Is Big Brother watching you – and who is watching Big Brother?

December 2008

In strategic partnership with the King Baudouin Foundation and the Compagnia di San Paolo

Nicolas Beger
Damian Chalmers
Joana Cruz
Jacki Davis
Edouard de Tinguy
Robert Dover
Marie-Hélène Fandel
James Forster
Jonas Hartelius
Peter Hustinx

Natalie La Balme
Hans Martens
Björn Muller-Wille
Jim Murray
Caroline Persson
Alexander Schellong
Jo Shaw
Aidan White
Kay Withers
Fabian Zuleeg
Is Big Brother watching you – and who is watching Big Brother?

Nicolas Beger
Damian Chalmers
Joana Cruz
Jacki Davis
Edouard de Tinguy
Robert Dover
Marie-Héléne Fandel
James Forster
Jonas Hartelius
Peter Hustinx

Natalie La Balme
Hans Martens
Björn Muller-Wille
Jim Murray
Caroline Persson
Alexander Schellong
Jo Shaw
Aidan White
Kay Withers
Fabian Zuleeg

Articles in this publication represent the views of the authors and not necessarily those of the EPC.

December 2008

ISSN-1783-2462
# Table of contents

About the authors 4

Foreword 6
by Jacki Davis

## I. THE CHANGING LANDSCAPE

United in diversity? 9
by Natalie La Balme and Edouard de Tinguy

Power to the people? The implications of the social network revolution 16
by Kay Withers

Can Big Brother distinguish fellow citizens from aliens? 22
by Jo Shaw

## II. WHO IS ‘BIG BROTHER'? THE DRIVERS FOR INCREASED SURVEILLANCE AT NATIONAL AND EU LEVEL

The surveillance society: trends and implications for data protection 28
by Peter J. Hustinx

Restraining Big Brother’s ‘courtiers’ – the need for a bill of rights 34
by Jonas Hartelius

A worthwhile sacrifice? Trading privacy for better public services 41
by Fabian Zuleeg

eGovernment: data growth and growing concerns 48
by Alexander Schellong

Thank you for sharing your data 56
by Marie-Hélène Fandel and Joana Cruz
Big Brother in practice?
Passenger information: the new growth industry
by James Forster
The telecoms sector and the Data Retention Directive
by Caroline Persson

Journalists under pressure in security-conscious Europe
by Aidan White

III. WHERE DO WE GO FROM HERE? THE IMPLICATIONS FOR FUTURE POLICY-MAKING

Warm words and cold acts: the future of policing and judicial cooperation
by Damian Chalmers

The use of intelligence data by European agencies – misplaced concerns?
by Björn Muller-Wille

The securitisation of EU policies: trends and comparisons
by Robert Dover

Protecting the right to privacy: why the EU must stand by its principles
by Jim Murray

Keeping the Internal Market together in the knowledge economy
by Hans Martens

Constructing a Europe of asylum in a securitised world
by Nicolas Beger
About the authors

Nicolas Beger is Director of Amnesty International’s EU Office.

Damian Chalmers is Head of the European Institute at the London School of Economics.

Joana Cruz is a former Programme Assistant at the European Policy Centre.

Jacki Davis is Communications Director at the European Policy Centre and Editor of Challenge Europe.

Edouard de Tinguy is Programme Associate in the Paris office of the German Marshall Fund of the United States.

Robert Dover is a Lecturer in International Relations in the Department of Politics, International Relations and European Studies (PIRES) at Loughborough University.

Marie-Hélène Fandel is a Policy Analyst at the European Policy Centre.

James Forster is Manager Facilitation, Government and Industry Affairs, British Airways plc.

Jonas Hartelius is Senior Fellow at the EastWest Institute in Brussels and Scientific Adviser at the Swedish Carnegie Institute, Stockholm.

Peter J. Hustinx is the European Data Protection Supervisor.

Natalie La Balme is Programme Officer in the Paris office of the German Marshall Fund of the United States.

Hans Martens is the Chief Executive of the European Policy Centre.

Björn Muller-Wille is Senior Lecturer in the Department of Defence and International Affairs at the Royal Military Academy of Sandhurst.

Jim Murray was formerly Director of BEUC and President of the Transatlantic Consumer Dialogue (TACD).

Caroline Persson is a European Policy Adviser at BT.
Alexander Schellong is Senior Consultant at CSC’s Management Consulting Division and Research Fellow with Harvard University’s Program on Networked Governance.

Jo Shaw holds the Salvesen Chair of European Institutions and is Co-Director of the Europa Institute in the School of Law at the University of Edinburgh.

Aidan White is General Secretary of the International Federation of Journalists.

Kay Withers is Deputy Director, Media Standards Trust and a former Research Fellow in the Strategic Research Team at the Institute for Public Policy Research (IPPR).

Fabian Zuleeg is a Senior Policy Analyst at the European Policy Centre.
Foreword

by Jacki Davis

Hardly a day goes by without reports in the media about some new facet of what many regard as Europe’s emerging ‘Big Brother’ society, amid fears that we are moving towards realising the terrifying vision set out in George Orwell’s famous novel Nineteen Eighty-Four of an all-knowing, all-seeing government which uses pervasive and constant surveillance of the populace to exercise total control over its citizens.

Yet more CCTV cameras being installed in our streets, shopping centres and even parks; reports of companies using information gleaned from social networks such as Facebook to make ‘hiring and firing’ decisions; new rules on retaining mobile phone or airline reservation data… all these stories and more are fuelling concerns that we risk “sleepwalking into a surveillance society”, as the UK government’s Information Commissioner Richard Thomas put it in 2006.

Whether such fears are justified or not, one thing is certain: our movements and behaviour are being tracked and recorded on an unprecedented scale. Vast amounts of information about individuals are being collected and stored – not only by governments but also by the private sector – and that data is being used in numerous different ways, some which we have agreed to but also others of which we are almost certainly unaware.

Added to this are concerns about data which is collected for one purpose being used for another in today’s digitalised world, where sharing information has become easier than ever; fears that incorrect personal information is being stored and used without people’s knowledge; and growing alarm over reports of the personal data of millions of citizens stored on CDs being lost by careless civil servants.

The steady increase in the amount of data on individuals being collected, stored and shared is being driven by many factors.

The most obvious of these is the increased concern about security sparked, initially, by the 9/11 attacks on the United States and the subsequent ‘war on terror’. This has prompted an intense debate about how to strike the right balance between protecting Europe’s citizens from attack and protecting their civil liberties, and concerns that politicians are using the terrorism
threat to stifle debate on the gradual erosion of people's privacy. But there are many others which often go unremarked.

First, there is the simple fact that advances in technology are making all this possible: in today's digitalised world, it is far easier to collect and store massive amounts of data about individuals and use it in ways which would have been unimaginable a decade ago.

Then there are the changing attitudes towards data among the general public – particularly among the younger generation, many of whom are happily sharing sensitive personal information with each other on social networks like Facebook, even though they may have concerns about how much information governments and official bodies have about them.

Above all, there is the increasing value of such data to governments seeking to plan and provide public services more effectively; and to companies striving to gain a competitive edge over rivals by tailoring their goods and services to meet their existing and potential customers' needs. In today's increasingly knowledge-based economy, personal data is clearly becoming an ever-more important and valuable commodity.

While many of the issues all this raises are a matter for national governments, the EU is playing a growing role in this area. This is not only because Member States are increasingly coordinating their responses to security challenges and, for example, sharing vital information about suspected terrorists or criminals. It also reflects the fact that, in the EU's Single Market, the issues raised by the collection and use of data by companies operating across borders cannot be dealt with by one country alone.

As this issue has moved higher up the policy agenda, it has prompted an intensifying debate about whether individual Member States and the Union as a whole are striking the right balance between protecting citizens and respecting their civil liberties, between using such data for the benefit of individuals and society and respecting people's fundamental right to privacy.

Eurobarometer polls highlight the EU's dilemma: they suggest that the public believes that the Union does have a key role to play in the fight against terrorism and crime but, given that it has very limited powers in this area, it also risks being accused of ignoring the growing unease about the amount of information being kept about us and the risk that this data will be misused.
Many of these issues surface regularly in European Policy Centre debates under the auspices of our three flagship programmes: EU Integration and Citizenship, Europe’s Political Economy and Europe in the World. But this is a cross-cutting issue which is affecting an increasing number of policy areas.

This issue of *Challenge Europe* aims to contribute to the debate over how to strike the right balance, with articles by many leading experts in this field.

It starts by considering how attitudes towards privacy, the balance between security and civil liberties, and the concept of ‘citizenship’ are changing. It then analyses the factors driving the steady increase in the amount of data on individuals being collected, stored – and shared – by both governments and the private sector, and examines the implications of all this for individual citizens, businesses and governments. Finally, it assesses what impact all this is having now – and might have in future – on policy-making at national and EU level.

Two striking conclusions emerge from this collection of essays. Firstly, the debate about Europe’s emerging ‘Big Brother’ society is much more complex than it may at first appear, given the need to weigh up the benefits of these developments for our societies against the dangers they pose to our fundamental values and rights.

Secondly, that there is a need for much wider public debate on these issues, given that many people are unaware of some of the uses all this information is being put to. This publication aims to make a modest contribution to that debate.

Jacki Davis is Communications Director at the European Policy Centre and Editor of *Challenge Europe*. 
I. THE CHANGING LANDSCAPE

United in diversity?

The terrorist attacks on the United States in September 2001 have led to new anti-terror legislation, tougher penalties for terrorist crimes and increased surveillance powers. This essay compares public attitudes across Europe to giving up some civil liberties as the ‘price’ for greater security, and considers what impact this might have on policy-making at the EU level.

by Natalie La Balme and Edouard de Tinguy

After September 11 2001, international cooperation in the field of intelligence, justice and law-enforcement intensified considerably. The fight against international terrorism, and the wish to “never again have another September 11th”, led to new anti-terror legislation, tougher penalties for terrorist crimes and enhanced surveillance powers. Inevitably, this soon raised the challenge of determining how to maintain the right balance between security and civil liberties, between the imperatives of protecting open societies while maintaining their transparency and freedoms.

Proponents of increased security measures claim that these measures are crucial to protect civilians against international terrorism. Critics, on the other hand, point out that some of these measures imperil basic civil liberties, including the right to privacy – the basic foundations of democratic societies.

How does the European public position itself within this debate and influence the decision-making process in this field?

Before trying to answer this question, let us start with a word of caution. In spite of the vast research on the concept, the definition of ‘public opinion’ remains controversial. The difficulty of defining public opinion, as an object of empirical study, is perhaps still best expressed by V.O. Key: “To speak with precision of public opinion is a task not unlike coming to grips with the Holy Ghost”.1

The task of describing a ‘European public opinion’ is even more challenging. Hence, it is important to stress that, while we can talk of a European public opinion, this often hides wide differences amongst the public in the different European countries.
In fact, it seems clear that approaches to the issue of security versus civil liberties differ substantially from country to country and the responses vary, most probably according to different historical experiences but also to different perceptions of the threat of terrorism.

Indeed, public attitudes towards this issue seem closely correlated with attitudes towards – and the perceptions of – the threat of terrorism. In order to determine what the European public’s attitudes are and how they constrain, or not, the decision-making process, we will first look at how Europeans have perceived the threat of terrorism since 9/11 and how this perception has evolved. We will then address the issue of how citizens of different European countries value civil liberties, in order to conclude on whether or not potential divergences make it difficult for this issue to be efficiently dealt with at the EU level.

**Perceptions of the threat of terrorism**

In the aftermath of 9/11, Europeans were clearly concerned about what were often called the “new security threats”, notably international terrorism. When asked to evaluate a list of possible threats to their countries’ vital interest over the next ten years, more Europeans identified international terrorism as an “extremely important” threat in 2002 than any other issue mentioned (such as Iraq developing weapons of mass destruction, Islamic fundamentalism, or immigration).

