
# Following Society's Digital Footprints: Critical Policy Issues for the Digital Economy

Victoria Nash and William H. Dutton

Policy Forum Discussion Paper 20

Oxford Internet Institute
University of Oxford
June 2011



Report of a policy forum held at the Oxford Internet Institute, University of Oxford, on 16 February 2011, organised in conjunction with the Horizon Digital Economy Research Centre, University of Nottingham.

# Introduction

We live in an increasingly data-rich world. Everyday activities, like buying groceries, catching a bus, or driving a car can now generate significant streams of electronic data which from which new services can be developed, but also from which other individuals, companies or government agencies can infer a great deal about our personal behaviour. Added to this are the myriad new technologies which hold such rich possibilities for improvements in our health, entertainment, communications or simply our everyday living. Many of these new services and devices automatically capture data about even very intimate aspects of our lives, such as our travel patterns, search habits, our musical tastes, our home electricity usage and even medical data such as blood pressure or heart rate. In many cases, much of this data is collected, processed and re-used without our conscious intervention, awareness, or consent. What is more, this information has a growing, tradable value and the market for this information and its storage is expanding at a great pace. Novel services and applications based on these data are continually being developed, which together with the emergence of new data sources and forms will encourage further widening scope of its collection and use.

As these developments unfold, two major questions arise:

- Are there any genuinely new socio-economic or policy challenges or concerns raised by the generation, collection, processing, storage and use of the data deluge?

- Are we confident that existing policies and practices governing these processes are fit for purpose?

A policy forum was held at the Oxford Internet Institute on 16 February 2011, organised in conjunction with the Horizon Digital Economy Research Centre at the University of Nottingham. Attended by experts from across academia, industry and government, and with a multi-disciplinary focus, this forum sought to address these two questions, and to set out a series of recommendations for research, policy and practice. These position papers and debates identify the growing complex of actors coupled together in the web of transactions critical to the digital economy—a development that poses a new challenge to understanding and regulating the privacy of personal information and its protection in the digital age.

# I. Contextualising the Discussion

Early sessions in the forum were devoted to identifying the main technological, social, economic and legislative drivers that are shaping future scenarios. Whilst it is clearly artificial to separate these various factors, they are set out distinctly here for the sake of analysis. The ways in which these various factors are constantly combining and recombining to shape current and future practices of data collection and use is at the heart of this discussion paper.

## Privacy Policy and Regulation

Alan Westin, an early pioneer of privacy studies, defined privacy as: "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others".[1] In practice, the definition and legal context of privacy, and data protection, vary across nations. While the central themes of this paper apply across different legal-institutional jurisdictions, given the high level at which they are discussed, we will focus primarily on the UK and Europe more generally, given a common framework governed by the European Data Protection Directive.

The European Data Protection Directive (95/46/EC)[2] is the main regulatory framework governing collection, storage and use of personal data in Europe. It has been subject to extensive review over whether it needs updating in the digital age.[3] At the time of the forum, the results of this review were not yet available, but two participants, involved in the review, argued that it was unlikely that the underlying principles would be significantly altered, although more guidance might be given on their interpretation and application, where a number of uncertainties remain a key issue for all actors in the digital economy. For example, one fundamental area for clarification and possible extension might be the very definition of 'personal data'.

A related set of issues are tied to the difficulties of international differences in policy and regulation and their harmonization. For example, in an era of cloud computing and international design and operation of both devices and applications, the European Directive is clearly inadequate to govern the flow of personal data across international borders beyond Europe. Here, the contrast between European countries' strict principles of data protection and the more relaxed regimes enjoyed elsewhere, such as the US, was highlighted as adding further complexity to the question of who can access our personal data and how it is treated. The Safe Harbour agreement with the United States was implemented in 2000[4] to ensure that data could be exchanged between European countries and US organisations, so long as those organisations had 'adequate' measures in place to protect the data and personal privacy. This arrangement is still regarded with suspicion on both sides, with some concern within Europe that the bar for 'adequacy' is set too low, and further that it is largely reliant on voluntary self-regulation, whilst in the US, there is some resentment at what is often seen as an informal barrier to free trade. The exchange of data between Europe and countries outside the US is even more fraught.

---

[1] Alan F. Westin (1967) Privacy and Freedom. New York: Atheneum.

[2] The text of the Directive can be found in full at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[3] According to the European Commission's Justice Directorate, the purposes of the Review are to: Modernise the EU legal system for the protection of personal data, in particular to meet the challenges resulting from globalisation and the use of new technologies; Strengthen individuals' rights, and at the same time reduce administrative formalities to ensure a free flow of personal data within the EU and beyond; Improve the clarity and coherence of the EU rules for personal data protection and achieve a consistent and effective implementation and application of the fundamental right to the protection of personal data in all areas of the Union's activities (available at: http://ec.europa.eu/justice/policies/privacy/review/index_en.htm).

[4] Committee Decision 2000/520/EC, details available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML

## Technological Advances

The vast array of technologies that are automatically collecting personal data was set out as one of the most significant recent developments. Whilst many of the technologies discussed were simply extensions of familiar devices or services, such as advances in mobile phones or personal music players, others, such as social networking sites or biosensor networks represent quite new developments. In both cases, however, participants were clear that whilst the motives for data collection might be benign (recommending new music I might like, or contacts I might know), the extent of the 'digital footprint' left by individuals in their daily activities was expanding rapidly, and with significant implications for the protection of personal privacy. It is perfectly possible that such unobtrusive but pervasive collection of apparently 'low-level' and non-sensitive personal data might actually accumulate into broader-scoped intrusion for the majority of individuals in the medium term.

More conventionally, concerns are raised about the development of new technologies or applications designed for the explicit purposes of control and surveillance. Enforcement of law and order and maintenance of national security are clearly goals central to the very existence of the state. However, some participants described how technologies such as automatic number plate recognition or augmented reality were being introduced into policing with more focus on their exciting possibilities for solving crime than their implications for personal privacy or data security. The proliferation of CCTV across the UK is an example of this drive for increased surveillance in the name of crime reduction. Two participants had recently attended a Home Office conference on the use of augmented reality (supplementing the physical world with data) in detecting and solving crimes. They noted this as an example of the apparently common view in many professions that 'more data is necessarily a good thing'—perhaps because you can do more things with it, even if you don't yet know what.

Against this backdrop, other emerging technological advances were presented as having potentially game-changing features. As Horizon's Derek MacAuley noted in his introduction to the forum, we could begin by challenging one of the key assumptions, namely that we need to give away our data in the first place. We have a right to know what data is held about us, but wouldn't open data requirements be better met by genuinely retaining control of our data? This is increasingly a real technical possibility, with the development of new technologies that enable users to import an application that can process their data and submit a response, rather than the original data being submitted to calculate that response. A good example here might be drawn from tele-health or mobile health initiatives. Remote monitoring of patients with long-term medical conditions is quite standard, with personal data such as blood glucose levels or oxygen saturation routinely generated and transmitted to a remote care team. In many cases there is a clear need for the raw data to be transmitted so that it can be interpreted by medical staff, but in some cases all that needs to be checked is that measurements remain within certain set limits. In such a situation, there would be no need for the data to be transmitted, as in many other contexts where a single response could replace the transfer of personal data, such as the simple Accept/Reject required when a shop or online store checks to see if there are adequate funds in a purchaser's account.

## The Internet of Personal Things

One of the major technological developments around the 21st Century Internet is the so-called 'Internet of Things'. This refers to the movement from the Internet being primarily tied to connecting individuals, with their own identifiers, to connecting devices—things—each with their own unique identifiers. For example, a household's energy meter will be linked with the utility company in a network of things, but, of course, the data collected by meters provides information about the household that could reveal personal information, such as

when a family wakes up, how efficiently they use their energy, when they turn on their coffee pot, when they go on holiday, and so on. As more and more things tied to individuals and households are networked, the Internet of Things will provide an increasingly valuable source of personal information, some of which (such as that relating to healthcare) may be very personal.

## Economic Developments in Markets Relating to Online Data

On 3 January 2011, Goldman Sachs' private investment in Facebook gave the social networking site an effective valuation of $50 billion,[5] illustrating the scale of what is at stake in the digital economy. Whilst that has yet to be tested publicly on the stock exchange, the valuation of Facebook was based on two features of its service: the sheer number of individuals signed up to use it (over 500 million active users in January 2011) and the vast array of personal data that each person volunteers about themselves. Although a much smaller contender, LinkedIn floated at $4.25bn in May 2011 and has seen significant gains in its share price since that point. In both cases, the value consists not so much in the discrete pieces of information that every user provides, but the way that the data can be combined to create holistic profiles of individuals' lifestyles, employment, habits, preferences and connections, all of which can be upsold to deliver highly personalised advertising.

If the above two examples demonstrate the inherent value of individual data profiles, a further economic development in 2011 has been the advance of services which offer remote data storage and processing. Known as cloud computing, such services have been embraced by the business press as an excellent way of decreasing capital expenditure by moving data storage and processing to the operating costs column of corporate balance sheets. Whilst such companies should, in principle, be able to specialise, providing the highest degree of data protection, and removing a substantial burden from smaller businesses, they also throw up new challenges, such as concerns about data location and jurisdiction, vulnerability to hacking or loss, and questions about ownership of data should service providers be bought or go into administration.

## Expanding Networks of Actors

From these two examples alone, it is clear that the economics of data are changing rapidly, but one less well-documented way in which the digital economy might be shifting, and which has big implications for the management of personal data, is the increasingly complex ecology of actors involved in providing data services. It was noted that in most electronic data services in the 1990s there would have been just three parties: the data subject, the data controller and potentially a data processor. In 2011, the picture is much more fragmented. In one everyday activity such as where an individual uses a social networking site (SNS) on an Android phone, a minimum of seven different actors might be involved in generating, collecting, storing, processing or using the personal data:

**1.** A primary subject, A…

**2.** …who is finding out about the status or location of a second subject, B, using the SNS;

**3.** A primary data controller, i.e. the application developer (the SNS); who is then running various adverts which are profiling the primary subject via…

[5] Reported in the Financial Times at: http://www.ft.com/cms/s/0/e0dad322-173c-11e0-badd-00144feabdc0.html#axzz1JWv77tKS

**4.** …a second data controller, namely an ad network device that will cross-reference the data subjects' identity amongst other application developers.

