not other uses of the term privacy, it is a broad term. It covers

[12] Barrett G, J Cassell, J Peacock, M Coleman. National survey of British public's views on use of identifiable medical data by the National Cancer Registry. *BMJ* 332 : 1068 doi: 10.1136/bmj.38805.473738.7C (Published 28 April 2006)

[13] The event occurred several years ago, and the identity of the celebrity is not particularly important here.

both the storage of data in computers and also photographs that invite us to make inferences about someone's health status.

What Is Privacy?

The real-world debates have unfolded in parallel with academic explorations of privacy by socio-legal and other scholars. The debates are both extensive and detailed, and no attempt to summarise them is made here. It is, however, useful to make the following brief points:

- There are many differing conceptions of privacy, and of informational privacy – the latter being concerned with rights over the uses of personal data;
- Socio-legal writers argue that privacy is, at best, an elusive concept and at worst an unhelpful one;[14]
- Privacy is, largely, a Western concept and there are very different conceptions of privacy (or none) in other cultures;[15]
- For some sociologists, the privacy debate is part of a wider debate about the nature of public and private life. Sennett, for example, has argued that we used to have vibrant public, social spaces, but these have been driven out by various conceptions of the private – the idea of private lives behind our curtains, formerly public spaces being bought up and controlled by private firms (eg some shopping centres).

Manson and O'Neill's Analysis

Data protection policies provide reasonable assurance most of the time, but when they fail they lead us into a regulatory minefield. In practice, lawyers

[14] Solove D. Understanding Privacy. Cambridge MA, Harvard University Press, 2009.
[15] For an interesting discussion see O'Hara and Shadbolt, chapter 7.

and other practitioners must do the best they can within existing regulatory frameworks. Here, though, we are allowed to look forward and try to imagine what a more robust set of policies might look like.

Manson and O'Neill reviewed current thinking and practice in informed consent – the consent that you will be asked to give before a complicated medical procedure, or before you enter a clinical trial or other research study. The basic idea is that you give permission to someone else to do something to you that would usually be unacceptable, such as cut you open with a knife, or give you a blue pill in a trial, not knowing whether it will help you or harm you. In the course of their work they considered the role of consent in relation to uses of personal data, and the idea that abuse could be an intrusion of one's rights to privacy. This is the territory highlighted by the examples given earlier.

They point out that data protection regulations encourage us, often without us realising it, to think in rather mechanical ways about information, and hence about privacy. Commentaries often implicitly assume that:

- Information is like a discrete object, such as a vase or a book. You can track its movements and the ways in which it is used;
- Personal information is inherently valuable. Your last blood test result, the date of your last hospital visit and your DNA sample are valuable, with or without other information about you.

This is a reasonable way to think about a test result or your medical notes, because this is exactly what happens to large volumes of personal data every day. They get moved around within computer networks, or on trolleys, or in

the boots of consultants' Jaguars.[16] If they are lost, there is a problem. It is more difficult to provide treatment to you, and the notes may be found in a skip, and make an interesting read for someone.

But there is a problem here, which can be traced to a 'mechanical' view of information, and particularly personal information. If there is something called personal information, there must also be non-personal information, and we have to distinguish one from the other. But a moment's reflection suggests that the distinction is not helpful. Information about us is in the public domain, and for good reasons, such as our names and addresses in voter registers. It may be possible to make inferences about you from publicly available information, for example from a report in a local paper about your fund-raising for cancer research; or, from information you posted on a social networking site some time ago; or, because a friend bumps into you in your local surgery.[17] The converse argument is that it may be desirable, in practice, to protect an entire document, because of the inferences that can be made about you from it, even though most of the information in it is mundane.

The good news is that there are alternative ways of thinking about information. These are very familiar to us, but for whatever reason are not used in debates about privacy. Manson and O'Neill[18] offer several examples including:

- Information is – in their attractive phrase – inferentially fertile. If I notice that you always seem to have an alcoholic drink in your hand, I may make inferences about your health. Nobody has

[16] Consultants always seem to drive Jaguars in these examples.
[17] The inference might be wrong, of course. But it may still be made.
[18] Manson and O'Neill, chapter 2.

communicated anything about your health directly to me, but my brain starts whirring anyway.