Perceptions of the extent of this threat, however, varied in the different countries. The British felt the most threatened (74% regarded it as an extremely important threat) and the Dutch were the least worried (with only 54% regarding it as extremely important).

This perception of the threat of terrorism has varied from year to year and country to country, but has remained at a high level. In 2006, 66% of Europeans still considered it an extremely important threat (at the high end, 77% of the Portuguese and, at the lower end, 55% of the French). Recently, though, this concern has slightly declined. Those who felt they would be very likely to be personally affected by international terrorism declined by 10 percentage points in France between 2007 and 2008, 13 percentage points in Germany and eight percentage points in the Netherlands.

In terms of addressing the threat of terrorism, the public feels that the EU is better placed to take decisions on this issue than national governments.
Indeed, 79% consider that fighting terrorism – and other global issues such as protecting the environment (71%) or fostering scientific and technological research (70%) – is better taken care of at the EU level.\(^5\)

In fact, most Europeans often tend to have significantly more confidence in the EU than in their national institutions: half say that they trust the Union, compared to around a third who have confidence in their national parliament (34%) or their national government (32%).\(^6\)

Hence, EU citizens generally support the establishment of an Area of Freedom, Security and Justice in the Union, even if most of them consider the policy details somewhat abstract.\(^7\)

**Towards an Orwellian society?**

In December 2006, 64% of the European public agreed that “we need more equality and justice even if it means less freedom for the individual”.\(^8\) But looking more in depth, significant and interesting differences appear, notably with respect to generations and levels of education.

Age is clearly a discriminating factor, with 69% of respondents aged 55 and above agreeing with this statement compared with only 55% of those aged between 15 and 24 – a 14 point difference. Among those aged between 25 and 59, 62% agreed with this proposition.

Does this mean that, in future, a lower percentage of citizens will accept giving up freedom in the name of equality and justice? It is difficult to say, as several dimensions must be taken into account.

First, as we saw, perceptions on this issue seem closely correlated to perceptions of threat and, notably, the threat of terrorism. A terrorist attack such as 9/11 or the events in London and Madrid could easily shift opinions. It is also difficult to tell whether there is a generational issue at play, with people generally more willing to give up some freedom for more security as they get older.

Education is also an important factor. This survey showed that the lowest agreement rate is among students (55%) and the highest among those who left school aged 15 or younger (68%) and among 16- to 19-year-olds (67%). Among those who left college in their 20s, only 58% agreed that we need more equality and justice even if this means less freedom for the individual.
Hence, the higher the level of education, the less in favour people are of reducing freedom.

It is interesting to note, however, that political affiliation does not impact on the level of support for more or less equality and justice; nor does the overall opinion of the EU. Indeed, whether people tend to trust the EU or not – or indeed have a positive, neutral or negative image of the Union – does not tend to have an impact on their responses. However, knowledge about the EU does: the more people know about the EU, the more reluctant they may be to allow more equality and justice if it means less individual freedom. This survey also revealed considerable differences between Member States, with level of agreement ranging from 46% in the Netherlands to 80% in Portugal.

Education and age remain a determining factor in most of these countries, as shown by the Dutch results: 36% of 15- to 24-year-olds agreed with this statement compared with 61% of those aged over 55.

Beyond the question of equality and justice versus liberty, it is interesting to delve a little deeper and see whether the public is in favour of giving governments greater authority to monitor certain aspects of their daily lives.

In 2006, the German Marshall Fund Transatlantic Trends survey asked whether, as part of the effort to prevent terrorism, the public was in favour of greater government authority to install surveillance cameras in public places, and monitor communications on the Internet, banking transactions and citizens’ telephone calls. The overall results show that 78% of the public favoured surveillance cameras in public places, 54% the monitoring of communications on the Internet, 50% monitoring banking transactions and 39% monitoring citizens’ telephone calls.

Yet, and again by looking more closely at the results, the following differences appear clearly.

Installing surveillance cameras in public places is not generally controversial. Majorities in all the countries tended to agree with this, albeit with varying levels of support (France 72%, the Netherlands 86%, the UK 84%, Romania 67% and Portugal 81%).

As we move closer to issues which directly concern individuals, support declines. Only 42% of the French and 34% of Romanians supported the
monitoring of citizens’ communications on the Internet by their government, compared with 68% of the Dutch and 61% of the Portuguese. When it comes to monitoring citizens’ calls, only 28% of the French supported their government having greater authority in this field, 45% of the British, 32% of the Romanians and 39% of the Portuguese. Only a majority of Dutch (55%) approved of this measure as well.

What is at play here? Perceptions of these different measures clearly differ from one country to another. Support or opposition most probably depend on the citizen’s perceptions of – and trust in – their own government and the EU.

In Romania, for example, support for these various measures is quite low, although 78% of the public agreed with the more general statement that “we need more equality and justice even if it means less freedom for the individual”. This may be linked to a lack of trust in one’s own government. On the other end of the spectrum, the Dutch very strongly supported these measures, hence they probably have a high level of trust in their own government but are more reticent to give up freedom for more equality and justice.

The UK is at times described as a “mass surveillance society”, and YouGov poll for the Daily Telegraph newspaper in autumn 2006 revealed that 79% of the British public agreed with this description. However, 66% did not trust the government to keep information on databases entirely confidential and 52% felt unhappy about having their own personal details recorded on the national database.

That said, more than 90% of Britons approved of having cameras in banks and other buildings, on tube trains and buses, more than 80% approved of them on high streets and outside pubs, and 65% in taxis.

But when we move from this general idea of surveillance society to the idea of individual surveillance, it appears that 79% disapproved of the use of high-powered microphones to listen in on conversations in the street and 70% disapproved of using chips in Identity Cards to track the movements of every individual possessing one.9

**Decision-makers under constraint?**

All of these results highlight the fact that, while the public is in overall agreement with general measures aimed at improving day-to-day security
(surveillance cameras, etc.), people are more reticent about more intrusive measures related to individuals’ private lives. What does this mean in terms of decision-making on these issues at the EU level? Do public attitudes constrain the different Member States?

Those clearly advocating new laws and international agreements typically point to three circumstances which they believe make these changes imperative: the extreme violence of the new terrorism, its use of the newest technology for communication and organisational purposes, and the transnational character of the threat. These issues have been addressed at various levels of the EU – in the European Commission, the Council or the European Parliament. New bodies have also been established to monitor civil liberties in Europe, such as the European Fundamental Rights Agency or the Article 29 Group.

But be it at the national or European level, public attitudes clearly constrain Member States in their decision-making processes. On the national level, the most recent example is that of the Edvige database in France. Set up in July 2008 by government decree, this database aimed to track anyone “likely to disrupt public order”. Close to 100 civil liberties associations launched a petition and collected some 120,000 signatures, forcing the French government to review the criteria for this database. What is true at the national level is even more so at the EU level, where deciding on and implementing measures in this area is even more challenging.

Hence although it is difficult to delve into the black-box of the decision-making process and clearly identify the impact of public opinion, it seems clear that, as the threat of terrorism is declining in public perception, addressing this issue at an international level will become more and more difficult. The political challenge is, in fact, to find a socially acceptable balance in these security measures, as they are – and will remain – under the scrutiny of civil society.

Natalie La Balme is Programme Officer and Edouard de Tinguy Programme Associate in the Paris office of the German Marshall Fund of the United States.

Endnotes

Transatlantic Trends 2008.
5. Eurobarometer 69, spring 2008.
7. See Eurobarometer 290, June 2008: ‘The role of the European Union in Justice, Freedom and Security
   Policy areas’.
Power to the people? The implications of the social network revolution

The soaring popularity of social networking sites such as Facebook and MySpace underlines how attitudes towards privacy and information-sharing are changing, especially among the younger generation. This essay argues that regulators have not woken up to this new reality, which challenges the traditional top-down approach to policy-making.

by Kay Withers

The problem of the Internet has been troubling policy-makers for some time, ever since it moved beyond being solely the concern of geeks and into the homes and lives of families throughout Europe.

Across Europe, internet penetration will shortly reach 50% of the population, and in the UK, for example, almost two-thirds of the British population are online and four out of five 5-to-15-year-olds have access to the internet at home. It is therefore not surprising that the Internet – and its related threats and opportunities, particularly for children and young people – should get politicians and the media so excited.

The Byron Review, published in March 2008, and the UK Parliament Select Committee Report into Harmful Content on the Internet and in video games published in July of the same year, both reflected on approaches to ensure young people were kept safer online.

The Byron Review was praised for its “excellent and balanced view”, but the more hard-line report from the Culture, Media and Sport Select Committee, chaired by Conservative MP John Whittingdale, has in contrast been criticised for over-emphasising the World Wide Web’s “dark side” at the expense of understanding the opportunities it offers.

While both reports raised questions about the scale and ease of access to harmful or inappropriate content online, it is the behaviour of young people themselves – especially where they are considered too open and transparent with personal data – that seems to cause the most consternation.

The concerns expressed by policy-makers and politicians, their estimations of the risks young people are exposing themselves to, and the suggested
solutions for keeping young people safe, are the starkest indications of the extent of the cultural change now underway. They also highlight a growing generational divide between the attitudes of young people and their parents and regulators.

The most significant driver of behavioural change has been the rapid take-up of social networking sites. In the UK, almost three quarters (72%) of children have visited a social networking site and more than half of these have set up their own profile. Over half (56%) of the European online population visited social networking sites last year and regular users are forecast to rise from 41.7 million now to 107.4 million in the next four years. Part of the attraction for young people is that the most popular of these sites – MySpace, Facebook, and Bebo – are free to use.

But more than this, social networking sites offer young adults the opportunity to develop a sense of self and identity at a point in their lives where they are beginning to make the transition towards gaining autonomy from their parents and formulating independent relationships with peers.

By their very nature, social networking sites demand self-disclosure. In order to ‘exist’ in the context of a social networking site, users must “write themselves into being”. They must build their digital identity by adding information about themselves, including their name, address or location, age and birthday, e-mail and instant messenger addresses, and mobile phone numbers, as well as information about likes and dislikes in the fields of music, television programmes, films, books and so on.

Not all of this information is obligatory – one’s profile can be as detailed or as sparse as desired. But there is a strong rationale for young people to make their profile as ‘attractive’ as possible, for example by adding photos and other content, in order that other people on the network will want to befriend them.

Research carried out by the Institute for Public Policy Research (IPPR), conducted with Internet users aged between 13 and 18, found that social networking profiles were frequently referred to as being used for “self-advertising”: “You’re like advertising [on Bebo], so you like put your own picture up and your own information.”

Data from the US shows that, of users of social networking sites, 79% have included photos of themselves, 66% photos of their friends, 49% the name
of their school and 40% their instant message screen name. One in 20 teenagers with social networking profiles disclose their full names, photos of themselves and the town where they live in publicly viewable profiles.\(^9\)

For politicians, this kind of behaviour raises concerns in that it is presumed to leave young people exposed to unacceptable risk. The Child Exploitation and Online Protection Centre (CEOP), a law enforcement agency in the UK, has previously commented that these “new environment[s] can facilitate new forms of social deviance and criminality”, particularly in enabling “new opportunities for sexual expression and deviance both to young people and adults with a sexual interest in this group”.\(^10\)

In response, they have demanded that the default setting for profiles of young people aged under 16 should be ‘private’; i.e. viewable only by people who have been ‘vetted’ or accepted as friends.

In the real world, this apparently simple solution quickly falls down. For one thing, the attraction of the network is too great. During middle adolescence, peer feedback and acceptance is a particularly important part of psycho-social development. Social networking sites offer young people the opportunity to display or advertise themselves in pursuit of new friends.