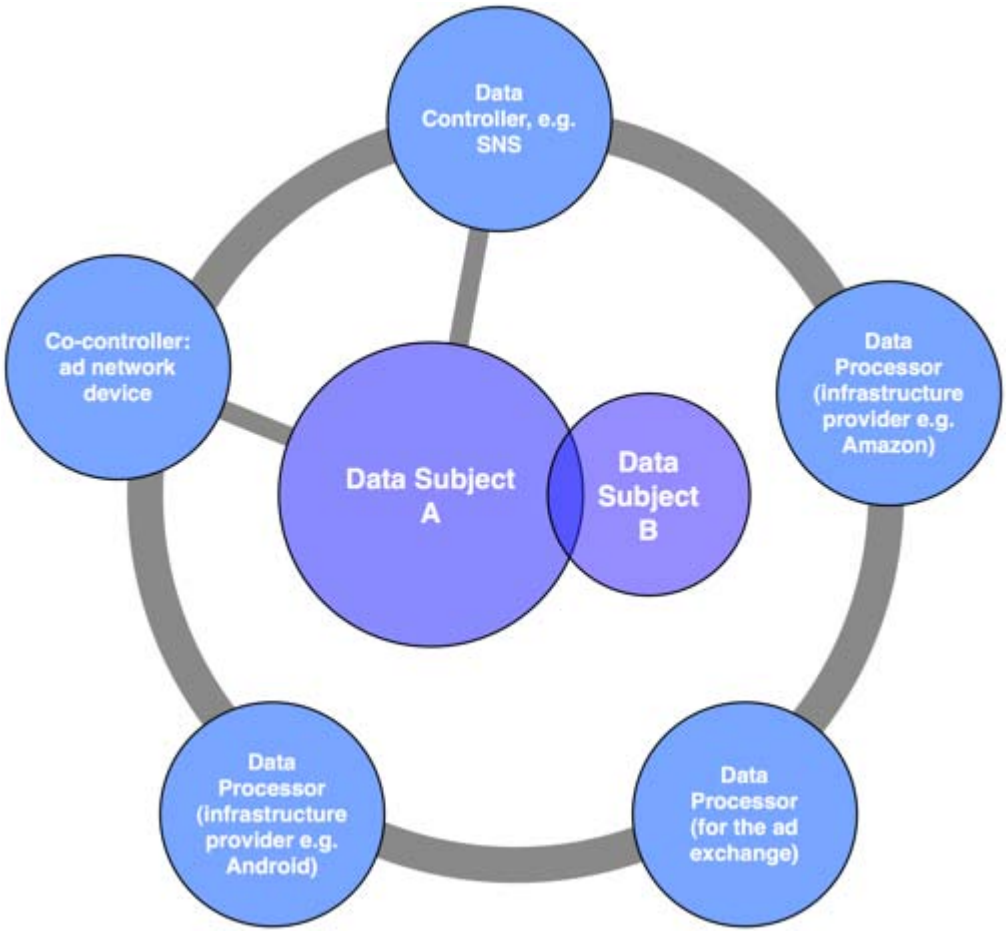
**5.** There are at least three different data processors—the ad exchange…

**6.** …the phone's infrastructure provider (Android) and…

**7.** …the infrastructure provider who is hosting the data in the cloud (e.g. Amazon EC2).

In such a new and complex scenario there may be legal uncertainty over the role of each actor, and with modern arbitrage services it is entirely possible that even a cloud service provider might not know where the data is held at any one point in time. Data protection was introduced in an era when electronic transactions amongst even three actors would have been considered too complex for individual consumers to fully understand, monitor, or control. This underpinned arguments for a more expert data protection office, such as the UK's Information Commissioner. The expanded array of actors makes these issues far more difficult to manage, and potentially throws up new challenges for current data protection regimes.

**Figure 1. The evolving network of actors involved in a data exchange relationship.**



## Social and Demographic Change

In many affluent western nations, the combination of an ageing population and working women having children later has led to the development of what has been dubbed the 'sandwich generation'. Whilst most such countries have effective and affordable health care systems, the support structures for social care are often much less sophisticated and the scope for market innovation is huge. It was suggested at the forum that this might provide a clear scenario in which the market for personal monitoring services and applications for assisted living could be subject to rapid growth over the next decade, and that this could be an area where new ethical and legal challenges might arise as those individuals who most need the services could struggle to fully understand the likely uses and implications of the data they are surrendering.[6] There may already be clear legal frameworks in place to protect the interests of those who cannot autonomously decide for themselves (such as the Mental Incapacity Act),[7] but the social, familial and economic pressure to conform with services such as remote monitoring or biosensors may undermine the autonomy of those who are not incapacitated.

In this context it was pointed out that there are often unexpected social consequences of technological change. For example, would relatives or neighbours visit an elderly person as frequently if they knew that a firm or medical service was monitoring their daily activities? It was also noted that there is perhaps a hidden digital exclusion issue here. For example, whilst much political capital is made of schemes seeking to connect 'silver surfers', for those who cannot or choose not to get online it will become ever more difficult to make informed choices about whether to release the sort of data collection that assisted living services require, which in many cases, may be effectively impossible to refuse. Many of those who most actively promote digital inclusion have an economic interest in doing so—and this applies even to some of those partnering in academic programmes, such as the Digital Economy Programme. This is because the viability of many digital commercial services is dependent on the take-up of the Internet, such as the revenue of online news services. This should be no surprise; the consumer is always part of a lucrative value chain, but where personal data is a key component in that value chain, individuals are not necessarily well placed to understand what their data is worth. In the UK, both the Communications Consumer Panel and OII (through the multi-partner Privacy Value Networks project) have been carrying out studies that aim to discover how much value people place on their personal data and how their attitudes to privacy are shaped by its use in different contexts.[8]

Moreover, it has long been known that even when consumers or citizens are concerned over their personal data, they are likely to subordinate their concerns if it means that they can obtain services that they see valuable to their health, or safety or even convenience.[9]

---

[6] Although not discussed at the Forum, another similarly challenging scenario might emerge at the opposite end of the age scale, as children and young people spend ever more time using technology as part of their everyday lives. Many services already specify a minimum age for use in their Terms of Service (thirteen for Facebook, effectively eighteen for Google), but it is unclear whether this offers sufficient protection to young users who inevitably wish to use these services. Part of the revision of the European Directive is directed to providing enhanced protection for children and minors.

[7] The UK Mental Capacity Act 2005, available at: http://www.legislation.gov.uk/ukpga/2005/9/contents

[8] Privacy Value Networks project, details available at: http://www.pvnets.org/ **;** Online Personal Data: the Consumer Perspective (2011) Communications Consumer Panel, available at: http://www.communicationsconsumerpanel.org.uk/Online%20personal%20data%20final%20240511.pdf

[9] Dutton, W. H. and Meadow, R. G. (1987), in Levitan, K. B. (ed.), 'A Tolerance for Surveillance: American Public Opinion Concerning Privacy and Civil Liberties,' Government Infostructures, Westport, CT: Greenwood Press, 147-70.

Therefore, while citizens and consumers value personal privacy, they are not necessarily willing to give up other valued services to protect their privacy. This likelihood places even more responsibility on government and industry to design privacy into products and services in order that users do not need to provide unnecessary personal information to obtain services in the private or public sector, as discussed below as 'privacy by design'.

# II. New Technologies, New Challenges?

Whilst it was clear that there are multiple factors driving participants' concerns about the implications of the so-called 'data deluge', it was initially less clear whether these concerns were genuinely new, or simply related to the scale of the problem. Over the course of the day, it became apparent that technological developments are on course to digitally capture far more actions, creating an exploding array of digital traces in ways that will create a range of new legal and regulatory uncertainties. Discussion therefore crystallised around several core challenges and questions, which are set out below.

## Consent and Control

The issue of consent is highly problematic. Given that informed consent is one of the grounding principles of fair data use, it is worth noting that, in many circumstances, data subjects will not really understand what they are consenting to. One issue is the complexity and length of many service agreements; another is the complexity of the data exchange and its processing. As one participant noted, the challenge comes not so much in consenting to hand over the raw data, it is predicting and understanding precisely how it will be used. The significance or sensitivity of data is a matter of context and interpretation; further, data controlling institutions don't always have clear intentions regarding their likely uses of data, so it is doubly hard to see how individuals can truly give informed consent.

In addition, there may be circumstances where individuals have little or no choice about handing over their personal data. For example, whilst it is true that no one has to use an application such as Twitter, if they want to do so, they have no choice but to agree to the terms of service. Choice is even more illusory in situations where the service has a significant life-impact, such as when applying online for state benefits or receiving health-improving sensor technology. This goes against the common understanding that consent must be freely given, i.e. that not to consent is a realistic and feasible option.

The concept of informed consent has been at odds with practice for some time. One of the early insights about organizational information systems was that data collected for one reason is often of great value for other reasons, never anticipated by those who initially decided to collect this information. The ad hoc use of operational information is of great value to a diverse array of unanticipated uses. In fact, the current move to open government data to the public, such as through linked data systems, is based on the fact that data collected for one purpose can have a multitude of other applications, particularly when used in combination with other data. This is exacerbated by the tendency of managers and professionals to collect all the information they can, even when advised not to, in case information proves to be of value at some later point. Data of no perceived value to a particular actor at one point in time can be of value to other actors, at other points in time, or

when linked with other data. This clearly undermines the concept of informed consent on the basis of expectations about explicitly defined and delimited usage.

## Privacy by Design

If the tide can't immediately be turned on the ever-increasing generation of electronic personal data, aren't there better ways of limiting damage to privacy by ensuring it is securely transmitted? Several participants questioned why data isn't more frequently encrypted—or, indeed, not broadcast at all. The most obvious answer is that this would be more complex for the technologist implementing the service or product, more costly for the organisation providing it, and because it is not a statutory requirement under current regulation.