- Information is context-dependent. The importance attached to information depends on the context, on what the parties expect about one another. I may tell my children to behave better, and later that day a passing police constable may also tell them to behave better, with very different results.[19] Information is not a thing, an object that always has the same effect.
- Successful communication depends on established norms. If someone sets out to communicate information, say about a change we should make in our lifestyles, we might not understand the information, or may mistrust the source. It is easy to be confused by messages about the diets we should adhere to, in part because scientists can be reluctant to make definitive statements (except about obvious risks such as smoking); yet we need certainty in our lives, which are quite complicated enough already. And it is easy to distrust messages when they come from governments or corporations who appear to be putting their interests above ours - in statements about salt levels in prepared foods, for example.

Manson and O'Neill identify a central problem in the data protection view of privacy: we simply cannot equate personal information with information that makes people identifiable. They do not stop here, but go on to make three proposals which are relevant to the arguments here:

1. We should consider other rights – not just privacy – when we are evaluating 'secondary uses' of information;
2. Confidentiality may provide a sounder basis than privacy for regulating the uses of health and health care information;

[19] This may not be true for you.

3. In practice, any workable solutions will require us to place our trust in institutions.

Privacy first. They argue that it is helpful to think about the various invasions and intrusions into our privacy, to separate them out and consider them in turn. For example, the celebrity photograph may not be a privacy issue at all, given that the celebrity was walking down a street, and she and the photographer were both allowed to be there. It may, though, potentially be a breach of confidence. The celebrity had a confidential relationship with a professional, and the professional's existence was inferred from the photograph. Similarly, we might choose to re-visit Section 60 (or Section 251 now), and wonder just how the use of our data for medical research can be construed as a privacy problem. This secondary use has few or no implications for the individuals who provide the data, given that those data will only ever be used in aggregated form, including hundreds or thousands of individuals. So, the threat of intrusion into individuals' privacy lies somewhere between 'very small' and 'nil'.

Manson and O'Neill go on to argue that confidentiality offers a firmer basis for policy making than privacy. The current ways in which both privacy and information are used, in practice, cannot work. But it seems reasonable to suggest that the real sensitivity, for many of us, concerns the confidential conversations we have with doctors and other health professionals. We should, therefore, try to find ways of making sure that the content of consultations is not divulged. This shifts the focus from data/information to conversations, or communications.[20] Highly developed social norms already govern relationships between health professionals and patients. Trust is crucial: if patients do not trust professionals then they may be reluctant to seek help, and thus jeopardise their own health. The argument put forward

[20] Manson and O'Neill, pp. 123-7.

is that it should be possible to regulate *behaviour*, for example by monitoring whether health professionals divulge information to any third party inappropriately.

The confidentiality proposal helps us to understand the issues that are, or at least will be, involved in the uses of data held in electronic patient records. Some 'secondary uses' of data are already established, and most of us seem comfortable with them. The issue will be to make sure that the contents of conversations, and other communications, between patients and health care staff are not divulged to a third party. That is, it will be helpful to distinguish between releasing data that might break confidences, and data that might, aggregated with data from other patients, be legitimately used for planning, research or other purposes.

Their third proposal is that any workable alternative will require us to place our trust in certain institutions. In this paper the institutions include the medical and other professions and also include those who handle our information such as IT professionals and ward clerks. This might appear to be an obvious point, but it is made against a background din of commentaries about the untrustworthiness of institutions. One only needs to think about banks and – for English readers – MPs' expenses to appreciate the problem. Manson and O'Neill argue that any solution will depend on two things, which in this context are trust in doctors and others involved in our treatment, and accountability arrangements that encourage appropriate behaviour.

The current arrangements in the NHS and other health services are not considered further here. The remainder of the paper will focus on two different types of institutional arrangement, namely the implications of 'web 2.0' and new policies on making NHS data available to third parties. Both

pose challenges that have few obvious precedents in debates about privacy and confidentiality.