As one respondent interviewed as part of our research commented: “If you want to make new friends on the Internet, then [if you have it set to private] no one can view your profile to make friends with you.”\(^11\)

Second, even if a young person restricts his or her profile to make it only viewable by ‘friends’, the concept of ‘friendship’ is stretched so wide in relation to social networking sites that this hardly constitutes any kind of safety buffer at all.

But the starkest conclusion to draw from the suggestions made by policy-makers and the real-world failure of their proposed solutions is that they simply do not understand the extent to which digital technologies and their pervasiveness in everyday life have altered the way in which many view and manage privacy – particularly those who have grown up with constant connectivity as the norm.

The characterisation of regulation as slow to respond, heavy-handed, inappropriate and ill-suited to the fast-moving, innovative, flexible, networked world of digital media is not uncommon.
The ‘anarchic’ nature of the Internet means it is near impossible to dictate, and indeed to police, rules for behaviour from on high. Nonetheless, public policy approaches to the question of privacy seem intent on doing so, working from the assumption that there is one definition of privacy, that it should be enforceable across services such as Bebo et al, and that a centralised approach will serve this aim best.

Finally, they are wedded to a definition which equates privacy with obscurity. Any surrender of this suggests an overwhelmingly public or transparent existence – a state of affairs which sits very uncomfortably with the pre-digital generation.

In actual fact, privacy has always been something of a moveable beast: a state of affairs that has been defined by an individual sense of what we are and are not comfortable sharing. Over the years, the norm has of course been shaped by social factors and changed in accordance with the times: we no longer expect the modesty of dress or behaviour promoted throughout the Victorian era, nor do we consistently rue the day such stringent expectations disappeared.

The level of connectivity we now experience means it is now often easier to share than not to share. For instance, whereas a lack of mobility previously meant ‘private’ conversations took place in our own homes or, if outside, in a call box designed to protect discussions from being overheard, mobile phones have freed us – and conversations with our friends, family, colleagues, doctor, bank manager – from the constraints of time and place landline phones once bound us to.

In busy lives, it is often more convenient to use the time otherwise spent staring blankly out of the train or bus window to organise social activities, arrange appointments or discuss other aspects of our daily lives – to get something done using the technology that is available at our fingertips – regardless of who may be sitting next to us, listening in.

The prevalence of technology and the pressure to be connected in order to exist successfully in modern society means there can be no blanket declaration of what is and what is not privacy. For individuals, it is a case of managing their exposure on a case-by-case basis and assessing risk as they see fit.

Where does this leave policy-makers? Well, for one thing, it is of course important that individuals have a thorough understanding of the
risks implicit in sharing personal information and data, and that they are capable of making informed decisions. This is less to do with enforcing a view of privacy and much more about encouraging a higher state of media literacy, particularly amongst young people who can be seen as most at risk.

In giving away so much, few young people make any assessment of the impact their actions – recorded and available to all now, and in the years to come – could have on future desires and decisions, particularly those related to job and university applications. A greater sense of the ‘imagined audience’ – the people viewing profiles and content who are not friends or acquaintances – is necessary so that young people can think twice before posting content or information which may be suitable amongst friends, but less so for future employers.

This can be achieved by encouraging young people to create content – to give more away – albeit under the guidance of media professionals, and to think more about the audience they are trying to reach as well as the audience who may stumble across their efforts unawares.

Secondly, it is important that legislators ensure imbalances of power are addressed. This means providing citizens and consumers with the tools to check that their privacy – however defined – is being respected. Ensuring that the tools we have carved out in this area – data protection and freedom of information legislation – are accessible, intuitive and fit for citizens’ purposes, is essential. Likewise, regulators may also have a role in stimulating and encouraging action amongst industry to make sure they meet their consumers’ needs, if this is not readily forthcoming.

The Internet has threatened the hierarchical, top-down way in which we approach many of the challenges society faces. It is difficult for policy-makers to let go, to appreciate that there is not a perfect solution and to trust that the best result is likely to emerge from users’ themselves.

It is important that we take stock of, and make attempts to understand, what changes to privacy and our concept of ‘private mean’ for society as a whole. But at the same time we must recognise that privacy was never an absolute and it has always changed as society has changed. While being aware of what we are giving up, there may also be much to gain: opportunities for collaboration, information sharing and improved services, for example.
The choice now is not between absolute privacy and absolute transparency, but managing a delicate balance between the two. It is up to regulators to provide the framework to ensure that this is what citizens themselves can achieve.

Kay Withers is Deputy Director, Media Standards Trust, and a former Research Fellow in the Strategic Research Team at the Institute for Public Policy Research (IPPR).

Endnotes

11. Boy, 15, C2DE.
Can Big Brother distinguish fellow citizens from aliens?

Is ‘national citizenship’ becoming an increasingly irrelevant concept in protecting the population from security threats, in light of increased mobility and phenomena such as the emergence of ‘home-grown’ terrorists? This essay argues that while these developments have complicated the picture, it would be premature to pronounce the death of ‘national citizenship’ in the security versus liberty debate.

by Jo Shaw

What is the relationship between citizenship and security? Is formal membership of a national state still, if it ever was, a useful proxy for determining who is to be afforded what type of security, for settling the means by which security is to be promoted, and for identifying the relevant geographical area within which controls can be imposed?

To put it another way, have we moved decisively away from the era where – at least during times of war – enemy aliens would be regularly interned, regardless of any individual assessment of their hostile intent (or lack of it)?

In today’s world of cheap travel and increasing population mobility, is it either desirable in principle or feasible in practice to use the boundaries of national citizenship as the basis for identifying particular communities as inherently suspect in the context of established security threats such as political violence or organised crime?

If one cannot use citizenship, are there other proxies or criteria, such as the controversial ‘ethnic profiling’, which could assist in identifying threats and risks for the purposes of feeding policy-making? Or do the answers to maximising security simply lie in adopting the broadest possible measures which apply regardless of national citizenship? And, finally, is there a specific ‘European’ set of answers to these conundrums?

There have been three particularly significant drivers for the rapid development of EU law and policy in justice and home affairs since the 1990s. These drivers are partly specific to the process of European integration and partly related to more general global trends – for example, cheap travel; global movements of capital; trends towards transnational organised crime; ever-greater economic inequalities (especially between
north and south); and generalised tensions between the more secular but still Christian-dominated ‘West’ and the Islamic world.

The first of these factors has been the argument that – in the context of a single market where goods, services, persons and capital can move with relatively few restrictions – it no longer makes sense to apply either a concept of national security or a notion of combating crime and criminality in one specific territory, without regard to the possibilities for more effective regulation of such questions offered by using the EU as a whole as a reference point for policy-making rather than individual Member States.

The second factor concerns the so-called ‘war on terror’, which has reached a particular crescendo since the bombings in New York and Washington on September 11 2001 and the inception of US-led military action in Iraq and Afghanistan.

The third and final driver involves many different aspects of population mobility and migration, especially the pressures which were placed during the 1990s and early 2000s on the asylum and refugee structures of many EU Member States – not least as a result of the wars in the former Yugoslavia, but also as a result of conflict in the Middle East and Africa; the many human tragedies which occur in the Mediterranean Sea and elsewhere as individuals and groups seek to cross the borders into the EU in search of a better future (often also suffering at the hands of organised trafficking gangs); and the intense politicisation of many aspects of the post-settlement integration of immigrants, especially problems of social cohesion and welfare for both immigrants and receiving societies.

These developments have been laid across an evolving and still rather unsatisfactory set of treaty and institutional arrangements for policy-making in relation to what has been termed, since the Treaty of Amsterdam, the ‘Area of Freedom, Security and Justice’, with particular lacunae still evident, especially in relation to matters of parliamentary and judicial control.

In addition, there is an increasingly visible trend of ‘variable geometry’ – or flexible integration – building upon the existing opt-outs or other special arrangements for Denmark, Ireland and the UK.

In the midst of these trends and factors, it would still be a considerable oversimplification to maintain that national citizenship is becoming an irrelevant legal and political status or marker. In fact, there are
many countervailing forces cutting across those of Europeanisation and globalisation.

It is certainly true that the EU and its Member States have largely eschewed the approach to so-called “homeland security” which has dominated in the United States. This has focused in very large measure on treating the ‘alien’ as a suspect classification, concentrating restrictive measures on this category of persons.

Within the EU itself, or at least within the Schengen area, restrictions on free movement based on nationality are limited. Furthermore, the European Convention on Human Rights (ECHR) provides fundamental rights’ guarantees which constrain all European states in relation to the use of the term ‘alien’, without more qualification, as a suspect classification in this way.

Equally, as is well known, terrorist attacks such as those in the UK in 2005 or certain politically-motivated murders in the Netherlands, such as that of the controversial film-maker Theo van Gogh, have been committed by people of the same nationality as (most of) the victims.

Clearly, for whatever reason, radicalisation processes and a commitment to indiscriminate political violence have cut deep into European societies and national populations in a way which does not appear to have happened in the United States.

But despite this, it is clear that national citizenship retains both a legal and symbolic value, amidst the pressures of globalisation and Europeanisation. This occurs in a variety of different contexts and for a variety of different reasons, some pragmatic and others more principled in character.

For example, national citizenship is the gateway to EU citizenship and, consequently, differences in the rules on acquiring citizenship across the 27 Member States will inevitably create a variety of incentive structures for persons seeking to enter and settle in the different Member States.

This rule governing the acquisition of EU citizenship can be understood as an expression of national sovereignty, insofar as the Member States remain the ‘masters of the Treaty’, and has considerable consequences for the current state of EU law.

At present, the extent of EU regulation of the legal status of third-country nationals who are settled long term in the Member States is rather
limited (and in any event the UK and Ireland have both opted out of the relevant Directive). 1

Member States are now obliged to grant settled long-term residence status to those who have lived in the country for a minimum of five years. However, there are very limited facilitation arrangements for transferring that status to other Member States and even more limited access rights in relation to their labour markets. The depth and extent of the protection offered to them is also scant compared to that accorded to EU citizens who take advantage of the right to free movement (and indeed members of their families who are third country nationals).

In the context of political rights, national citizenship remains the main criterion acting as the gateway to what one might call the “gold standard” of political participation, namely the right to vote in national parliamentary elections.

EU law has made significant inroads in this respect, with the right to vote in European Parliament elections explicitly accorded – under Article 19 of the EC Treaty – to citizens of Member States resident in other Member States under the same conditions as nationals, and implicitly recognised as an EU citizenship right by European Court of Justice case law. As the European Parliament grows in importance as a legislature, its elections are likely to grow in political salience.

Article 19 of the EC Treaty also gives migrant EU citizens the right to vote in local elections in the state of residence, under the same conditions as nationals, as an expression of EU citizenship as a form of citizenship of residence.

However, EU law has no impact on voting rights in national elections, or indeed in elections to sub-national units, such as the Länder in Germany or the autonomous communities in Spain. (Interestingly, in the UK, EU citizens can vote in elections to the Scottish Parliament and the Welsh and Northern Irish Assemblies – but this is a national anomaly).

Third-country nationals are not covered by EU law in this area, and their voting rights are generally scanty and limited to local electoral rights in some Member States (with the exception of rights for Commonwealth citizens in the UK). Furthermore, EU law does not interfere with the extent to which Member States allow expatriate citizens to ‘export’ and use their voting rights.
While the implementation of the Schengen Agreement has seen the removal of frontier controls between most of the Member States (an arrangement which even extends to a number of non-Member States), it does not – as is well known – apply to the UK and Ireland. In fact, in the context of the UK e-borders project, it would appear that there will be effective passport – or at least identity – controls on pretty much all movements between Great Britain and the island of Ireland, including Northern Ireland, within a few years.