'Privacy by design' has a long and successful history[10] but is still not routinely implemented. This may in part be because it is still not cheap and easy to use, and the incentives to make it so don't yet exist.[11] And unfortunately, if there is a lot of money to be made from collecting data in a non-secure way, then this will usually provide a strong rationale for doing so, especially in an internationally competitive market where it is difficult to unilaterally introduce new and costly security standards. This is hard enough for a big multi-national, but almost impossible for a Small or Medium Enterprise (SME). A more practical alternative would be to build secure, compliant systems for SMEs that would ensure any applications they run operate in a secure and privacy-respecting environment. Apple, for example, does check all applications officially supported on its devices, and so could, in theory, impose standards that would effectively create a secure environment. This raises its own controversies, however, as the degree of control Apple maintains over devices such as iPhones or iPads could also be seen as limiting the inherently generative potential of the net.[12] There are also clearly trade-offs to be made: we may want to maximise privacy, but it can't be denied that the potential value to be gained from mash-ups of existing open data sources, such as through location applications, such as Google Latitude or EchoEcho, is substantial. Indeed, the supposedly immense potential of the semantic web is built on the assumption that valuable information can be automatically extracted from the layering of different data sources. How should these trade-offs between values, services and privacy be made?

Given that technological advance is so rapid, some participants asked why we can't do more to instil certain 'offline' norms into new communication products (and particularly social networking tools), such as ensuring that one's activities can't be 'overheard', or being able to indicate when one doesn't want to be contacted or exposed to adverts? It may be the case that offline conversations and interactions cannot be perfectly controlled either, but this is no reason not to aim for such control online. Certainly human–computer interaction (HCI) as a discipline has tried to do this, but it has proved difficult to build awareness and sensitivity into online communication.

---

[10] See for example, the report by the UK Information Commissioner's Office (2008), Privacy by Design, available at: http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf

[11] Although some such as the UK Information Commissioner's Office have tried to make the business case for investment in privacy by design. See Information Commissioner's Office (2010), The Privacy Dividend, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_dividend.pdf

[12] See for example, J. Zittrain (2008) The Future of the Internet and How to Stop It, Yale University Press.

One participant asked whether we ought to challenge the preference for data longevity. Often data is generated in an ephemeral way, but systems are built to store and record data for the longer term, beyond when it is needed. Designing systems and data retention policies and practices to respect privacy might thus involve removing the possibility of storing data for longer than is necessary, if at all.

The discussion reminded participants that there is no single magic bullet, a one-off tool or process that would make data exchange completely secure. In addition, there are many other factors that may limit the development of privacy-respecting tools and services. Cashless payment systems, for example, have been hampered in the past by conflicts over patents, whilst developing legislation on competition and data portability in the social network sphere is another example of how broader policy initiatives can impact on privacy design standards.[13]

It is also useful to remember that many systems have unanticipated implications for privacy. For example, early discussion of the cashless society raised fears over transactional data as a particularly revealing digital footprint of an individual's activities. Unexpectedly, electronic payment systems spawned the ATM or cash machine that allowed individuals to withdraw cash more easily, thus enabling them to pay for more items without recourse to a cheque or credit cards, resulting in greater privacy and a less defined digital footprint.

## Sensitive Data

In addition to consent, participants also considered other aspects of the current European data protection regime, such as the definition of personal data and sensitive personal data. The concept of 'sensitive personal data' was seen to be particularly problematic and ambiguous because in theory any personal data could be seen as sensitive, depending on its context and use. Although the European Data directive (unlike the UK Data Protection Act) does not use the term 'sensitive' it does restrict the processing of personal data in certain categories (which broadly map on to the definition of sensitive data in the UK context), namely:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- data relating to physical or mental health.[14]

The linkage of a variety of seemingly innocuous information about an individual could be used to make inferences about one's physical health or political opinions, for example,

[13] Data portability concerns the individual's right to shift data from one system to another, without being tied down. This argument was previously used to enhance competition amongst mobile phone operators, ensuring that users could ask for their contacts' numbers and information to move with them if they moved network; the same argument is now being applied to social network sites. See for example the Press Release from the European Data Protection Supervisor in January 2011, responding to the review of the EU legal framework for data protection: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2011/EDPS-2011-01_Data_protection_reform_strategy_EN.pdf

[14] See Article 8 of the European Data Protection Directive (ibid).

making this classification hard to maintain in a digital world of linked data. It would, of course, also be naive to think that only this limited category of data is problematic. Notably, it does not include financial or economic information, despite the fact that fraud and identity theft may result from the insecure processing or storage of data such as bank details. Further, the vast array of personal data that is already available and exchanged—such as profiles on social networks sites and personalised settings on next generation phones—is bound up with concepts of personal identity. There are many possibilities where the legitimate use of this data could embarrass or harm an individual. In such ways, definitions of personal data, sensitive personal data, and the concept of data protection, are creating uncertainties for the individual, but also the wide array of actors involved in the provision of digital services and information. Legal and regulatory uncertainty is of course not new, but is a risk that could undermine innovation in the economy.

## Data Provenance

A related concern was raised about data provenance, which may reveal more about us than we would imagine. It might seem strange to suggest that the act of generating or creating data could potentially reveal as much information about us as the data itself, but if we consider the process of tagging content, for example, it is clear that inferences could be made about the tagger, even if that individual does not believe he is releasing personal information about himself. In the context of the social web or Web 3.0, where users layer tags of meaning on top of others' content, this is a worrying prospect. Tim Berners Lee recently argued that anonymity in computer transactions will be soon be impossible, as a result of the ancillary information available from which our identity can be inferred even if we are able to shield it explicitly.[15]

## Adequacy of Current Legislative Framework

As well as the very detailed discussion of regulatory principles as outlined above, there was broader discussion as to whether the current EU data protection framework (under review at the time of the forum) was fit for purpose, or whether the rapid pace of change in technology challenged its fundamental principles. Whilst participants disagreed on specific points such as the suitability of the sensitive/non-sensitive personal data dichotomy and the adequacy of the limitation of purpose principle, all agreed on the importance of regulatory clarity. Confusion about the interpretation and application of different elements of existing legislation were perceived to be bad for individual data subjects, and costly for data-handling businesses, although exceedingly difficult to resolve.

One rather new 'grey' area, emerging more prominently with the growth of user-generated data, is the ownership of electronic data once a person dies. It may legally become part of the deceased person's estate, but does that mean, for example, that it should be deleted on request of the family? Or that it should not be deleted at all? Under UK law, for example, the deceased is not covered by existing privacy legislation, so it is not the case that we can be said to have any automatic rights to the deletion of our digital footprint once we're dead.

There is currently ongoing policy discussion of the 'right to be forgotten' in many EU member states; but this needs to be considered in tandem with the concept of a digital legacy, and the extent to which we leave behind not just atomised digital footprints but an imprint of our identity which might (or might not) have a greater significance after our demise.

[15] Tim Berners Lee, Royal Society Web Science Conference: Exploring the Future, 29-30 September 2010.

## Considering Privacy in a Broader Ecology of Policy

In this discussion, an important caveat was raised by Bill Dutton. He noted that whilst most of the day's discussion had focused on privacy and data protection, there were other policy areas that impinge on privacy that might also be affected by the same technological scenarios under discussion. Freedom of expression is already being challenged by our use of social networks; and conversations between friends, which might have been ignored if spoken in a pub, have already resulted in a prosecution when they took place online[16]. Similarly, principles of fair use and copyright have already been brought into question by the conflict between digital rights management technologies and peer-production or file-sharing. Other relevant policy areas for future discussion might include public liability, competition policy, property rights and inheritance or employment policy. Protection of privacy must be balanced with the pursuit of other legal and regulatory rights and privileges. It is increasingly difficult to consider any single policy issue in isolation when all are being reshaped and balanced by a larger ecology of policies and regulations.[17]

## Changes to Occupational Practice

As well as considering challenges to existing regulatory frameworks, participants also considered how trends in data generation and collection might also affect professional practice and institutions, such as health or policing. In regards to the latter, some emerging research on criminalisation was highlighted[18] which argues that increasing electronic surveillance might be criminalising certain sorts of activities that could be better regulated in other ways. It was also suggested that the nature of certain sorts of work might be changing, again as an unintended effect of new technologies. For example, one participant argued that criminal investigations today make greater use of electronic prompts such as number-plate recognition and CCTV, and are less reliant on behavioural observation and personal judgment. It was also noted that privacy was often protected by sheer lack of resources—as with number plate recognition, where there is simply not enough manpower to act on all the information generated.

At the same time, it was noted that professional practices can also protect privacy even in the face of obvious benefits that could result from data-sharing. The example of the e-Diamond project[19] was highlighted, which potentially enabled the study of large sets of mammography images. However, because the images belonged to discrete health trusts, each with their own conceptions of ownership and responsibility for protecting their data, data sharing was significantly impeded. This is an example where the inflexibility of past professional practice and institutional bureaucracy can inhibit beneficial sharing of data. However, it also illustrates the more general tension between the provision of new and valued services conflicting with earlier interpretation, and appropriate application of principles protecting privacy. This is a key dilemma of the digital economy.

---

[16] See, for example, the case of Paul Chambers, who was convicted for sending a jokey message over Twitter, in which he threatened to bomb a Liverpool airport in his frustrations over snow closures. http://www.guardian.co.uk/law/2010/nov/22/twitter-joke-trial-paul-chambers-appeal

[17] William H. Dutton, Anna Dopatka, Michael Hills, Ginette Law, and Victoria Nash (2011), Freedom of Connection – Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet. Paris: UNESCO.

[18] See for example, L. Zedner, 'The Inescapable Insecurity of Security Technologies?' in Aas, K. F., et al. (eds), *Technologies of Insecurity: Surveillance and securitisation of everyday life* (Routledge 2008)

[19] http://www.ediamond.ox.ac.uk/

## Improving Privacy Practices

There are, of course, extensive guidelines and legislative frameworks that cover the collection and use of personal data in a variety of different contexts, such as health and medical care, social care, or crime and policing. But these frameworks can be inadequate when it comes to practitioners engaging with the public, as when a medical professional reveals personal information about a patient. Such problems arise in the digital arena as well as in face-to-face conversations. There are many examples of accidental data breaches, for example, when sensitive data is lost, or an insider breaches security protocols. Participants suggested that this should be a focus of the professional training process: perhaps there is a difference between a practitioner knowing in the abstract what confidentiality policies apply to the data they use and the techniques used in actually discussing this with their data subject, or indeed the sensitivity they then show in handling the data. This could perhaps be an increasingly important addition to training in many professions.