Privacy 1.0 and 2.0

In this section Zittrain's recent arguments about privacy and the Internet are used to frame thinking about health and health care information. Zittrain argues that we have lived through a long 'Privacy 1.0' era. In relation to computers, concerns focused on relationships between the individual and the state, and individuals and large firms, and on ways in which they might be able to collect and collate large volumes of data and – to put it bluntly – abuse it. Developments such as the ID card debacle in England,[21] and the excessive zeal unleashed by the PATRIOT Act in the USA[22], where the Federal Government monitored email traffic without US or other citizens knowing, do nothing for one's confidence in governments. There is also unease about the activities of large firms, and particularly large Internet firms. Concerns about the uses of personal data flare up from time to time, for example over Google Street View and attempts to change privacy settings in Facebook.

Zittrain acknowledges the importance of Privacy 1.0, given that governments and large Internet firms will be with us for the foreseeable future. But he argues that the architecture of the Internet has introduced a new set of privacy concerns. The key point is that, in Privacy 1.0, the chief concerns are governments and large firms. While they might have extensive powers, and in the case of governments be able to give themselves new ones, their freedom of action is limited in practice. A range of important norms, backed up by laws and regulations, govern their behaviour. But the advent of large scale

[21] Benyon-Davis P. The UK National Identity Card. Journal of Information Technology Teaching Cases 1**;** 12–21:2011.
[22] Weimann G. Terror on the Internet. Washington DC, US Institute of Peace Press, 2006.

digital networks, with peer-to-peer applications such as social networking and file sharing, changes the situation. It is the Internet equivalent of the shift from hierarchies to network governance, with control moving from central points, and being superceded by a world where there is no central control. Control, if the word means anything at all, is distributed across the network. Current assumptions about privacy are no longer so relevant, and we need to think about Privacy 2.0.

Identifying the problems here takes a little imagination, but only a little. Let us say that there is already a certain amount of information about you on the Internet. Your work contact details are easy to find. You have a Facebook account, and a Flickr account with holiday photos freely visible. Now suppose that the guy in the dorm room (the same one we met earlier) decides to compile a collection of photographs of smokers, or of people near sexual health clinics. Alternatively, he might decide to combine all the information he can find about particular individuals, which might be in several different places but can now be 'mashed together'.

This is where some of Manson and O'Neill's arguments come to life, albeit with a twist. Remember that they point out that information is inferentially fertile. The prospect facing us, in the digital era, is that lots of people in dorm rooms and garages can exploit *both* characteristics of information. The fact that data can be captured and manipulated allows people to combine data in different ways. And, because it is possible to make inferences from it, that combined data may tell them rather more about you than you feel is reasonable. But because the mashing up is being done in a dorm room on the other side of the world, you have no idea it is happening, and even if you did it would be very difficult to trace.

This looks like an unholy alliance of digital data, inferential fertility, and a software environment that allows all sorts of manipulation beyond our gazes. Zittrain, like other commentators, recognises the problems that lie ahead.[23] Like Manson and O'Neill, he appreciates the importance of establishing appropriate behavioural norms, and backing them up with appropriate regulations. Detailed, and widely accepted, practical arrangements lie in the future. They will, though, need to be based on behavioural norms, and written into hardware and software, for example in making it possible for individuals to track data wherever it is moved or copied. There would be an audit trail for everything you post, and ideally a way of retrieving information, or at least challenging the ways in which it is presented by others. As for now, however, peer-to-peer developments serve to emphasise the impossibility of preserving informational privacy, and offer indirect support to the view that confidentiality offers a more realistic basis for thinking about what can, or must, be protected.

Information-As-A-Service

In this last section, the arguments about information held within health systems and information available out on the Internet come together. Just as in the last section it is difficult to pursue the arguments very far, but they raise important issues about the governance of information in the future.

The Information Centre for Health and Social Care is responsible for the publication of a wide range of information about the NHS in England.[24] In a bill before Parliament in London, the Centre is being given new powers. One of these requires it to act as an 'honest broker', and make data available to third parties, which might be private firms considering bidding to provide NHS services, local organisations interested in understanding the health

[23] For example, Lanier J. You Are Not A Gadget. London, Penguin, 2011.
[24] http://www.ic.nhs.uk/

profile of their neighbourhoods, or firms interested in providing 'value-added' information services to the NHS and to other firms. This is novel territory for the NHS. But, if 'digital era governance' arguments prove to be correct, we should expect to see much more of this kind of policy, both in England and elsewhere.[25] It is not just of parochial interest.