This is a highly controversial development, and it appears to extend control over movements within a Member State as well as between two states. As such, it can perhaps be understood as an example of a state instituting the broadest type of legislation which cuts deep into traditional freedoms existing within states, rather than simply adopting legislation which uses national citizenship or territorial divisions between states as its main reference point.

Moreover, from time to time Schengen states do reinstate frontier controls for public-order reasons (for example, in order to restrict the movement of those alleged to be involved in football hooliganism during a major tournament). In any event, they also retain the power to impose controls in the form of identity checks within states rather than at the frontier (for the purposes, for example, of ascertaining nationality) and to fine those who have forgotten to carry the relevant ID or passport.

Finally, it is clear that there are still active debates within a number of states about the nature of national identity and/or citizenship which focus on, for example, what it means to be British, or Spanish, or Belgian. These are all states where there are sub-national territorial challenges to the very existence of the state as a whole, with active movements promoting secession or greater political and legal autonomy.

In the UK, for example, Prime Minister Gordon Brown (who is Scottish) has sought to foster a debate about Britishness and to ask the question: what does being a British citizen entail?

At his request, former Attorney General Lord Peter Goldsmith wrote a report which tried to make sense of some of the many anomalous rules which make up the body of British citizenship rights and duties, many of which are the result of historical contingency or pragmatic political concessions. It suggests, for example, curtailing the voting rights of Commonwealth citizens, focusing more narrowly on protecting the exclusivity of British citizenship rights. At the
same time, the Home Office has been working on documents which focus on restricting access to British citizenship by using techniques such as enhanced tests for newcomers and forms of probationary citizenship.

These focus on the idea of outsiders ‘earning’ access to citizenship, and many of the underlying policy arguments which are used to justify restrictive measures have strong securitisation elements embedded within them. These types of restrictions on acquiring citizenship are visible in many other EU Member States.

It is therefore hard to conclude that there is a single trend either undermining or sustaining the core of national citizenship as a legal and political status. On the contrary, we can see complex sets of countervailing forces heading in different directions at once. It would therefore be premature, in the extreme, to pronounce the death of national citizenship in the context of current developments around security and liberty.

Jo Shaw holds the Salvesen Chair of European Institutions and is Co-Director of the Europa Institute in the School of Law at the University of Edinburgh.

Endnote

II. WHO IS ‘BIG BROTHER’? THE DRIVERS FOR INCREASED SURVEILLANCE AT NATIONAL AND EU LEVEL

The surveillance society: trends and implications for data protection

New technologies are being used to track individuals’ movements and activities for different reasons – some innocent or even positive, others more problematic. This essay examines what is driving this process and argues that existing frameworks must be kept under constant review to ensure they remain effective in light of social and economic changes, technological advances and globalisation.

by Peter J. Hustinx

In June 2006, the Surveillance Studies Network – a team of social researchers with a special interest in surveillance issues – was commissioned by the UK Information Commissioner to write a report on the surveillance society.

This report, presented in November 2006 at the 28th International Conference of Data Protection and Privacy Commissioners in London, took the view that we are already living in a surveillance society.¹

Surveillance as discussed in the report involves the purposeful, routine and systematic recording through technology of individuals’ movements and activities in public and private spaces, for different reasons, some of which are innocent or even positive, while others are more problematic.

The report analyses the surveillance society as a product of modernity, which started to develop as soon as rational methods began to be applied to organisational practices. This helps to avoid two traps: “thinking of surveillance as a malign plot hatched by evil powers and thinking that surveillance is solely the product of new technologies.”²

To be sure, it also helps to identify strategies needed to deal with the negative aspects of a surveillance society. The report mentions quite a few, and they go far beyond the right to privacy and personal-data protection.
It is a matter of taste whether one prefers to see the surveillance society – or the ‘Big Brother’ society as some call it – as something to avoid ‘in the future’, or to deal with ‘in the present’ as effectively as possible. However, the report makes a powerful case for the latter and suggests different ways to do this.

It also highlights different trends and different actors in a larger historic perspective. Certainly, the development, production and marketing of information and communication technologies is playing a major role, but in clear and close interaction with new ways of delivering products and services in a modern society, both in the private and (semi-)public sectors.

The key feature in this context is a trend towards more and more personalised services, even in areas still dominated by principles of social equality. The capacity of information technology to support and facilitate this growing trend of personalisation goes hand in hand with its capacity to store and remember information, to track and trace individual behaviour, and, where necessary, to identify characteristics which may be regarded as attractive or unattractive in different environments.

Hence the need to ensure that the use of these new technological tools complies with legal safeguards, such as the principles of data protection which give rights to individuals to protect their interests, impose obligations on responsible organisations, and ensure adequate oversight and enforcement through sanctions where needed.

If we can now see (briefly put) information technology, business, government and our modern way of life in general as the main contributing factors, we should still be aware of two other important trends.

The first is a growing emphasis on the prevention of risks. This leads to the use of information technology to ‘exclude’ individuals who seem to match a certain profile, and the faith that large information systems will be able to make this selection both efficiently and effectively.

The second is the growing tendency of governments to impose duties on private-sector organisations to collect, retain or report data for public interest reasons, outside the scope of their natural activities. This is why financial institutions, telecoms operators and airline companies are now involved in data operations which clearly go beyond their own interests and appear to be at odds with legitimate privacy expectations.
The 28th International Conference in London was not only a platform for discussion and raising awareness of these trends and related issues, but also the right place to act on the challenges posed to privacy and data protection. This resulted in the launching of a statement – ‘Communicating Data Protection and Making It More Effective’ – which received general support from data-protection authorities around the world.

The main points of this ‘London Initiative’ include:

- The protection of citizens’ privacy and personal data is vital for any democratic society, on the same level as freedom of the press or the freedom of movement. Privacy and data-protection may, in fact, be as precious as the air we breathe: both are invisible, but when they are no longer available, the effects may be equally disastrous.

- Data Protection and Privacy Commissioners should develop a new communication strategy in order to make the public and relevant stakeholders more aware of these rights and their importance. They should initiate powerful and long-term awareness-raising campaigns and measure the effects of these actions.

- Commissioners should also communicate better about their own activities and make data protection more concrete. Only when these activities are meaningful, accessible and relevant for the public at large is it possible to gain the necessary power to influence public opinion and to be heard by decision-makers.

- Commissioners should assess their efficiency and effectiveness, and where necessary adapt their practices. They should be granted sufficient powers and resources, but should also use them in a selective and pragmatic manner, while concentrating on serious and likely harm or the main risks facing individuals.

- Commissioners should reinforce their capacities in technological areas, with a view to producing advanced studies, expert opinions and interventions, in close interaction with research and industry in the field of new technology, and share this work together. The excessively ‘legal’ image of data protection must be corrected.

- Commissioners should promote the involvement of other data-protection and privacy stakeholders – such as civil society and NGOs – at national or
international level, to develop strategic partnerships where appropriate, with a view to making their work more effective.

Commissioners have been engaged in a work programme of follow-up activities along these lines and recently evaluated progress at their 30th International Conference in Strasbourg in October 2008. The emphasis on “better communication” and “effective data protection” will continue to guide their strategies in the near future.

As European Data Protection Supervisor and one of the main initiators of the London Initiative, I have strongly supported these efforts. The need for effective data protection has also been a driving force in my consultation activities. The need for ‘effectiveness’ is of course not only a legal concept, but also a practical requirement with great strategic consequences. The right to privacy and personal-data protection can, after all, only be made ‘effective’ in practice, and this certainly includes situations where the need for protection is greatest.

This leads to three main conclusions: first, the EU and its Member States must give full effect to the data-protection frameworks that already exist; second, they must ensure adequate protection in areas not yet covered or in need of additional protection; and third, they must ensure continued effectiveness in the light of changing circumstances.

The EU Directive on the protection of personal data (95/46/EC), implemented in 1995, is still the most important element of the present data protection legal framework.

The European Commission has called for a better implementation of the principles of this Directive in national law and is pursuing different activities to promote this goal, including infringement procedures against individual Member States – an approach that I have fully supported. This goal is also promoted when national data-protection authorities work together to clarify some key provisions of the Directive or undertake joint enforcement actions.

This Directive does not apply to the areas of law enforcement presently dealt with under the EU’s ‘third pillar’: cooperation between police and justice in criminal matters. This is an area where the need for adequate safeguards is evident, but where it has also been difficult to reach conclusions within the present institutional arrangements, which require unanimity. A general framework for data protection in this area is now close to adoption, but it is
also clearly in need of further improvement, to be expected perhaps on the basis of other institutional arrangements.

The need for improvement has now also become visible in the EU’s ‘first pillar’, especially in areas where the interaction with information technology is most relevant.

A revision of the e-Privacy Directive (2002/58/EC) is currently before the European Parliament and the Council. One of its results is likely to be an obligation to report breaches of security resulting in personal data being compromised, under certain conditions, to competent authorities and individuals concerned. This will raise public awareness of the need for more improved security and effective protection of personal data.

Improvements are also necessary and to be expected in relation to the introduction and growing use of radio frequency identification technology (RFID) for identifying consumer goods and perhaps also monitoring individual behaviour.

The European Commission has announced that it will publish a Recommendation to specify some key data-protection principles in this area and to promote self-regulatory solutions. I have called for adequate legislation in the event that such solutions prove insufficient or ineffective.8

The general frameworks and other instruments mentioned so far are also important when new policy or legislative measures are proposed which may have an impact on the protection of personal data. The existing rules then also serve as criteria to determine whether the new initiatives are acceptable and comply with data-protection standards, or need to be amended or supplemented by other safeguards. Ensuring adequate feedback on these questions to the Commission, Parliament and Council is an essential part of my role as European Data Protection Supervisor.

Finally, it is necessary to ensure that existing frameworks continue to be effective in the light of social and economic changes, new technologies and globalisation. This is why – while fully supporting the Commission’s call for a better implementation of Directive 95/46/EC – I have also stated that a revision of the Directive is unavoidable in the near future and that adequate preparation and planning for this are crucial.9
I am very pleased to note that the first careful steps towards a revision of the Directive, in the form of preparatory studies, have now been taken, and I look forward to all subsequent steps in the right direction.

Peter J. Hustinx is the European Data Protection Supervisor.

Endnotes

4. See Articles 7 and 8 of the EU Charter of Fundamental Rights, which are to become binding when the Lisbon Treaty has been ratified.
Restraining Big Brother’s ‘courtiers’ – the need for a bill of rights

The fight against terrorism and crime prompted the Swedish government to introduce new measures to ‘eavesdrop’ on Internet traffic passing through its territory. This essay uses the Swedish experience as a case study to highlight the legal and ethical problems such measures raise, and argues that a ‘bill of rights’ is needed to reset the balance in the security versus liberty debate in favour of the individual.

by Jonas Hartelius

Sweden has traditionally always been an open society. Its first Freedom of the Press Act in 1766 – the first of its kind in the world – made all public records open to inspection by everyone, except in a small number of well-defined areas such as national defence.

It has, at least at the political level, also been a very keen supporter of the United Nations and the EU, aiming to be ‘best in class’ when it comes to implementing EU Directives swiftly, and has adopted the European Convention on Human Rights (ECHR) as domestic law.

Recent developments have, however, challenged that tradition and highlighted many of the key issues raised by the emergence of the ‘Big Brother’ society.

**Swedish signals’ intelligence**

During World War II, Sweden developed world-class capacity in signals’ intelligence. Swedish mathematician Professor Arne Beurling cracked the German crypto-system Geheimschreiber in 1940, and shared much of that material with the Allies. Sweden also helped Finland with intelligence from Soviet radio communications.

The Swedish signals’ intelligence system was later (1942) bundled up in the ‘Försvarets Radioanstalt’ (FRA – Swedish National Defence Radio Establishment), which exchanged large volumes of signals’ intelligence material with similar agencies in other countries.