This discussion also highlighted the extent to which effective privacy policy requires integration of privacy standards and techniques at every stage of the process: product or service conceptualisation, product or service design, development of implementation and training practices, product or service training, and institutional operations. If data purposes were better specified at the design stage, people/organisations might be able to minimise the data collected. In this context, the importance of occupational observation and reflection was also noted; if we are to avoid the problems caused when disruptive technologies are unthinkingly absorbed into professional practice, there need to be more opportunities for both professionals and product or service designers to observe and reflect on what actually happened in the daily activities of a particular occupation.

## How Much Do We Value Our Privacy?

An alternative approach would be to make the exchange of data more explicit, and, in particular, to share some of the benefits gained, such as through advertising on social network sites. In practice this already happens—free services such as Facebook or Google are supported by targeted advertising, which relies upon the use of personal data. It's unclear to what extent consumers are aware of this tacit transaction, however, and there are few good models of transparent corporate behaviour. Quite apart from ethical questions (such as who should benefit from the use of people's data), finding ways of making these transactions more transparent and more symmetric—less unequal—would help consumers make a more informed decision about who gets access to their data.

Much of the preceding discussion assumes we understand how our data will be used and that our rational expectations of the ways in which technologies will affect our lives will be fulfilled. In practice this is often not the case. Research into the societal implications of new technologies has frequently revealed their unexpected consequences and the unpredictable emergence of new social practices.[20] Nor should we assume that concerns about privacy practice will be the same in all countries as privacy preferences and norms vary cross-nationally and culturally. For example, on social networking sites in the United States, such as Facebook, most people use their real names. In China, on QQ, nearly everyone uses a pseudonym. Several studies have also shown that our understanding and valuation of privacy is dependent on the context in which the information is exchanged.[21] We should not

[20] See for example, Dutton, W.H.D, (1999) Society On the Line: Information Politics in the Digital Age, Oxford: OUP.

[21] See for example H. Nissenbaum, (2009) Privacy in Context, Stanford University Press; or Adam Joinson, Ulf-Dietrich Reips, Tom Buchanan and Carina Paine Schofield (2010) Privacy, Trust, and

even take it for granted that we will continue to value personal data as highly in a world where it becomes increasingly easily and frequently exchanged, or remixed and re-used, potentially with significant personal or mutual benefit.

# III. Implications for Policy and Practice

Whilst the group did not recommend any specific changes to legislation, several issues were felt to be deserving of further attention by researchers and policy-makers:

- **Transparency:** whilst organisations, such the Information Commissioner's Office in the UK, are undertaking good work to empower citizens in accessing, interpreting and evaluating the data held about them, there is still a long way to go before this is a straightforward and worthwhile task. For example, we already have rights of disclosure such that we can request, for example, our credit record or a breakdown of our electricity usage, but this data is not always made available in a clear and easily usable form, and it is certainly very difficult to make any useful connections between the various sources of data held about ourselves.

- **Interpretation and enforcement of legislation:** even if the Data Protection Directive is left unchanged or improved in certain ways, a major problem will remain with its implementation. Data protection is enforced in many different ways across the EU, and this is problematic in an era in which data is so readily and easily moved across state boundaries.

- **Instilling privacy norms:** there might be ways of legislating to improve privacy norms, particularly within private companies. Should there be more specific mention of 'privacy by design' principles, for example, in the specification of data security requirements? Equally, regulation concerning other policy issues, but which could have a significant effect on privacy, (such as competition policy which may require the portability of data across SNS), should be drawn up in a way that encourages good privacy practice.

- **Professional ethics:** It was clear from the forum discussions that there are very different ethical codes, norms, and practices between disciplines and professions, such as between an anthropologist and a computer scientist, or between a medical professional and an engineer. These may be obvious to those with experience of working on multi-disciplinary projects, but they are not as well-understood as might be expected, because collaboration across disciplines is still relatively uncommon. Uncovering these differences and finding ways of working across them is essential if new technological designs, products or services are not to falter at the final stage of implementation and use.

- **Public value of privacy and its infringement:** there is an increasing body of research in this area, which is expanding our understanding both of how to measure public valuation of harm, and how privacy is interpreted and valued in different

---

Self-Disclosure Online. Human–Computer Interaction, Volume 25, Issue 1, pp. 1–24.
http://people.bath.ac.uk/aj266/pubs_pdf/joinson_et_al_HCI_final.pdf

contexts. This research should be a significant resource for policy-makers re-shaping regulation relating to privacy and data protection.

- **Authentication:** online identification and authentication is a long-running challenge that requires more sustained attention. Many services do not require detailed personal identification, but merely authentication or verification that the person can legitimately receive the relevant service. For instance, if a person has a library card, they should be able to borrow a book without revealing more personal information. More effective solutions around authentication could reduce some concerns over personal privacy, such as by mitigating the need to give out lots of sensitive personal data on a regular basis simply as a means of obtaining a service.

- **Human–computer interaction:** this well-respected research field was portrayed as delivering more for research than for policy and practice, but also as a field where more investment from and collaboration with industry could help design more 'sensitive' online communication and data-gathering tools.

- **Focus on users:** whilst policy forums such as this one are usually focused on identifying recommendations for high level policy-making, this was one topic where some participants felt that the real focus ought to be technology users. How can we better educate or empower users to enable them to take more ownership of their data? How can we encourage the development of more applications where the 'computation comes to the data' rather than the other way round?

- **Digital legacies:** as outlined above, there is a need to better understand the importance of the data we leave behind. It may have commercial value, but it also has emotional and personal or self-constituting value; and this exacerbates the complexity of how it should be treated: within the term of a service contract, beyond that but within our lifetimes, and after our death.

The number of issues that arose in our forum could cause some to pause before entering an area so fraught with uncertainties and countervailing tensions; indeed, regulatory uncertainty is itself a recognised inhibitor of innovation. However, this is hardly the time to surrender on these issues. New digital technologies are being developed rapidly across the globe in an economy increasingly interconnected electronically. Concerns over privacy will not, and should not, be a brake on the development of new digital products and services. On the contrary, it may be that those who have the most imaginative and effective approaches to the protection of privacy will win out in a global marketplace where privacy protection is a shared concern.[22] Likewise, it may be those nations and regions that develop the clearest and most effective legal and regulatory frameworks that are able to capture the value of the advancing digital economy. What is clear, is that these issues cannot be ignored.

[22] Dutta, S., Dutton, W. H. and Law, G. (2011), The New Internet World: A Global Perspective on Freedom of Expression, Privacy, Trust and Security Online: The Global Information Technology Report 2010-2011. New York: World Economic Forum, April. Available at SSRN: http://ssrn.com/abstract=1810005

# IV. Challenges Going Forward

Participants were asked to conclude by reflecting on the day's most interesting or challenging issues. Those reflections included the following:

- Better technological product or service design is possible if designers take more time to understand the core skills or practices involved in different professional settings. This should at least help to mitigate the unintended consequences when core skills (such as observation) are undermined by changes in technological practice (e.g. electronic surveillance or automatic recording).

- We may be observing the beginning of a divergence between the domains of information security and privacy. Some of the day's discussions appeared to show a fundamental difference between more optimistic privacy experts who believe that we can design more effective privacy-protecting devices, and more pessimistic security experts who were more likely to predict the failure of these systems. This may be due to increasingly sophisticated understandings of trust and trustworthiness in computing, but in any case, it reveals a fundamental difference of opinion between groups of people who most need to work together to protect privacy.

- The challenge of multi-disciplinary working and collaboration must be embraced, and in particular, there are several research areas in which more engagement between technologists and social scientists could enhance the design process: behavioural economics, for a different way of understanding human motivations and possible influences; social science studies of privacy attitudes, and in particular those that focus on children or young people who may (or may not) use products in different ways to older users; and management science for insights into how to institutionalise certain norms of privacy through training and management.

- The challenge of building privacy-respecting tools which are effectively invisible to the user, i.e. that respecting privacy simply becomes part of people's usual working routine.

- The complexities resulting from the emergence of an expanded ecology of actors in this new data-rich arena; we need a far more sophisticated understanding of the dynamics of data exchange, processing and control if we are to ensure that current data protection regimes are fit for purpose.

- The need to move away from focusing on a single issue, such as privacy, to considering it within a larger ecology of issues that are co-evolving in the digital age, such as freedom of expression. Multiple policy values are shaping the future of privacy.

- The need for more effective transparency practices—there has to be a better way of explaining to service or product users what personal data is being collected and how it will be used. Examples of best practice here would be very helpful.

- The promise of user-controlled computation devices which, by moving the application to the data rather than the other way round, would reduce the need to hand over personal data to third party organisations—this was widely regarded as very encouraging, but still at a very early stage.

# References

Communications Consumer Panel, (2011) *Online Personal Data: the Consumer Perspective* available at: http://www.communicationsconsumerpanel.org.uk/Online%20personal%20data%20final%20240511.pdf

Dutta, S., Dutton, W. H. and Law, G. (2011), *The New Internet World: A Global Perspective on Freedom of Expression, Privacy, Trust and Security Online: The Global Information Technology Report 2010-2011*. New York: World Economic Forum, April. Available at SSRN: http://ssrn.com/abstract=1810005

Dutton, W.H.D, (1999) *Society on the Line: Information Politics in the Digital Age*, Oxford: OUP

Dutton, W.H.D., Dopatka, A., Hills, M., Law, G. and Nash, V. (2011), *Freedom of Connection—Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet*. Paris: UNESCO.

Dutton, W. H. and Meadow, R. G. (1987), in Levitan, K. B. (ed.), 'A Tolerance for Surveillance: American Public Opinion Concerning Privacy and Civil Liberties,' *Government Infostructures,* Westport, CT: Greenwood Press, 147-70.