On the face of it honest brokerage is an excellent idea. It is difficult to obtain NHS data, even in pseudonymised form, for any purpose. Even academic researchers, having obtained all the necessary consents, can end up empty-handed, with NHS organisations somehow failing to get round to handing over data. (And if you believe in markets in health care, then you will be excited by the idea of an 'information marketplace'.) But the arguments set out earlier alert us to two potential problems. The first is that the plan is likely to run into the same problems as the clinical researchers we met earlier. Every request will have to go to a committee,[26] and some apparently reasonable requests will be caught in the difficult area set out in the Section 60 example earlier. This may well be irritating for those involved, and the only consolation is that plenty of people will empathise with them.

The second problem is potentially more serious. It seems possible that the 'honest broker' proposal is based on the assumptions that Manson and O'Neill criticised: information is something that is moved around. But, as we have seen, it is also inferentially fertile. An apparently mundane data item may reveal a great deal about one or more people, in the right context. And, as Zittrain has pointed out, the Internet is the place where extensive combination and re-combination is possible. The potent dual nature of information, with the simultaneous ease of combining digital data and

[25] Dunleavy P, H Margetts. The second wave of digital era governance. Paper delivered at the American Political Science Association Conference (4 September 2010 : Washington DC, USA).
[26] A sub-committee of the National Information Governance Board for England.

inferential fertility, may fuse here with the availability of new data (which has hitherto always been held within the NHS, subject to strict information governance regulations). The danger is that data which has been carefully checked, to make sure that it contains no personally identifiable information, will be released into an environment where identification is perfectly possible, through combination with the wealth of direct and inferential information available on the Internet.

It may be that there are technical solutions which will address, or at least minimise, the risks. Cryptographers have developed a number of ways of ensuring that it is not possible to identify an individual from fragmentary information, eg to get back from an anonymised dataset to an individual's details.[27] But real-life experiences with the publication of datasets, which the publishers were confident were anonymised, do not augur well.[28][29] The inferential fertility of information on the Web would appear to pose considerable challenges to cryptographers and policy makers.[30]

Concluding Comments

This paper, following Manson and O'Neill's analysis, has argued that existing privacy regulations cannot work, for health care or other data. There are fundamental problems with the ways in which privacy and information are defined and used. Confidentiality may offer a more solid basis for policy making.

If one then moves on to consider developments on the Internet, two new governance problems arise. The first, which is a broad policy issue as well as

[27] For example, by adding random noise to the results of a query.
[28] Lamberg L. Confidentiality and Privacy of Electronic Medical Records. *JAMA.* 285(24):3075-3076:2001
[29] http://www.wired.com/threatlevel/2010/03/netflix-cancels-contest/
[30] http://www.computer.org/portal/web/csdl/doi/10.1109/SP.2008.33. [doi: 10.1001/jama.285.24.3075]

a health policy one, is that personal data held in various places can be traced and combined, in ways that many people do not realise are possible. The second concerns the 'controlled' release of data from health organisations, for use by a range of third parties. There is a risk that these data, combined with data already available on the Interent, will lead to privacy breaches. That is, they may lead to unwanted intrusions – all the worse because people may not be aware that they are happening. It is possible that there are technological solutions to this problem, but at the very least it poses a challenge that have not previously occupied health policy makers.

Finally, we return to electronic patient records, those pivotal technologies mentioned earlier. The attraction to policy makers is obvious, as they are the very stuff of Modernist Heaven, promoting safety, efficiency and technology simultaneously. As noted earlier, the proposal that confidentiality should be protected makes sense for this technology. The challenge will be to ensure that the many demands on them do not lead policy makers to chop up our data, passing it on to others in tiny pieces, believing that they are safe. And all the while, our friend in the dorm room is quietly piecing your or my record back together again.