With the shift in global communications’ patterns mainly to cyberspace, the FRA was losing its raison d’être by the early 2000s, until the then Social
Democratic government stepped in to try to resuscitate it, essentially by proposing to give it blanket permission to eavesdrop on Internet traffic passing through Swedish territory in order to combat terrorism and crime.

After a change of government in October 2006, to a Conservative-Centre-Liberal-Christian Democrat coalition, this was translated into a government bill presented to the Swedish Parliament in March 2007. Everyone expected it to pass easily, as it had been drafted by the Social Democrats, now in opposition, and presented by the new government. But in spring 2008, the media woke up to the story and launched the most volcanic discussion on privacy and the ‘Big Brother society’ in decades.

The Swedish ‘FRA’ debate

Critics hammered the proposal from all sides, ranging from accusations that journalists’ sources would not be protected to charges that it would breach the right to secret communications enshrined in the ECHR.

A ‘civil cyber war’ broke out between ‘cyber pirates’ and FRA employees, who hacked into each other’s systems. Great concern arouse about the exchange of ‘raw intelligence’ with other countries, some of which were not of a democratic mindset. Even Conservative and Liberal newspapers criticised the Bill, and several members of the government bloc threatened to vote against it. However, when it came to the Parliamentary vote in June 2008, 143 members voted in favour, 138 against, one abstained and 67 were absent. The opposition voted against, but only one government member ‘rebelled’.

However, the debate raged on and in early September, several Liberal members announced that they would vote to repeal the law when the Parliament reopened later that month. This sparked a political crisis, prompting a profound revision of the Act to reinforce the protection of privacy.

The most important changes were that permits for signals and electronic intelligence eavesdropping would have to be granted by a court and only for the channels indicated by the court; that the FRA would have to apply for permission, even when serving the government’s needs; that eavesdropping on communications between two parties both living in Sweden would be prohibited; and that eavesdropping would be permitted
only at the request of the Government, Government Administration or the Armed Forces.

The criteria for initiating eavesdropping would be to combat external military threats; Swedish participation in peace-keeping or humanitarian international operations; terrorism affecting national security; serious threats against infrastructure; and a small number of other cases. The government had nominally salvaged the FRA law by gutting its most controversial provisions, but the critics were not fully convinced.

As the debate continued, a European Court of Justice (ECJ) decision in September 2008 profoundly altered the balance between human rights and the fight against terrorism. In 2001, the United Nations Security Council and the EU had put three Swedish citizens of Somali origin and a Swedish-Somali bank transfer network (al-barakat) on a watch-list for allegedly financing terrorism. The individuals were later taken off the list. The network sued to have its assets unfrozen. The ECJ ruled that an EU decision could not overrule fundamental human rights, such as the right to defend oneself against accusations.

**Technical and scientific considerations**

Running automated Information Technology systems to monitor human behaviour raises delicate technical and scientific considerations.

Striving for ‘total information’ is not a solution, as an unfiltered influx would still have to be sorted. Warning flags would flourish like bamboo and the ‘miscellaneous’ box would rapidly overflow.

Preventative monitoring of electronic communications is often based on profile systems, with certain names and phrases triggering further analysis – a ‘McDonaldisation’ of intelligence, with fast-food logistics techniques used to run a tight system. It is based on Weber’s ideas of rational control,\(^2\) takes thinking and individual judgment out of the process, and thus suits the bureaucratic mindset of ‘control’.

Here, one major problem is to find a balance between sensitivity and specificity. Sensitivity is the ability of a method or system to identify the really bad cases (of illness, drug intoxication, fraud, etc.). Specificity is the ability to rule out false alarms. Even a minor deficiency in the specificity can make false alarms much more frequent than genuine cases for low-frequency events.\(^3\) The collateral damage can be considerable.
The total analytical capacity is probably a state secret in most countries. But it is clear that the main bottlenecks in surveillance systems are the human factors, such as translators, interpreters, analysts, etc.

Even with good linguistic capabilities, innuendo and hidden meanings may be lost. In the police investigation into the 1986 assassination of Swedish Prime Minister Olof Palme, the phrase “celebrate wedding in the streets” became the focus of an investigation into some Kurds with alleged affiliations to the PPK (the Kurdistan Workers’ Party). The phrase was believed to be a code for “assassination”, but eventually the trail petered out.

Labeling people’s political views can also be delicate, even difficult, and names can be mixed up. In Sweden, there are two well-known media people with the first name “Carl” and the family name “Hamilton”, as well as a famous fictitious agent of the James Bond type (created by Jan Guillou). This creates the potential for enormous confusion.

Furthermore, sometimes, the conclusions drawn can be unwarranted. Dr R.V. Jones, Director of British Scientific Intelligence in World War II, later wrote that he would have more concerns about a government misinterpreting or making false conclusions about him based on personal information than about the government having that information per se. Today’s systems seem to have very few quality checks in this respect.

Further problems are caused by the difficulties in keeping databases up-to-date, as illustrated by the case of a police officer who shot and killed someone suspected of travelling in a stolen car. In fact, the car had been retrieved and resold, but the police data had not been updated.

With the unfiltered exchange of raw data between governments, agencies, companies, media and other parties, quality control becomes spurious. Those acting upon the information can always pass the buck to the earlier links in the communication chain.

Finally, there is a decisive philosophical caution related to the whole business of building surveillance and monitoring systems: these can only keep track of what they are designed to detect; anything ‘outside the box’ will be difficult to handle and act upon.

The security and intelligence services are organisational environments in which conspiracy theories and paranoia flourish. They are often staffed by
Challenge Europe – December 2008

people who have little tolerance for uncertainty and ambiguity and are obsessed with order and structure. This makes them disinclined to deal with ‘deviant’ information.

Such organisations also have conceptual filters. This is likely to lead to ‘failures of imagination’, where the analyst or organisation deems certain situations to be impossible on the basis of the available facts. Many terrorist attacks have turned out to be of this kind.

For these reasons, even if the intelligence and security services were given total access to all electronic information, they would not necessarily be able to act sensibly upon it.

**Ethical and legal considerations**

The current Swedish FRA debate and parallel debates in other countries also raise ethical and legal considerations.

The ECJ ruling on the *al-barakat* case seems to have re-established the rule of law in the fight against terrorism and the financing of terrorism. In the same way, any further proposals for increased IT surveillance, etc. will have to take into consideration human rights such as the right to secret communication.

Professional groups working in gathering, analysing and acting upon information from surveillance systems must develop their professional ethics in the same way as lawyers and physicians did a long time ago, and police officers, journalists and others have done in the post-war period.

Here, Dr Jones has offered thoughtful advice, formulating two doctrines for intelligence work: “minimum force”, which is an established principle for military and police action; and “minimum trespass against national and individual human rights”. Both would restrain Big Brother’s courtiers.

Ethical and legal considerations must also set limits on ‘dual’ or ‘multiple’ use of information; for example, health records which have originally been collected for other purposes.

Methods and systems are likely to be challenged as to their reliability, admissibility, etc. in court cases and administrative decisions. Investigative journalist Tim Shorrock has highlighted the dangers of ‘outsourcing’ intelligence to private companies, whose behaviour is governed by less
stringent rules. The subsequent diminishing control through established bureaucratic procedures will probably prompt calls during trials for detailed revelations of the methods used to gather intelligence – for example, if torture has been used.

For these reasons, the monitoring by intelligence and security services of electronic information should be fully subservient to the protection of human rights.

**A ‘Bill of Rights for the Information Age’**

Challenging the widely-held belief in intelligence and security services that the state has the right to access all information in electronic form, Bryan Glastonbury and Walter LaMendola have drafted a ‘Bill of Rights for the Information Age’, which lists 15 proposals relating to the use of IT.

They argue that human rights, as set out in the Universal Declaration of Humans Rights, “should be reasonably and prudently considered in all processes of IT development, use, and application”. This means that any electronic surveillance system should be subject to the same regulations and supervision as other forms of monitoring and documenting human behaviour.

They also rule out any automated decision-making by an IT device if it affects a human being. There should always be a designated person accountable for decisions. This would rule out ‘suspicious’ persons being automatically put on watch-lists, etc. through data mining or trawling. It would also require very high levels of quality control of the data circulating in any IT system, as ‘data smog’ makes it difficult to evaluate information during field operations. (The police shooting case mentioned above clearly indicates the dangers of leaving old data in circulation.)

The authors also insist that people affected by IT device-aided decisions should be fully informed at all times and have an incontrovertible right to appeal against all such decisions through the courts or formal appeal processes. This would rule out the original design of the FRA Act, but seems to have been only partially addressed by the new version.

Personal information should to be regarded as the property of the person who is the subject of the data (or guardian, etc.), and permission obtained for any use of this data, putting an end to the current widespread sharing and selling of personal data, such as information about customer behaviour patterns.
Other recommendations include compensation for damages for unintended and unrecognised consequences of IT use; legislation to protect personal data, etc.; and restricting IT development and applications to peaceful uses only. To this one might add that any IT system used to pinpoint people would have to be scientifically validated before it is put to administrative use.

A Bill of Rights for the Information Age would reset the balance in favour of the individual. It would reduce the blanket application of IT in fighting crime, etc. to cases where there is a certain level of suspicion. It would put tangible restraints on Big Brother’s use of IT for the blanket monitoring of the population at large. Still, it is not likely to be enacted in the near future.

Jonas Hartelius is Senior Fellow at the EastWest Institute in Brussels and Scientific Adviser at the Swedish Carnegie Institute, Stockholm.

Endnotes

3. See, for example, C. McCue (2007) Data Mining and Predictive Analysis, Amsterdam: Elsevier, for a general discussion.
7. See, for example, H.L. Wilensky (1967) Organizational Intelligence, New York: Basic Books.

References

The literature in this area is immense. The above works have been useful to add substance to the line of argument in this text. They could serve as an introduction to some of the central issues.
A worthwhile sacrifice? Trading privacy for better public services

Governments are now collecting and storing vast amounts of their citizens’ personal data, sparking growing concerns about how this information is being used. But while acknowledging that safeguards are needed to prevent this information from being abused, this essay warns against overlooking the potential benefits of using it to design and deliver better public services such as health, transport and housing.

by Fabian Zuleeg

Many of Europe’s citizens are concerned about how the public sector treats their personal data. Not only do various government departments in different countries seem careless – hardly a week seems to go by without news of another loss of private data – but citizens are also worried about how information about them is used and shared between different public-sector organisations, as well as being shared with, or even sold to, companies.

But the nightmare scenario of ‘transparent’ citizens without privacy – the ‘Gläserne Bürger’ often referred to in the German media – is only part of the story. The potential benefits of sharing data are also very significant, offering real opportunities to better design and target public services, saving European taxpayers’ money. Data can also be used to personalise services, ensuring that citizens get what they want rather than what a planner decides they might need, and opening the door to much more evidence-based and effective delivery.

Europe’s opportunity to lead from the front

There are a number of pertinent issues related to the exchange of data at the European level.

Data exchange between public services is critical for individuals’ mobility in the EU’s Single Market. For example, health and social security records must be fully portable between countries to enable genuine free movement of people.

The European Commission could also use data much more proactively in designing, evaluating and customising EU policies, to be at the forefront of
evidence-based policy. Indeed, the EU can become a vital centre for such analysis, developing benchmarks and using data from different countries to test policies and determine what works under what circumstances.

This could be of real benefit in many areas, including, for example, public health, where it could help to test the effectiveness of measures such as advertising restrictions. It is also increasingly being used to judge how the Single Market is working by, for example, testing statistically to what extent prices correspond across borders, and could even help to pinpoint firms guilty of uncompetitive practices. It can also be used to test the impact of price or income support on agricultural production or the effect of different price levels on energy consumption, and provide a vital tool in the impact assessment and ex-post review of European legislation. The applications are almost endless.