Information Commissioner's Office, (2008), *Privacy by Design*, available at: http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf

Information Commissioner's Office (2010), *The Privacy Dividend*, available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_dividend.pdf

Joinson, A., Ulf-Dietrich Reips, Tom Buchanan and Carina Paine Schofield (2010) 'Privacy, Trust, and Self-Disclosure Online', *Human-Computer Interaction*, Volume 25, Issue 1, pages 1 – 24. http://people.bath.ac.uk/aj266/pubs_pdf/joinson_et_al_HCI_final.pdf

Nissenbaum, H., (2009) *Privacy in Context*, Stanford University Press;

Zedner, L., (2008) 'The Inescapable Insecurity of Security Technologies?' in Aas, K. F., et al (eds), *Technologies of Insecurity: Surveillance and securitisation of everyday life* (Routledge)

Zittrain, J. (2008) *The Future of the Internet and How to Stop It*, Yale University Press.

# Forum Participants

Anne Adams, Open University

Bob Anderson, Horizon Digital Economy Research Centre, Nottingham University

Ralf Bendrath, European Parliament

Grant Blank, Oxford Internet Institute

Iain Bourne, UK Information Commissioner's Office

Alistair Bridge, Communications Consumer panel, OfCom

Ian Brown, Oxford Internet Institute

Lindsey Brown, Bristol University

Ray Corrigan, Open University

Bill Dutton, Oxford Internet Institute

Lilian Edwards, University of Strathclyde

Robert Ghanea-Hercock, BT

John Hand, EPSRC

Rae Harbird, UCL

Anthony House, Google

Marina Jirotka, Oxford eResearch Centre

Adam Joinson, University of Bath

Richard Jones, School of Law, University of Edinburgh

Andrew Martin, Computing Laboratory, University of Oxford

Derek McAuley, Horizon Digital Economy Research Centre, Nottingham University

Vicki Nash, Oxford Internet Institute

David Waterman, Oxford Internet Institute

Yorick Wilks, Oxford Internet Institute

Joss Wright, Oxford Internet Institute

**Is Augmented Reality Augmenting Privacy Invasion?**

Dr. Anne Adams, Institute of Educational Technology, Open University

[This proposition paper presents privacy reflections on the home office recent showcase on augmented reality for security and counter terrorism]

Although my past research has been within the field of security and privacy my recent developments and funding have been within the fields of mobile and ubiquitous technology, resources and elearning. More recently this has led me towards newer developments in Augmented Reality (AR) Virtual Reality and Social Worlds. However, through not directly researching into privacy and security issues I've found myself encountering groups that don't consider these issues in the same way as privacy advocates and interesting privacy and security dilemmas. Recently I have developed my privacy model into a template that is being used nationally by social workers in their confidentiality training. Most recently I was invited to propose discuss some security and privacy issues in a discussion panel co-ordinated by the home office.

In a panel on security and privacy at the recent Home Office showcase on Augmented Reality there were issues raised about the balance between the need for information sharing to ensure security against privacy and ethical concerns. One of the panel members who had been a police officer many years ago, argued that if the public were asked 'do you want secure lives or privacy' they would opt for security. It was highlighted, however, through discussions that not only should it not be a question of one or the other but that life is often not that simplistic. Augmented reality has the potential to complicate further these decision making processes as the degree of information overload and the increased likelihood of profiling with personal information increases.

Augmented reality was defined within the forum as way of supplementing the physical world with virtual data. This has tended to focus on mobile device applications involving location based software as well as tagging of objects and individuals. Within the security services this is starting to be merged with face recognition software, 3D modelling and crowd sourcing information extending the potential development for these systems (see fig 1)

**Profiling People and AR**

A futuristic projection of AR can be seen in fig 1. The reality isn't quite as frightening but has the potential to get there. A trial was given at this event of face recognition software used through a head mounted camera that could be merged with data bases on the person and real time display critical details about that person for operatives e.g. the police in the field. Other devices were presented that allowed for mapping software to be merged with helicopter images and tracking devices so that individuals could be effectively tracked and pursued as well as their activities monitored. The inclination was slightly more towards covert operations with regard to discussion of tracking systems although there was some discussion of how to reduce the likelihood of errors. The Demenzies accidental tube shooting was discussed as well as reducing the likelihood of this occurring again.

Fig 1 futuristic potential through face recognition to tag and merging profiles in AR [image on http://thenextweb.com/2009/06/23/augmented-reality-beginning-tourism/ ]

With regard to profiling members of the public there was a great sense that this had been felt to support police and security forces in their work. However, there was a growing sense that this was now guiding and driving policing rather than traditional observational techniques. It was noted anecdotally, by one of the participants that DMV look-ups are increasingly encouraging the police to guide their daily practices by the technology. Police are less likely to respond to suspicious behaviour and more likely to respond to a negative DMV result. It was noted that the Yorkshire ripper was caught because of a blue serge suit, highlighting the increased importance of police work being driven by observational techniques not information on systems.

The inherent privacy issues around profiling was felt to be uncertain by most of the participants. For example the National Policing Improvement Agency had recently been negotiating with various privacy advocate bodies how far down you could aggregate data towards the individual to keep it meaningful enough for it to be useful to those in security BUT maintain a reasonable element of anonymity to retain privacy. The answer was 12 people, if anyone else needs a magic privacy number.

**Use of Social Media & AR**

One approach that seemed to be growing in importance within the AR developments was the use of crowd sourcing systems. Many new systems have utilised social media and public engagement to allow the public through twitter, facebook etc. to comment, record and act on local events from disasters to social events. Social media allowed a quick response to the Tsunami disaster and allowed for aid to be collected and distributed in a far quicker way. This has led to many developments in the US supporting the use of social networking as a route to collecting larger quantities of data about an event. Fires in California were photographed, tagged and videod by

locals and information posted on a site which led to a public movement to change some public policies around health and safety in the region. It isn't surprising then that many companies are thinking of developing these systems to feed into security and crisis management organisations. Neighbourhood watch organisations could be mobilised to record and upload their findings to sites for quick response from the emergency services. Recording suspicious looking cars and people hanging around school gates was noted as one useful outcome. One worrying perspective in these developments is that no-one seems to be considering the validity of the information being collected and the potential for malicious attach. A group could decide to maliciously focus on one person or a group of people and continue to report on their activities, or any misdemeanours that they make. This is an odd perspective on privacy since it reviews the notion of the public as potentially invasive rather than the notion of 'big brother'. Added to this is the potential for vigilantism to use this information inappropriately, thus taking the law into their own hands.

**Use of Video, CCTV & AR**

The merging of video and geo-location data was being used within many systems. However, discussions around the privacy implications of these systems was limited. There was a discussion on CCTV cameras and the risks to privacy invasion through the increased quantity of this data collection. However, as noted by another participant, the quantity of this video data and its poor quality was increasingly making it too costly to search and poor as evidentiary material in court. The increased development of higher quality systems with automated searching techniques was touched upon. However, as noted by another participant the automated licence checking systems had produced so many responses that there were not enough police to stop the cars that the system had to regularly turned off. The limitations of the system and manpower were highlighted as the key privacy protection mechanisms in force within these services.

It is interesting to note as a final point that Logica are in the process of linking up all the courts systems which are currently siloed. Previously a criminal who was convicted in one part of country would go into another region and commit the same crime and his previous record would not be known by the courts. Many criminals made a habit of touring the country flitting between counties to remain under the authorities' radar. This could be an invaluable and necessary system but it also has potential privacy implications depending on access rights. The details of this were not discussed.

Finally discussions focused on the increasing importance of public opinion on privacy issues. A distinct flavour of media hype was proposed by the audience although discussions were promoted by myself on the varied nature of privacy and trust expectations which need to be considered when developing systems. This opinion was mirrored by several of the home office attendees who noted that this issues was one that was going to grow in importance. A keynote from Microsoft summarised that this was the one key issue in system development that we still are no nearer in solving whilst the problems surrounding are still increasing.

EUROPEAN COMMISSION – DG JFS

# NEW CHALLENGES TO DATA PROTECTION

## FINAL REPORT

## *Executive Summary*

## I. Aim of the Study

The purpose of the study was to identify the challenges for the protection of personal data produced by current social and technical phenomena such as the Internet, globalisation, the increasing ubiquity of personal data and personal data collection, the increasing power and capacity of computers and other data-processing devices, special new technologies such as RFID, biometrics, face-recognition, increased surveillance (and "dataveillance"); and increased uses of personal data for purposes for which they were not originally collected, in particular in relation to national security and the fight against organised crime and terrorism; and to produce a report containing a comparative analysis of the responses that different regulatory and non-regulatory systems (within the EU and outside it) offer to those challenges, and that provides guidance on whether the legal framework of the main EC Directive on data protection (Directive 95/46/EC) still provides appropriate protection or whether amendments should be considered in the light of best solutions identified.

The study covered the following countries and jurisdictions: the Czech Republic, Denmark, France, Germany, Greece and the UK; and outside Europe, the USA (Federal level, California and New Jersey), Australia, Hong Kong, India and Japan.

## II. The Challenges

The plunging cost of storing, transmitting and processing personal data means that little technological or economic incentive remains for system designers to minimise the collection of such data. "Web 2.0" technologies allow users to share (often sensitive) information about themselves and those around them to an unprecedented degree. Remotely-readable RFID tags are now often attached to consumer goods, while similar tags are included in many nations' passports and are also being used for road toll payment systems, public transport ticketing, library book management, and in new contactless payment cards such as MasterCard's "PayPass" and Visa's "Paywave". CCTV cameras are proliferating in urban areas and on roads, with automatic recognition of car number plates. Biometrics such as facial images and iris scans are increasingly used to identify individuals. All such information can moreover be transferred around the world at low cost, and duplicated across databases and portable computing devices. Anonymisation of data will be increasingly impossible to achieve. These technological developments will produce a "digital tsunami" of data about individuals, which are accessible for surveillance and marketing purposes, and can be used to exercise control over the individuals.