To realise this potential, however, there is a need to rethink the EU’s ‘architecture’ in this context. The responsibility of Eurostat, the EU’s statistical agency, for collecting and analysing statistics does not extend to this kind of data. This might be the ideal time to create an EU strategic framework to realise the benefits it can provide. A dedicated analysis and evaluation agency could provide a focused and comprehensive EU effort to exploit the new opportunities fully, improving public services across the EU through the use of personal data.

**Public data?**

The providers of public services are among the major collectors and users of personal data.

Effective delivery of public services requires knowledge about individual characteristics, circumstances and preferences (for example, medical care requires detailed patient data). Public services also need aggregate data on what citizens want and use to plan, for example, education or transport provision. Furthermore, in its role as official record-keeper and to underpin its legal responsibilities, the public sector holds information such as voting registers, and birth and death certificates. Finally, it requires economic data to determine taxation levels, including income taxes and social security contributions.

Public services have held this kind of data for a long time, but the development of modern information and communication technology,
including the use of electronic records, has fundamentally changed what can be done with it.

The amount of data which can be held and accessed is now virtually unlimited. Once collected, the information can be stored cheaply, and easily copied and transferred. Different databases can now also be connected with each other, linking information on citizens held by a range of public agencies. Even data held by companies can be integrated into these databases, providing an unprecedented level of knowledge about individuals and the population as a whole.

**Use or abuse?**

This is raising fears among many European citizens. Some are worried about how this data might be used by governments to undermine personal freedoms in light of the current fight against terrorism or if, in future, ‘police states’ take control of such databases. The sharing of personal data between a range of public organisations also raises concerns: while we might be happy with our doctor holding information on our health, would we be equally happy if this information was easily accessible to other public sector organisations?

Citizens are also concerned about what happens when this data falls into the wrong hands, a fear fuelled by recent losses or thefts of data such as the personal details of 25 million people connected to child benefit payments in the UK. ‘Identity theft’ has become a much discussed topic in some countries.

In addition, many Europeans are worried about the extent to which companies might be able to access public data: could, for example, health and benefit records end up being used in employment or loan decisions? This fear is not unfounded – in some countries, public data already finds its way into the hands of companies, for example when voting registers are used in credit histories.

The way in which data is used will also need to be adapted to new modes of public service delivery. For example, in the outsourcing of health-care provision through public-private partnerships, the use and ownership of data is often a crucially important component of the contract. This information is not a side-product but essential to delivery of the relevant services, often in the hands of the private partner. In this kind of situation, as Lorna Stefanick has argued, “accountability, transparency and control over governments must not be lost in the face of high-profile
demands to enhance national security or due to more mundane pressures to increase administrative efficiency”.

**Improving public services**

While these concerns are significant – and often justified – collecting, storing and analysing large amounts of data on citizens is necessary to inform policy-making and service delivery.

As the Organisation for Economic Co-operation and Development (OECD) pointed out in a 2005 report: “In today’s complex and diverse societies, limitations on resources along with conflicting demands necessitate good decision-making and the setting of priorities...In order for both citizens and their elected officials to make choices that will best address the people’s needs, high quality, shared, accessible information about how the nation, smaller community or population group is doing on a variety of dimensions is absolutely essential.”

Working with the private sector is, in many areas, also a necessity – the public sector has to have access to private-sector data, expertise, products and services in areas such as ICT, pharmaceuticals or construction. Using data more effectively can also make public services more effective and efficient, and could have clear benefits for users if it means services can be customised.

Furthermore, large databases of personal data can be a powerful tool to combat fraud, making it easier, for example, to cross-check eligibility for social security benefits against personal incomes and assets. They can also be used to prevent, detect and combat crime, for example by monitoring suspicious monetary flows. The police and security services are increasingly being forced to adapt to the new knowledge society and, as a recent article in The Times pointed out: “The growing fragmentation and complexity of communications is hindering the ability to locate data which is an essential tool in tackling terrorism and organised criminality.”

Data can even be used to protect us directly from crime: the Professor Baker Report into the Harold Shipman serial murder case in the UK (where a family doctor killed more than 200 of his patients) concluded that statistics on death rates and drug prescriptions should be collated and analysed to a much greater extent to enable authorities to spot unusual patterns much earlier.”
It can also be used to identify and eliminate waste, for example by comparing the cost effectiveness of delivery at different locations and is becoming an increasingly valuable commodity which public services can use to raise revenue (by, for example, selling voting registers). The benefits of this may not be obvious to individual citizens, but it makes public services more productive, meaning they can deliver more for the same amount of taxes.

Detailed information on individuals also enables better targeting of public services, ensuring that only those who require support can access it, for example through means testing. Services can be targeted even more precisely using private data, for example by adjusting education programmes to target those most likely to benefit from a specific training course. This is where the real opportunities lie – by combining data evaluation with customisation.

Having this information available provides, for the first time, the opportunity to evaluate public policies extensively using real-life data, enabling public services to determine what works. For example, extensive data on how effective medication is for different age groups or when combined with other drugs, or how it interacts with lifestyles, goes well beyond what medical trials can provide. This could enable doctors to design treatment according to what works best for someone with a certain lifestyle, medical history and symptoms.

Being able to analyse and predict households’ consumption patterns and how they react to incentives such as price increases only becomes possible with large databases which show what people actually do (what economists call ‘revealed preferences’) rather than what they say they would do (‘stated preferences’). This is crucial in many areas where governments aim to influence individual behaviour to tackle ‘lifestyle risks’ (smoking, alcohol and obesity) or protect the environment (driving or recycling).

The public sector is also a major employer, and staff time is often the most important input in the delivery of public services. Employee data, combined with other information such as training and qualifications forecasts, can be used to plan services. Workforce planning is crucial to deliver services, for example to ensure that the right medical specialisms are available in the right locations. But the use of employee data can go further than this, for example to develop benefits packages tailored to individual needs to retain or attract certain rare skills.
This raises many concerns, not least the use of such information in performance assessment and pay, and using data more proactively in service delivery is also not necessarily welcome by all professional groups. But under certain circumstances, data-crunching by computers can help to plan and even deliver more reliable services than the individual touch of a teacher or doctor.

Where do we go from here?

We are still a long way away from these applications in most countries and most public services. Private-sector firms are starting to explore some of the possibilities, but the public sector is lagging behind and its ability to realise the full potential of the available data is much more restricted.

Safeguards are, of course, necessary, especially in the area of public services. Ownership and control of private data needs to be clarified. Where general services are concerned (i.e. those citizens cannot ‘opt out’ of), the public sector has a responsibility to safeguard this information. At the very least, citizens should be aware of how the information they provide might be used in future. They should also have the right to prevent their data being used in ways which they disagree with. For as The Economist has warned: “The hard lesson for governments is that citizens will adopt technology when it is both optional and beneficial to them, but resist it strenuously when it is compulsory, no matter how sensible it may seem.”

However, experience has shown that when individuals make abstract choices about data, they tend to choose data protection, but if they are personally affected (for example, by illness), they are much less likely to value privacy highly. Their attitudes also tend to depend very much on what the data is used for.

Making data available is also a key tool for citizens: for example, providing information about hospitals and doctors helps people to determine what they can and should expect from them. Realising this benefit will require a much greater use of existing data, but also requires stringent quality control and independence. For as the 2005 OECD report warned: “An over-abundance of data is readily available in the press and especially on the Internet.... because of the unprecedented range and number of sources available, users are unable to navigate through them or assess their quality: the final result is a certain degree of confusion.”

There needs to be a discussion at EU and Member State level of what data use should be allowed, and how it is assessed, analysed and disseminated.
Codes of conduct should be developed to ensure the public sector only uses this information in a way which is agreed and expected. However, knee-jerk prohibitions or attempts to slow down progress are not in the citizens’ best interest.

The 2008 Review of the Directive on Public Sector Information (PSI) Re-use provides an opportunity for the EU to put in place a regime which recognises how vital the availability of public-sector information is and, ideally, makes such data freely available in the knowledge economy.

The wider debate at the European level needs to move away from seeing ‘data protection’ overwhelmingly as a legal issue and towards a wider consideration of data as an asset, recognising the benefits of using private information to design and deliver better public services. The EU institutions should take a proactive approach by creating a framework and an agency which can take the lead in this area.

Fabian Zuleeg is a Senior Policy Analyst at the European Policy Centre.

Endnotes

2. OECD 2005 ‘Statistics, Knowledge and Policy: Key indicators to inform decision making’.
4. See http://news.bbc.co.uk/2/hi/health/1101480.stm
6. See for example http://www.guardian.co.uk/profile/michaelcross
eGovernment: data growth and growing concerns

Champions of eGovernment argue that it will deliver a ‘brave new world’ of efficient, effective and citizen-focused public administration. But is this really happening? This essay considers how information and communication technology (ICT) is being used to collect, store and share data, and what safeguards are needed to strike the right balance between innovation and regulatory regimes.

by Alexander Schellong

Are you in favour of more efficient and effective government? Of course you are. If one counted the reasons given most often for any type of government reform, these two would score the highest marks.

It is widely recognised that the characteristics of information and communication technologies (ICT) have strong impact on both. Government was thus among the first to utilise ICT. In the early days, punch-card machines were used for the census, and electronic databases replaced large amounts of data stored in non-digital form (for example, in files) throughout government once the technology was available.

Because information drawn from data is at the core of everything government does – analysis, decision-making or verifying eligibility for access to public services, to name just a few – the proliferation of databases, data mining and ICT in general is unsurprising.

However, it is this increase in databases, the kind of data being gathered, the way that data is protected (or rather the opposite) and the way it is used internally and externally, that have come under increased scrutiny and been criticised by many civil libertarians.

But the criticisms are not just about civil liberties. When governments implement ICT, outcomes vary. Large-scale projects such as the FBI’s Virtual Case File, the UK’s C-NOMIS or Germany’s FISKUS either failed completely or largely exceeded their estimated budgets, wasting billions of taxpayers’ money.

There are, of course, also successful projects but, by and large, the expected impact of eGovernment in moving into a brave new world of efficient, effective and citizen-focused government administration has not happened.
Understanding digital government

To understand the link between eGovernment and the collection, sharing and use of data, the following overview should help.

The use of ICT for internal and external government processes, fulfilling obligations and carrying out activities is called “electronic government” (eGovernment). In some cases, the terms eGovernance and eGovernment are used synonymously. However, eGovernance refers to the role of government in regulating (for example, adjusting property rights' laws to combat illegal downloading) and facilitating the growth of the information society and ICT (by, for example, funding schools' IT equipment).

Lately, the term digital government has been favoured by many researchers, because of the excessive use of letters like “e” (electronic), “m” (mobile), “i” (information) or “u” (ubiquitous) in government-related terms.

The following typology helps to classify our discussion of government technology initiatives (see also Figure 1).

The term eAdministration refers to the internal use of ICT – which might, of course, support the external use of ICT – which is subsumed under eServices. The use of ICT within the field of public participation in government, whether in voting or in the policy-making process, is referred to as eDemocracy. eGovernance can focus on government, society or the economy.

Following a common classification theme in eCommerce, eGovernment relationships are differentiated into three groups: Government to Citizen (G2C), Government to Business (G2B) and Government to Government (G2G).
G2G involves electronic exchanges between government actors at the unit, agency, local, state, federal or international level. Government to public servant relationships are a part of this spectrum. Transactions between government and business (of data, goods and services) are referred to as G2B. Examples are electronic public tenders or businesses making efficiency gains by integrating government-mandated processes into their value chains (for example, the automatic submission of statistics through a company’s accounting system).