Ongoing increases in processing power allow more information to be extracted from this mass of data, using data mining algorithms to discern patterns of behaviour and create "profiles" that in turn affect how individuals are treated. Public concerns over terrorism have led governments to share and analyse data about individuals' travel, finances and communications. E-government systems, intended to improve public service provision while reducing overall costs, are often built around population-scale databases containing sensitive personal data on millions of citizens. These records are commonly interconnected, analysed and "mined" to achieve state goals, at the expense of democratic and data subject control. Increasingly, "the computer" takes decisions that "significantly affect" individuals, on the basis of dynamically-created algorithms that even the officials or staff implementing the decisions do not understand, and that data subjects are unable to challenge. Data protection is

not (just) about privacy: it is about countering these increasing threats to fundamental European values.

Effective data protection therefore now depends upon the robust application of principles such as purpose limitation and the minimisation of personal data collection during the design phase of information system engineering; and careful scrutiny of the proportionality of government and private-sector databases and surveillance programmes.

## III/IV. Fundamental Imperatives and Basic Approach

Any review of the EU data protection regime should start with explicit recognition of the need to meet the requirements of the ECHR and the Charter of Fundamental Rights, and of the constitutions of the Member States. Failure to do so will endanger core European constitutional values and violate general principles of EU law, and will threaten the acceptance of the supremacy (or primacy) of EC and EU law by the constitutional courts of several Member States. More specifically, the basic European data protection principles, rules and criteria are part of that fundamental human rights fabric, and have stood the test of time, even if they may need strengthening in some respects.

However, their specific application and enforcement has been much less successful, and the new technological developments threaten to make the application of the principles yet more difficult (although some new technologies can help in their application).

Data protection law in the EU (in all areas covered by the previous three pillars) can and should therefore continue to rest on the basic data protection principles and criteria set out in Directive 95/46/EC. The application of these broad standards needs to be clarified, but they themselves do not require major revision in order to meet the new challenges. On the contrary, they reflect European and national constitutional/human rights standards that need to be strongly re-affirmed.

## V. Recommendations (only)

The study identified the following issues as those which any review of the EU data protection regime should focus, and formulated the following recommendations on those issues (References in brackets are to the sections in Part V of the Final Report where these matters are discussed in detail):

- ✓ **The problematic exclusions of certain matters from the scope of the Directive** (V.2):

*(i) Former First and Third Pillar matters:*

Recommendation: The basic data protection principles, rules and criteria enshrined in the Directive must be applied "seamlessly" to activities in all the areas previously covered by the different pillars. This includes the application of the (limited) exceptions for the old third-pillar activities listed in Article 13 of the Directive. If the challenges are to be met, there will have to be greater harmonisation, or at least approximation, of data protection rules covering those activities in the EU, based on COE Recommendation R(87)15. Also crucial is full judicial protection in the national courts, and through the ECJ with data subjects having full standing (with the back-stop being the European Court of Human Rights).

*(i) Exceptions for purely personal processing and freedom of expression, in particular in relation to social networking sites and "blogging" on "Web 2.0":*

Recommendation: It should be possible to apply data protection rules more lightly to relatively trivial activities on the Internet. We believe that the best way to address this problem is to regulate services that ordinary users rely on, particularly social networking sites. Companies should be made to provide default settings for their sites and services and tools that are privacy-friendly: if the default settings fail to protect privacy and personal data, the site that chose those settings should carry the primary responsibility for this. This would leave open the possibility of adopting (or where they already exist, retaining) a tort [civil wrong or *faut*] regime under which individuals can be held liable for wrongful or unjustified public disclosure of private information or "intrusion" over the Internet.

✓ **The vexed question of "applicable law"** (V.3)

Recommendation: Better, clearer and unambiguous rules are desperately needed on applicable law. We would tentatively suggest rules on the following lines (see the full Final Report for *caveats* to these suggestions):

– *within the EU/EEA*, the rules should, in our opinion, simply be based on the "country of origin" principle, as originally intended. However, it is an essential prerequisite for this that there is greater harmonisation, or at least approximation at a high level, between the laws of the Member States (see below).

– *non-EU/EEA companies "established" in the EU/EEA* should be able to comply only with the law of their EU/EEA country of main establishment (their European HQ), and should otherwise be treated as EU/EEA companies.

– in relation to *non-EU/EEA companies not "established" in the EU/EEA but that use "means" in the EU/EEA* (typically, non-EU/EEA companies that offer products or services to EU/EEA citizens and companies over the Internet), the rules on "applicable law" should be simplified, so that they too can adhere to the law in one (relevant) EU/EEA country only. Consideration could be given to making this choice of law possible within such a company's Binding Corporate Rules; the appropriateness of the choice of law would be one of the issues to be assessed in judging the adequacy and appropriateness of the BCRs.

– *non-EU/EEA companies that are subject to an "adequate" law* in their country (as determined by the Commission) should be treated on a par with EU/EEA companies, i.e., they should only have to comply with their own ("adequate") law - provided the States concerned also comply with the measures taken in the EU/EEA to ensure ongoing harmonised/approximated application of the law.

✓ **The need for much greater harmonisation (at a high level) within the EU/EEA, through various means including stronger enforcement action by the Commission** (V.4)

Note: The study examined in some detail the differences in the laws of the Member States on important issues such as: **core concepts and definitions** (V.4.A(i)), the **data protection principles** (V.4.A(ii)) and –**criteria** (V.4.A(iii)); processing of **sensitive data** (V.4.A(iv)); the rules on **transborder data flows** (V.4.A(v)); and the **laws of non-EU/EEA States** in these respects (V.4.B). The findings are in Part V, section 4; the full details in Working Paper No. 2. The basic conclusion is that there remain major differences in all these respects.

Recommendations: We do not recommend that the Directive should be replaced by a Regulation or a new, more tightly-drafted Directive. Rather, we recommend that the WP29 be asked, in consultation with the Commission (which in any case serves as its Secretariat) to carry out more, and more in-depth, surveys of national law and practice, with a view to formulating "best practice" and suggested interpretations (which is basically what they do already), but with an added requirement that the Member States should report on the extent to which they comply (or feel they should not have to comply) with such suggestions. It would then be up to the Commission, if needs be, to test out whether the WP29 guidance is the one that, in law, should be followed by the Member States - with enforcement action being considered as a normal means of testing this if required. We believe that this would not require any amendment to the Directive. However, it would signal a major difference in the Commission approach to ensuring more harmonised transposition and implementation of the directives, with WP29 opinions effectively, in appropriate cases, enforced by the Commission (subject, of course, to the supervision of the ECJ).

As a very modest step in that direction, aimed at enabling such actions by both the WP29 and the Commission, we recommend that, at least, the views of the WP29, and the extent and manner in which they are reflected in national law and practice in the Member States, be made available in a more structured, comprehensive form, and that the attention of relevant administrative and judicial bodies at national and EU level be drawn to them.

- ✓ **The need for more cooperation with non-EU countries, and greater recognition of "adequate" non-EU efforts** (V.5)

Recommendation: The "adequacy" process has not (yet?) had the impact that it potentially could have and should be reviewed. Perhaps provisional rulings could be an answer. In any case, the other, less formal measures, such as technical assistance, close cooperation (including "twinning" of EU and non-EU DPAs), and other processes should continue and be strongly supported. In the meantime, it is important, at a political level, to reverse the process of Article 25 of the Directive losing its potential international impact.

- ✓ **the need to ensure much greater compliance with and much stronger enforcement of existing law, at the domestic level, by the DPAs** (V.6)

**Recommendations:** We recommend that there should be "prior checking" of population-scale information systems in the Member State, especially in the public sector - but (i) before they are cast in concrete (i.e., starting in the early planning stage) and (ii) by better (technically) qualified staff. It is notable that the Australian Government has recently proposed that the Privacy Commissioner in that country should be given the power to require government agencies to prepare Privacy Impact Assessments. In the private sector, a similar role could be fulfilled by Privacy Audits or (real and effective) Privacy Seals, strongly encouraged by public procurement rules giving competitive advantage to data protection-compliant products and services (as is already the case in Schleswig-Holstein in Germany) (see below). More generally, we feel that consideration could be given to moving enforcement largely away from the DPAs, to the courts and the prosecuting authorities.

- ✓ **The need to strengthen the rights and remedies for individuals (possibly acting with or through relevant NGOs)** (V.7)

Recommendations: The basic requirements that should be met in order to make the "judicial remedy" referred to in Article 22 truly effective should be discussed in the WP29, and guidance issued in this respect - and the Commission should take enforcement action if

these requirements are not met. A study should be commissioned to look into possible means of supporting individuals in this respect, e.g., by changing rules on litigation costs; by allowing non-governmental/civil society groups to support, or be formally involved in, proceedings by individuals, or to act on behalf of groups of data subjects; by providing for default, liquidated damages awards; or by adopting special systems such as the US "*qui tam*" procedure.

- ✓ **the need to further develop supplementary and alternative measures (while understanding the built-in limitations and practical restrictions of such measures)** (V.8)

Note: The study examined in some detail both the potential benefits and the limitations - and the often deceptive, or broken, promises - of **Privacy Enhancing Technologies (PETs)**, including encryption (as a means of ensuring compliance with at least data security requirements) and a related issue: security breach notification; de-identification; and others, such as P3P and online subject access systems; **Privacy-Friendly Identity Management**, including (now largely outdated) centralised systems, more recent "user-centric" ones, "vendor relationship management systems", and the use of identity cards for miscellaneous purposes; **Privacy by Design**, including the use of Privacy Impact Assessments; **User Privacy Controls and Default Settings**; **Sectoral Self and Co-Regulation**; and **Privacy Seals**. Here, it must suffice to note our overall conclusions.

Recommendation: Any view of complementary and alternative measures must be based on realistic and technically correct evaluations of such measures. They should not be dismissed out of hand. However, they will have to be closely scrutinised, by technical as well as legal experts.

It may be useful to consider the establishment of a special body or office of the EU/EEA DPAs, closely linked to the WP29 and the Commission, to deal with the European Privacy Seal, European codes of conduct, and Binding Corporate Rules, on a quasi-commercial (or at least fully self-financing) basis, in a way similar to the system in Schleswig-Holstein.

Overall, the question of incentives and economics of privacy and data security are central. If the law makes the protection of privacy economically attractive (e.g., through procurement incentives, coupled with the issuing of serious privacy seals), or punishes breaches of data protection and data security rules (by placing the onus for protection on those who are in the best position to ensure them, rather than by allowing them to shift the costs to others, such as consumers), then data protection can have a future. We believe that requires the right combination of law and self or co-regulatory rules and mechanisms. We hope the above gives some food for thought on these.

- o – O – o -

Core experts:
Prof. Douwe Korff (UK/Netherlands)
Dr. Ian Brown (UK)

Special experts:
Prof. Peter Blume (Denmark)
Prof. Graham Greenleaf (Australia)
Prof. Chris Hoofnagle (USA)
Prof. Lilian Mitrou (Greece)
Filip Pospíšil, Helena Svatošová,
& Marek Tichy (Czech Republic)

Advisors:
Prof. Ross Anderson (UK)
Caspar Bowden (UK/France)
Prof. Katrin Nyman-Metcalf (Estonia)
Paul Whitehouse (UK)

# A Framework for Ethics in ICT

**Marina Jirotka**
University of Oxford
Oxford eResearch Centre

**Bernd Stahl**
De Montfort University
Centre for Computing and Social Responsibility

Following our Digital Footprints Policy Forum
Oxford Internet Institute
17th February 2011

The current approach to ethics within ICT is not adequate for the landscape of twenty first century research. In many areas of research, investigators now receiving public money for ICT research are under increasing pressure to have greater and broader accountability, both to the funding bodies and to the public. There is also a growing awareness that increasingly powerful technologies are being developed which have the potential to reshape society. Thus, for example, in areas of *Information Management*, new sources of digital data, data linking and aggregation are bringing issues of privacy, ownership and intellectual property to the fore. Or advances in technology monitoring *Energy Consumption* such as smart grids highlight what may be identified about an individual's or family's location and lifestyle information.

Whilst developments in science and technology have always run ahead of our ability to think through their ethical implications, the rate of change is now accelerating. Some mechanism is needed to open up debate on such changes and their implications amongst the ICT community of researchers and practitioners, and to allow them to identify and address ethical problems early in the process.

Ethics has been recognised as an important aspect of ICT since the inception of computers (Wiener, 1954). Some of the early headline issues, such as privacy, ownership and access have been discussed for decades in various guises (Mason, 1986), and are set to resurface in more pressing ways over the next decade. At the same time, the use or deployment of different technologies and devices may raise different ethical issues, whilst new applications raise new questions. As a result, there has been much recent activity in identifying ethical issues related to ICT (Floridi, 2010; Himma & Tavani, 2008; van den Hoven & Weckert, 2008).

Further evidence of the increasing recognition of the importance of ethics in ICT is provided by international funding requirements (e.g. EU FP7), professional standards (e.g. BCS, ACM) and was confirmed during the recent EPSRC "ICT Research – The Next Decade" meeting. It is not always clear, however, how such work translates into the different strands of activity in the broad area covered by the EPSRC ICT portfolio.

The Digital Economy programme carries a particular burden in this respect. Not only will the services being developed strain our concepts of what is proper, acceptable and "safe" use of

technology, their investigation of these areas in support of the programme could well be subject to objection from an ethical or public policy standpoint.

This raises a very important and still unresolved question as to how much *duty of care* EPSRC should have toward its funded projects. For example, it may be argued that just as the MRC makes transparent its duty to researchers through the deployment of a clear ethical model, so too should EPSRC. As the remit of projects funded by EPSRC becomes broader to include such issues as, *personal identity* and *digital inheritance*, there is a very real possibility that the deployment of devices developed on such projects could lead to *social harm* and impact negatively on quality of life.

What is required is a mechanism that enables ICT researchers to focus on specific ethical issues and the array of models for representing and addressing them whilst also enabling EPSRC to reflect upon what duty of care it has towards the research community.

Most aspects of life are potentially affected by ethical consequences of ICT. The *relevance of ethics* in ICT research varies greatly. In some areas the implications may be immediately obvious, for example, computationally controlled medication, whereas in others they might appear to be remote for example, designs of algorithms or communications infrastructure. However, problems also arise in what is probably the majority of ICT research that sits between these two extremes.

Awareness of ethical issues is of crucial importance in a programme explicitly targeted at intervention in social and economic life. The fundamental concern in its mission to promote quality of life is complemented by concern with the research process itself; explicit engagement with ethical issues will contribute to the public's sense of appropriateness of the research funded and can provide greater and more informed policy support. For the researcher, ethical awareness can inform the social impact of the innovation, assist with user and public engagement and technology acceptance. It is crucial therefore, for the ICT community as well as funding bodies have an appropriate and common understanding of ethics in the changing landscape. Such an understanding is currently missing from the Digital Economy programme.

Limitations of current ICT ethics, especially with regard to the Digital Economy programme include:

- A divergence of different stakeholders' and ICT sub-communities' conceptions of "ethics" and its relevance or importance
- The widespread adoption of the model of biomedical ethics (Beauchamp & Childress, 2008). Two aspects of biomedical ethics that lead to difficulties in ICT research are:
  - The emphasis on the danger of *individual* harm to *research subjects* and
  - The aim of the research( e.g .providing greater access to information, improving sense of well- being) is assumed to be *prima facie* morally good and ethically justified.
- A concentration on the process of doing research and *lack of attention to the product*.
- A siloed approach that may consider issues in fundamental research whilst ignoring links to product development or product end of life.
- The perception of ethics as an external imposition that stifles freedom and innovation rather than an important resource on which research is based.

The issues of ethics in ICT in general cannot be "solved" in the way technical problems can be solved. They require constant deliberation and controversial discussion. Ethics is dynamic

and context dependent, which means that new technologies and social developments may change that which is perceived to be ethical. Ethical debates may rarely lead to general consensus and often include incompatible positions. What is needed is therefore not only a snapshot of current views of ethics of the ICT community but a mechanism that will allow informed debate and the contextualisation of different views and positions.

Requirements of a novel understanding of ethics in ICT and especially the Digital Economy that may overcome these limitations and give the ICT research community the conceptual clarity and practical relevance it requires are:

- It should be rooted in and incorporate the understanding and life-world of ICT researchers and allow them to relate their observations and concerns.
- It should incorporate an array of models representing concerns across the portfolio of ICT research.
- It needs to lend itself to proactive, effective and flexible processes that can be embedded into ICT research projects.
- It should be concerned with identifying potential social harm from product deployment and use.
- It should provide the possibility for a more end-to-end approach where issues identified in fundamental research will have mechanisms to link to related issues further downstream in the lifecycle of the product.
- It should facilitate informed debate and reflection to contextualise differing views and should encourage participation from the public.

.

# *I can't tell you, it's "Data Protection"*

Rae Harbird
Department of Computer Science
UCL
Email: r.harbird@cs.ucl.ac.uk

## *Introduction*

I am a Computer Scientist working at UCL and I have been thinking about the implications of electronically stored information and data protection since I studied as an undergraduate in the mid-1980s. Recently, I have worked on the privacy implications and risks of information sharing in the field of child protection. At the moment I work in a team specialising in what is known as pervasive computing, a term which refers to a vision of the world in which small, networked devices are seamlessly embedded in our environment and which collaborate without our conscious intervention and knowing. Our research projects include the development (and deployment) of applications for the monitoring and measurement of athlete performance and Unmanned Aerial Vehicles in search and rescue missions. The leap from research to commercial product is not too great in these instances and Prof. Stephen Hailes, who leads the team, believes that we must remain vigilant of the privacy implications [1]:

> *"My feelings are that pervasive computing technologies potentially allow a level of intrusion into the lives of individuals far greater than ever before possible. Moreover, such devices are purposely built to be invisible, and are designed so as to be sufficiently cheap that they can pervade many aspects of our lives. The design aims make the technology extremely useful - it is capable of providing assistance in many areas of our lives and the non-networked versions already do; in particular it is capable of adapting to our needs as a consequence of the information we supply it with or that it can learn. Consequently, precisely the same attributes that make the technology useful also make it potentially rather dangerous if left completely uncontrolled."*

It is not necessarily useful to single out a technology, or group of technologies, which will specifically threaten the privacy of an individual in some future world. The key factors, I believe, which are shaping today's market for data and information are:

- The ever-increasing range and quantity of data that it is possible to collect about individuals.
- The ever-decreasing cost of obtaining, storing, transferring and analysing that data.
- The increasing profit or advantage to be gained, in either a legal context or an illegal context, from exploiting the personal information gathered.

This leaves us with the question of how to address the moral and ethical issues arising from the digital collection, storage, analysis and distribution of personally identifiable information. The answer will vary according to the circumstances and there are many, many situations in which the solutions to privacy-related dilemmas are not clear-cut. Perhaps this is best illustrated by using a couple of scenarios to illustrate some of difficulties arising when large amounts of personal information are processed and handled. The scenarios in this paper have been chosen, firstly, because they present interesting issues that have yet to be resolved, and secondly because the privacy implications of each has been discussed in more detail in recent research work to which the reader is referred. The scenarios also share another important characteristic; the moral and ethical issues presented existed before the advent of digital media (when information was recorded on paper and then stored in files) but the use of digital technologies has multiplied the difficulties in scale and complexity.

## *Athletics Coaching and Training*

New technologies are increasingly used to measure an athlete's performance at a level of detail not possible before. This is coupled with information about training, coaching guidance, trials and event performance as part of the daily work practices for coaches and athletes. Here are some examples illustrating how such technologies are used:

- High quality video is used to collect detailed information about limb movements.
- On-body sensors can be used for a variety of purposes including the collection of data on stride length and foot contact times over the length of a run, the athlete's heart rate and body temperature.
- Sensors embedded in the environment can be used to collect data for the duration of a sprint and variations in speed over the length of track traversed.