In the case of G2C, government establishes or maintains a direct link with citizens in order to deliver information or services. Citizens may also interact with government as part of the political process (for example, eVoting), which might result in citizen to citizen (C2C) interaction (for example, public deliberation).

In addition to classifying eGovernment relationships, technology-based public service delivery can reach different levels of sophistication. The most common levels are information, one-way communication, two-way communication and full transaction (the stage when processes such as requests for building permits are fully digitised, so that there is no paperwork involved or any need for applicants to go to a government office).

The way in which data, databases and data mining are used in the three relationships outlined above differs from case to case. Moreover, the issues surrounding databases should be considered by government officials at the information stage when providing online public services.

For example, when the US Environmental Protection Agency launched its Toxic Release Inventory, some environmentalists claimed it would divert the agency’s limited resources from effective regulatory action. Others criticised the type and value of the information provided. Industry representatives were concerned about revealing proprietary business information or provoking unnecessary public alarm. In fact, media coverage and environmentalists’ initiatives increased once the data was made publicly available.

The power of ICT

ICT has characteristics that need to be understood before carrying out any impact assessment. These characteristics underline why digital data and databases will continue to grow in the future, and why it is necessary to find
balanced governance mechanisms for ICT, for the organisations they are embedded in, and for us – the individuals using them.

ICT allows information processing, coordination and flows to be structured without the common boundaries of roles, organisational relationships and operating procedures found in government. As a consequence, the relationship between information and the physical factors of organisational size, distance, time and costs are altered.

Digital information makes geographical dispersion irrelevant, allowing for new forms of collaboration and networks. Information technologies facilitate the speed of communication and more selectively control access to, and participation in, information exchange.

Interestingly, the standardisation, routinisation and formalisation of information sharing are not only technical requirements for shared databases to be effective; they are also typical traits of bureaucracies.

Organisational memory that was once hidden in non-digital forms or an individual’s memory can be stored, managed and analysed in digital form to improve knowledge or facilitate decision-making – helped by the fact that information storage, provision and search costs are virtually zero once information is digitised. Moreover, the human constraints of processing large quantities of information are reduced (for example, through the use of search engines), and software applications make it possible to combine and reconfigure data so as to provide new information.

This has been spurred by the rise of Web 2.0 applications such as social networking sites, mash-ups, tagging, and wikis, with the underlying philosophy that comes with it – i.e. mass collaboration and data sharing – further facilitating the growth of data.

The public has followed this trend on a scale that no one imagined. Younger people in particular store and share data about their activities, location, buying behaviour or personal lives like no other generation before, and periodic incidents of security breaches, identity theft and fraud have not reversed this trend.

Often, this behaviour is based on a conscious decision: millions of users joined corporate loyalty programmes (offered by, for example, airlines, hotels or shops) in return for personalised services, rebates or points that can
be used in various ways. People may also just be following an intrinsic desire to share and connect. Wikipedia is one of the prominent examples of the powerful force of collaborative peer production.

Data is also gathered and stored by companies in ways which customers are unaware of, but while the public has less control over the activities of companies, there is generally greater concern when government is engaging in these types of activities.

**The rise of government databases**

The counter argument is that governments do not gather more data; they are just gathering and combining data in new ways – for example, databases, biometrics, face-recognition software, remotely readable chips: radio frequency identification technology (RFID).

They do so for good reasons: national security, accountability, to provide better public services and to bridge organisational silos. Yet, since 9/11, more data is being sought indiscriminately rather than selectively, meaning that innocent people's data is included through law-enforcement agencies' screening processes.

Indeed, studies have shown that bigger DNA databases produce better results. This may argue in favour of creating a comprehensive DNA database containing information on all citizens and not just those convicted of crimes, as this may actually help to exclude suspects, save investigative resources and have a deterrent effect overall.

The automatic transfer of data about passengers flying from Europe to the US sheds light on another important aspect of the discussion on databases and data sharing. In a globalised world, should countries grant access to their domestic databases and how can they protect personal data beyond their national borders?

Incidents such as the day in November 2007 when the UK government managed to lose two CDs with unencrypted data of more than 25 million citizens underline four key issues relating to government databases.

First, the government has a mandate to protect the public's data. Second, data security is not only about technology. Thirdly, government needs strategies to manage digital trust. Finally, the characteristics
that make ICT so valuable (for example, the ease with which it can be transferred) mean there are increasing vulnerabilities and risks: that data will be shared when it should not be, or that it will be lost, stolen or misused. At the same time, there is a risk that data will not be available when it should be.

Paradoxically, calls for new government databases and better interoperability do arise when the system of government fails. Accordingly, new databases to track and monitor individuals and institutions, or links between formerly separate databases, are built.

Moreover, many ideas for creating proactive, multi-channel, one-stop and joined-up government simply do not work without databases. The volume of data to be collected will grow constantly in the near future as more government transactions are digitised, and cases of data being cross-referenced (‘mined’) will also grow as the relevant software improves.

Even if a government body decides to discard data, it faces many difficulties.

First, because data storage costs are continuously decreasing, governmental organisations prefer to keep everything, creating ‘data cemeteries’. The expansion in the volume and kinds of data maintained by agencies have made it almost impossible to maintain an inventory of resources.

Second, interim systems sometimes bridge the incompatibilities between the old and the new system, thus keeping the legacy system alive and increasing its overall complexity. For example, the US Internal Revenue Service launched a new software application to support a total quality management initiative, but never shut it down after the initiative ended. The amount of work it would take to resolve issues relating to data exchange with other systems were considered too high.

Moreover, these ‘electronic mounds’ accumulate massive quantities of rules that conflict with changes to other systems (for example, to control user access or behaviour, or ensure that different software applications can work together). The possibilities of storing and searching electronic information may also justify the development of large sets of these rules, so ICT does not always cut red tape. This is why some have proposed a combination of laws and technology to require and make it easier for data to be deleted – and thus “revive our society’s capacity to forget”.

53
Policy options

The expansion of databases puts greater burdens on the political-administrative-ethical calculus to strike the right balance between innovation and regulatory regimes. The following questions should be considered by policy-makers in the planning stages of initiatives that include setting up databases:

- What type of data should be collected and why?
- Who collects, maintains and owns the data?
- How is the data collected?
- How long should the data be stored?
- Should the data be shared and why?
- Who will be affected by making data more widely available?
- What impact will the data have on different stakeholder groups?
- Is the data aggregated?
- Is there a minimum opt-out provision for those who provide the data directly or indirectly?
- What security measures and policies are in place to protect the data?
- How can the data be accessed and changed by those who provide it directly or indirectly?
- How can accuracy of the data be ensured?
- How can the data be reviewed and disclosed?
- Do third parties who provide or use the data have the same security standards and privacy policies?

Policy-makers should also consider educating the public better on issues such as privacy and identity self-management – a process which may need to begin as early as in elementary school. They also need to understand how trust and the perception of security in digital government is created.

In any case, there will be many alternatives for government, businesses and the public to choose from when incorporating ICT into their lives. The perception of what is right and wrong will evolve alongside the values they are measured against, and the databases and techniques they are applied to.

Alexander Schellong is Senior Consultant at CSC’s Management Consulting Division and Research Fellow with Harvard University’s Program on Networked Governance.
References

Thank you for sharing your data

Companies are taking advantage of advances in information technology to find out much more about their existing and potential customers. In the emerging knowledge economy, data about existing and potential employees could also be an valuable asset. This essay explains why and how companies are collecting and using this information, highlights the potential benefits and risks, and considers the implications for policy-makers.

by Marie-Hélène Fandel and Joana Cruz

Phone books, census or election registers have long been an important element of companies’ marketing strategies. In some EU countries, public authorities are even allowed to sell citizens’ information. The Internet and the use of electronic payment systems mean most of our commercial transactions are now recorded, as are people’s movements in public places and shops – not only for security reasons, but also to study their behaviour in stores. All this has fuelled fears that we live in an Orwellian society in which we are being permanently watched.

The ‘terabyte’ revolution is allowing super computers to capture and store massive amounts of information. This information has become the object of major analysis through data integration and data-set merging techniques. Information found in phone books (geographical location), census (gender, age, marital situation, household composition) or election registers (voting patterns) can now be matched with credit card information (consumption patterns and preferences) and web browsing (what you buy, when and in what order).

New technologies allow companies to link data and obtain a detailed profile of their customers’ behaviour and preferences, making it possible to draw a very accurate picture of each customer and his or her shopping habits, and even to predict future spending patterns.

Should individuals worry about their personal data being used by companies? Some argue that this is leading to an erosion of privacy and warn that the information can be misused, particularly when children or the elderly are targeted. But others insist it can have significant advantages for consumers, allowing them to get better service through personalised solutions, and may even benefit their health and wealth.
Why and how are companies collecting data?

Data, and data analysis, has flourished in the information society and has become a major commodity in the knowledge economy.

Customer preference data is enormously valuable to help companies gain a competitive edge. Knowing their customers opens up significant opportunities for growth: making it easier, for example, to predict demand and eventually reach a bigger market. On the basis of their knowledge of individual customers, companies can also divide a market into sub-categories (market segmentation) and build consumer profiles in order to offer them tailor-made goods and services.

One way of using this information is to offer products at differentiated prices: companies can use customer data to assess how much different groups can afford – and are willing to pay – for a specific product, for example, on the basis of where they live and what they earn.

In competitive markets, this is positive for consumer ‘welfare’ as it may enable low-income households to buy products that would otherwise have been beyond their reach. But in uncompetitive markets, market players dominant in a specific category of products or services may decide to charge customers inflated prices (beyond what they can afford) with the aim of making ‘abnormal profits’.

Data mining

The emergence of ‘data-mining’ techniques has significantly pushed forward the frontiers of data analysis. Data mining involves using data analysis to identify and ‘extract’ patterns and correlations in a large data-set. Such techniques can help companies serve customers better by adapting more quickly to changes in their preferences at various stages in their lives (going to university, getting married, having children, or winning promotion).

They can help to determine, for example, which health insurance best fits an individual or family’s needs, or to find better ways to meet those needs. In the health arena, for example, there is huge potential for better EU-wide data collection and analysis to improve understanding of patients’ medical histories, conditions and relevant treatment. This is, however, inevitably a very sensitive topic, particularly as regards the potential commercialisation of health data when healthcare is provided by the private sector.
Data analysis is also increasingly being used to improve the operation of a company, for instance to prevent delays or malfunctions, and respond to unforeseen events.

**Winning the global ‘war for talent’**

In the future knowledge economy, competitive advantage for companies will not only come from exploiting data to improve the goods and services they offer. Firms will also increasingly use data in relation to their human resources as part of their efforts to ‘win’ the global hunt for talent, as they compete for the ‘brightest and best’ workers in a dwindling labour pool.

Such data could be used in a negative sense to weed out ‘undesirable’ applicants by merging information provided by applicants during the interview process with all other information which might be available on the person concerned, ranging from previous job experience to criminal convictions. It could also cause problems if this information was used to draw unjustified conclusions: for example, assessing the likelihood that a candidate will take sick leave on the basis of information about his or her personal life.

However, on the positive side, companies may also begin collecting and using such data to provide customised services to attract high-skilled workers. The human capital embodied in a firm’s workforce is a crucial factor for success, and they will have to be increasingly proactive to attract and retain individuals who have the potential to add significant value.

To do this effectively, they would need much more information about their staff and potential recruits. This data could be used to determine, for example, what type of benefits will attract and motivate certain groups of potential or existing employees, such as skilled ICT workers, and what might motivate individual employees or potential recruits. For example, if a potential employee has children of school age, offering access to high-quality schooling could give a company a competitive edge which will make him or her choose to join one firm rather than another. Companies might even start to offer ‘fringe’ benefits such as in-house childcare which could have a big influence on an individual’s quality of life.