Amongst other things, this data can be used in conjunction with information about coaching techniques and the coaching programme in general to chart progress over time, make comparisons with other performances (by the athlete or by peers) and to evaluate coaching techniques. As one might expect, the livelihood and career progression of both an athlete and a coach is increasingly dependent upon such data and the analyses performed on it. Nevertheless, the ownership and control of this type of information is unclear and it is unlikely that either party will have thought about the implications. Some key considerations are: who may make decisions about persons or organisations with whom the information may be shared, and under what circumstances might it be shared? What should happen if the relationship between the coach and the athlete breaks down? In light of likely increase in repositories of such information it would seem that such issues should be considered with by the governing bodies responsible for conduct and ethics. The enabling technologies and the privacy implications of their use are explored in more detail in [2].

## *Provision of Services for Vulnerable Families*

Citizens wishing to access services from local government in the UK, such as those provided by social services, must provide consent for information to be recorded and shared with other departments. Indeed, in recent years, the government has actively encouraged information sharing as part of a multi-agency approach to service provision. It goes without saying that some of this information may be extremely sensitive in nature and will relate to vulnerable children and adults. Agencies within a geographic area generally draw up and ratify data sharing agreements covering what may be recorded, when and how consent should be obtained from subjects, when and how the information may be shared (with other agencies) and how to manage the lifecycle of data in a responsible manner, ensuring that it is archived or destroyed when it has served the purpose it was intended to fulfil. Data sharing agreements and related guidance for both the users and providers of services are often made publicly available on websites as a demonstration of good practice in the guardianship of the personal information. Despite the plethora of information available, we know that practitioners find it very difficult to interpret such guidance in a context-sensitive way and often make mistakes [3]. As one might expect this can lead to information being shared inappropriately but there have also been examples where information has not been shared when it was necessary to do so. The effects of not sharing information can be equally detrimental and may place vulnerable citizens at considerable risk.

Following the Laming enquiry in 2003, the UK government launched the development of ContactPoint, a large-scale national database destined to contain information about all children and young people, about 11 million entries. The aim was to assist professionals, enabling them to see what other agencies were working with a particular child or young person. Many security concerns were

voiced about ContactPoint and in 2010 it was scrapped as part of what the coalition government announced as "a full programme of measures to reverse the substantial erosion of civil liberties under the Labour Government and roll back state intrusion." Privacy and security issues surrounding such large-scale databases in the health services and social care have been debated for well over a decade and it is understood that, fundamentally, the way we design information systems has an impact upon the level of privacy and security afforded to the person-related information stored within it. This has been borne out on many occasions as information systems have contributed towards the violations of people's privacy. In particular, the centralised storage of information is likely to cause the breakdown of privacy and confidentiality as the subversion of security mechanisms by humans is so much easier where large amounts of data are managed in one place. The government's commitment to "rolling back state intrusion", appears to be selective and it is still going ahead with plans to implement a centralised database containing the initial assessment forms to be used by local agencies working with children. It is worth noting that privacy and security issues are complex and shortcomings cannot be addressed by the simple application of security mechanisms such as strong encryption or the installation of firewalls.

## *Discussion*

The scenarios elaborated above have demonstrated how the use of digital technologies worsens the privacy and security issues in situations where personal information is recorded and analysed. To counter this we must adopt practices so that privacy and security related goals are considered, from the outset, of any systems acquisition or development project. This can be achieved by using a privacy-by-design approach to systems engineering [4]. We must also remember that information systems do not exist in isolation and must be supported by organisational practices which reinforce the privacy and security objectives of the system. Finally, we must recognise that human beings find it difficult to make context-dependent, dynamic decisions about collecting, sharing and managing personal information and we should investigate how computer-based tools can assist people in assessing the risk to data subjects at the point in time when information is collected, shared or otherwise processed.

## *References*


1. Enterprise Privacy Group, "Privacy by design: an overview of privacy enhancing technologies", Information Commissioner's Office, UK, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, 11 (2008)
2. Kerwin, D. G., Fleming, S., Kuntze, G. et al. "Ownership and control of athlete training and performance data: it's time for decisions", submitted to Journal of Sports Sciences. (2010)
3. Harbird, R., Ahmed, M. O., Finkelstein, A. et al. "Privacy Impact Assessment with PRAIS", Proceedings of the 8th Privacy Enhancing Technologies Symposium. (2008)
4. Marsh, S., Brown, I. and Khaki, F. "Privacy Engineering. Cybersecurity Knowledge Transfer Network white paper.", (2008)

**Digital Footprints**
Position paper from Yorick Wilks for OII (16 February) meeting

*"And some there be, which have no memorial; who are perished, as though they had never been; and are become as though they had never been born." Ecclesiastes 44:9*

Ecclesiastes is my personal favourite for epigraphic quotes for articles: in this case, one sees how much less likely the condition described by the prophet is as time goes on. Facebook (FB) now has half a billion friends, and all of them will be dead some day but will almost certainly have some memorial, however thin in texture. FB is now devoting a lot of resources to assessing how much storage and access to give to the sites of the Facebook dead, as they continue to grow in number and possibly as a proportion of all its users.

My own interest in the issues of personal data flows from a large EC project called Companions, now finished but which I am extending to other areas. The original idea was a conversational system intended eventually interacts with a user over a long period, providing agreeable company while eliciting life information by conversation, but also seeking for user-related information in open web sources such as FB. The project's longer-term goal is to build up an intelligent structured life narrative for the user, something far more perspicuous and organized than a FB site, and one over which the user would have control , so that they could present themselves to others, possibly , their survivors, in a way they would wish. The Companion has been planned as a gleaner of data from open sites like FB and from the user's own holdings of documents and images (eg on iPhoto or Flickr). However, since some of the planned applications will be health-related, there is no reason why this user-based data hoard should not ultimately incorporate health information—certainly in countries (like Spain) where everyone has access to their own health information.

This is a more optimistic approach to personal data---avoiding the Ecclesiastes fate----and assumes dealing essentially with data under the subject's control and largely originated by them. This is the opposite way round from the focus of much public discussion, particularly in the UK where public and private organizations are almost certainly more intrusive than elsewhere, and where as a consequnce much public opinion is either negative or at least ambivalent.

Data Protection legislation is not my area of expertise any more than is the Freedom of Information Act. However, I do have informed beliefs about the state of these matters in this country, and I believe a great deal of reform and clarification are needed—that we cannot go on as we are—and that we need to move to a situation where individuals have and feel far more control over their own life data

than they do now. This is the paradigm we need to move to and we should be seeking legislative means to achieve it as rapidly as possible.

There are contradictions in the current UK situation, known to all intelligent observers, and way beyond the closed circle of experts. On the one hand: one is not allowed to publish the names of, say, one's cricket club on the web without registering one's intention; one cannot publish on a board the names and marks of one's students and, according to an OII speaker last year, one may not be able to publish a remark about someone's health, lest that imply access to privileged health information.

My point here is not so much to question these strong constraints on free speech and the right to publish (which would be intolerable in the US where only health information is at all protected) but to remark on the obvious contradiction between those constraints and the freedom of access of companies and the state to electronic transactions of all kinds. It is pretty much common knowledge that the UK State processes a substantial percentage of our emails and phone records at GCHQ as and when it chooses without need of magistrates, even though a journalist at the NoW has no such protected privilege. Police officers with whom I have worked told me that one third of the men in South Yorkshire between 18 and 50 are in the police computer, though the public seem unaware of this.

The contradiction is obvious, as is the ambivalence of the UK public, the most surveilled population in Western Europe: we may not approve of numberplate-reading police cameras on major bridges and more CCTV cameras than in the rest of Europe put together, but when an awaful murder occurs, we take some comfort in these records, and the traces of phone calls and credit cards transactions, and may even express regret that we, unlike Australians, are still able to buy the unregistered pay-as-you-go phones the IRA uses.

In the UK we suffer a radical contradiction in our attitudes to the public/commercial and private use of data: one that is not so clear in Germany, on the one hand , with its strong restrictions on all state access to data, and in the US, on the other, with its lack of constraints on access to data public and private. I believe the UK should move one way or the other, and my instincts tell me the US does a better job overall better than we do. Data should not be sacrosanct and we should scrap the Data Protection Act in its current form and simultaneously reform our absurd libel laws when use is made of such data (and many already agree on that point). However, there are overall regimes we could create different from both the German and US systems, and which remove the contradictions we currently suffer.

Some principles for moving to a more liberal approach to data and to ward off the incipient fascism that many see as a possibility in the UK, are as follows:

- if our data is open to the State and to Corporations so should it be for individuals to use as they chose—preferential access and exploitation must go.
- The key principle must be an individuals control of his/her data, both for their own purpose, like their own legacy and the right to know what is held on them, way beyond current access to Credit agencies, but at least to the Spanish system of access to our own state records.
- Eric Birch (2000) was the first writer I encountered who had a clear view on how an individual could combat state and corporate identification of individuals.

Abbie Hoffman , the head of the Yippie movement, was sensitive to these issues in the 1960's and his advice then (to Americans) was to give a different Social security number every time one was asked. But that device, though fun, cannot survive in the age of giant data processing and instant access to identity banks base on such numbers. Birch's suggestion is complex, but the essence is that we should move to a system where reveal as little or as much of out identity as we choose at each transaction so that so giant global data footprint outside our control can be assembled, where by state or corporate actors. Such a concept is perfectly consistent with the UK legal concept of identity, where one may still legally use any name one likes, as long as no fraud is intended.

The difficulties with this are in the details and how we minimise inevitable loss of information for criminal detection. There are many technical devices that could be more widely used than they are including proxy IPs to shield our computers from data gathering and linking of data. Tim Berners Lee said recently that soon anonymity in computer transactions will be impossible because of the ancilliary information available from which our identity can be inferred even if we are able to shield it explicitly. A key necessity will be payment mechanisms that are web-usable but as anonymous and reliable as cash: wider use of payments through anonymous digital phones would be an obvious start. There are many technical details and possibilities—to which may mean the use of trusted agents (what I would term Companion agents) to act for us at commercial and government portals—trusted both by the user and the provider-- what is needed above all is the will to move to such a system if enough of the population find the current situation (and its likely developments) intolerable.

Birch, D. (2000) *Digital Passports* (Parliamentary IT Briefing): IT and Public Policy.

Wilks, Y. (2010) (ed.*) Artificial Companions in Society: scientific, economic, psychological and philosophical perspectives*. John Benjamins: Amsterdam.