This, of course, raises numerous questions about how much companies should be allowed to know about their workers – and what they do with that information.
Data hunters and gatherers

As already pointed out, companies have already accumulated large databases on their customers. This has been done in different ways: by, for example, asking customers whether they would like to share their personal data for the company’s internal use (usually by ticking the appropriate box after reading the firm’s privacy policy); by carrying out customer satisfaction surveys; or by offering discounts, vouchers and loyalty cards. Customers will often agree to provide a great deal of information about themselves for even a tiny discount, without asking who will be using that information, where and for what purpose.

Companies can also collect data by simply buying it from public sector services (for example, voter registers). The German City of Bochum has generated revenues totalling some €220,000 a year through the (legal) sale of information contained on municipal registers.¹

Data can also be bought from firms specialising in the data-trading business, accessed through public-private partnerships (PPP), or acquired just by looking at individual credit card records. The question is how and when someone will have access to that data.

The information society and Internet have also opened up new, indirect ways of getting data without an individual’s consent. ‘Data hunting’ is a more pernicious form of data collection: an individual’s personal information is collected simply by using ‘cookies’ – a tool that allows for the identification of a user’s Internet browser. Users are assigned an identification number for each page they visit on the web, which gives companies the capacity to analyse users’ journeys through the pages of their websites.

Companies can thus proactively retrieve information on what, when and in which order users have visited their pages, and deduce from this what they were looking for and for what purpose. Internet ‘traffic’ is closely scrutinised by companies to track Internet users and potential customers’ preferences – and this is often done without the user knowing anything about the existence and role played by ‘cookies’.

‘Data scraping’ is a technique whereby companies proactively look for data. A bank might, for example, want to search court records for any information relating to a customer awaiting approval for a loan. Social networks and online content can also allow companies to use ‘word of mouth’ technology
to approach customers through peer groups, chatlines and social networking websites. Social networks are ‘manna from heaven’ for online advertisers and data hunters, providing access to a complex nexus of social interaction and social data that can be stored and analysed.

Companies can also provide better services to their customers through the use of personalised filters through which shoppers recommend products to other shoppers. Collaborative filtering works by association and provides information on what shoppers with the same taste have purchased (those who bought X also bought Y). This technique has been used very successfully in promoting films, books and music.

**What are the risks?**

Using the Internet and information technologies to buy what we need or want has become, for many of us, an everyday experience. But although consumers have thus been freely supplying information about their consumption preferences, they have not always been aware of the extent to which this information is used.

Such large databases can, if used for the right purposes (i.e. those customers agree with), be a real asset to improve the goods and services offered to the public. But used against their will, it poses a real problem: what happens if things go wrong? There are questions, for instance, about the quality of the information held on an individual. Is the information accurate? Has it changed? And if not, who is checking to see whether it needs updating? There are currently no ‘personal data auditors’ – but there might well be in future.

In the knowledge economy, consumers need to be empowered. They will probably increasingly request access to their personal information and, while they might not always be able to consult their ‘file’ in its entirety, they might well be in a position to correct any misleading information. This will probably become a key consumer right in the future knowledge economy.

As noted above, however, data collection does not currently always presuppose a customer’s approval. Data hunters in particular will seek information on the Internet and use it in ways the individual is unaware of. There is an asymmetry here, as customers do not know how much information companies have on them and companies have no obligation to release this information.
In a rapidly changing industry, competition can ensure that companies do not cross the line, as a scandal over how a firm uses personal data could hit it hard. But with market consolidation, we could end up in a situation where a majority of individuals use a single provider for Internet research, e-mails, their work calendar and social networking. In this context, can abuse of dominant position be prevented? And is Europe equipped to do so?

Handling the challenge of data protection

The EU as a whole has a fairly strict data-privacy regime compared to other regions in the world and, within the Union, some Member States (for example, Germany) have decided on an even stricter approach. But by restricting the amount of information that can be collected, are they also restricting access to new opportunities? Should policy-makers not focus instead on protecting individuals against potential abuse?

In the knowledge economy, data and data analysis will increasingly become a commodity and an asset. That information on individuals is being collected is not new. What is new is the speed and the ease with which companies can identify present and future individual preferences. With infinite computational and storage capacity, there is theoretically no limit to understanding consumer behaviours, predicting and influencing them.

New technologies constantly outpace existing safeguards, and traditional regulatory modes have proven insufficient to protect individuals. A restrictive regulatory backlash therefore risks preventing Europe from taking advantage of the many opportunities opened up by data-mining techniques while doing little to improve consumer protection.

Europe therefore needs to quickly adapt its data protection approaches to the challenges and opportunities provided by data mining. Digitalisation might have meant the end of privacy as we have traditionally known it, but it has also paved the way for a more sophisticated economy based on personalised products and services.

Marie-Hélène Fandel is a Policy Analyst and Joana Cruz a former Programme Assistant at the European Policy Centre.

Endnote

Big Brother in practice?

Companies in some sectors are increasingly being required by law to store customer data on the grounds that it may help in the fight against terrorism and crime. These essays examine the impact of these requirements on two of the sectors most affected by such legislation – the airline and telecoms industries – and highlight the problems they face in complying with these growing demands.

Passenger information: the new growth industry

by James Forster

How would you like your eggs this morning? Poached, boiled, fried or scrambled?

Hungry diners sitting at breakfast tables are familiar with waiters trotting out these lines. Restaurants are equipped to satisfy their customers when it comes to this fare. The same cannot be said for the airlines when asked by governments for passenger data: airlines are not equipped to provide data in different ways and they should not have to do so. Yet, notwithstanding the development of international guidelines on the provision of passenger information, that is exactly what is being demanded of them.

Since 9/11, passenger information has become a growth industry for many governments. The authorities claim that data is required in order to secure their countries’ borders, reduce illegal immigration and mitigate threats of terrorism.

Two basic types of data can be required:

1. Advance Passenger Information (API), which is basically passport biographical information and is generally collected at check-in and sent when the flight departs. To date, around 20 countries require carriers to send them API.

2. Passenger Name Record (PNR), which is information held in the airlines’ reservations systems. It is required by fewer countries, and can be obtained several hours and sometimes days in advance of the flight’s departure time. Providing this data has proved somewhat controversial, as the records can include data of a personal and sensitive nature: for example, payment details, medical conditions and special dietary information.
Airlines reacted quickly in the knowledge that more and more governments would be demanding data, and are well-prepared.

The International Air Transport Association (IATA) drove forward the campaign for international guidelines, and IATA, the World Customs Organization (WCO) and the International Civil Aviation Organization (ICAO) have agreed guidelines which recommend that the international UN/EDIFACT PAXLST message standards be adopted by countries requiring API. These recommend not only the content of the message, but also the format by which data is to be transmitted. In respect of message content, it is recommended that this be limited to that which can be captured by automated means; for example, passport swipe readers.

Unfortunately, the United States has gone further and demands additional data such as ‘country of residence’ and ‘address whilst in the USA’. Other countries have asked for personal address information.

Not only do the differing data requirements complicate life for customers; they also result in expensive reprogramming of airline computer systems that collect and generate the API messages. In the case of British Airways, software upgrades are required to our mainframe check-in system (DCS) which generates the API message, and to our remote check-in facilities, for example, self-service kiosks and BA.COM, the British Airways website.

To date, it has been standard practice – reluctantly I might add – for airlines to cover the costs associated with collecting and transmitting the data.

Most governments are content to receive the data in the standard UN/EDIFACT format and incorporate it at their expense into their own systems for analysis. However, this year India announced that it required the data in flat file format, and negotiations continue with Cyprus about their request for API in yet another form.

Airlines have a choice between developing their own systems to meet these demands for non-standard formats or contracting out the work to a third party to translate the messages from UN/EDIFACT to flat file. Either way, additional expenditure is involved and yes, you guessed it – the governments look to the airlines to cover these costs.
Currently, PNR data is only required by four countries: Australia, Canada, the UK and USA. PNR data is normally sent to the authorities by yet another message – this time from the reservations system.2

Transferring data to third countries outside the Union can breach the EU’s Data Protection Directive and national legislation. As a consequence, the EU has drawn up agreements with the countries concerned which are designed to protect the consumer by, for example, placing restrictions on how the data is used and for how long it can be stored.

The Association of European Airlines (AEA) supports the so-called ‘Austrian solution’. Under this vision, airlines would provide their PNRs to a central European database, managed and financed by the Union. The system would clean or filter the data and provide it as required to both EU and non-EU countries.

Time will tell whether or not the Union will support this proposal. Airlines are in favour of it, as they would only have to provide their PNRs to a single addressee and concerns about data protection would be allayed.

Providing PNR data should be straightforward, but it is not. The authorities have defined this data by listing a number of elements they require. Whilst some states require all of the data, others request only a limited set. Some include pure reservations data such as the method of payment and contact details, but others also want details captured at check-in; for example, baggage tag numbers and seat assignments.

This is fine for carriers that operate a common reservations and check-in system, but many airlines – including most of the major EU carriers – operate separate reservations and check-in systems. These airlines are faced with another challenge and yet more expense: how to transmit the PNR data held in their check-in systems? Some carriers have yet to answer this question.

Oh, by the way, I’d like my eggs scrambled - it just seems appropriate!

James Forster is Manager Facilitation, Government and Industry Affairs, British Airways plc.

Endnotes

1. Australia, Kuwait, the UK and USA require this data prior to departure.
2. IATA is working towards a standard for PNR data messages.
The telecoms sector and the Data Retention Directive

by Caroline Persson

In recent years, we have seen an increasing demand – not only from governments but also from Internet security companies and rights holders (in the music and film industry) – to force new legislation onto the telecoms industry, imposing more obligations on companies relating to the collection, storage and retention of data about our customers for all sorts of purposes.

However, it must not be the role of the telecoms sector to enforce the law. That task must remain with the regulatory authorities and judicial system in order to ensure that proper procedures are followed and that our customers’ right to privacy is duly taken into account.

It is, of course, true that BT and other telecoms companies hold essential customer data for billing purposes, and of course we adhere to the data protection and privacy laws, as well as helping the relevant authorities in the countries in which we operate. What is not true, contrary to what some privacy lobbyists may claim, is that telecoms companies want to store more data than we currently do.

However, one concrete example has forced BT and all other electronic communication providers in Europe to do just that – collect and store data (call and Internet records) on our customers for up to two years, supposedly in order to give countries more effective means to address potential terrorism threats and other serious crimes by monitoring traffic data.

The Data Retention Directive,\(^1\) which was controversially adopted by the EU in March 2006, can serve as a good case study for a new, additional obligation to collect more customer data in order to better please governments.

Controversial to say the least, this Directive goes further than previous legislation and beyond current practices (and let us not forget that telecoms companies like BT already have a track record in, as well as a duty to, assist the judicial authorities in their quest to tackle all sorts of crimes and injustices).

Its adoption was also controversial, as many MEPs and indeed civil rights groups, did not agree with the Member States that this new tool was justified. MEPs worried not only about a possible invasion of the public’s privacy and the increase in state surveillance but also about the burden placed on
telecoms companies (not to mention the cost incurred, which in the end may be passed on to the customer, in order to comply with this new Directive).

Another worry which united MEPs and telecom operators was that rights’ holders (the music and film industry) wanted the telecoms industry to store more data and be more closely involved in policing the network for copyright infringements – that is to say that data retention should not just be about fighting serious crimes and terrorism but about tackling copyright infringements as well.

All this is now history: after a series of hiccups, the Directive was passed, with the European Parliament and Council reaching an agreement under the so-called “co-decision procedure”, which led to additional requirements being introduced.

The Data Retention Directive seems to be a part of a general trend, whereby governments want more and more personal data to be captured (is this indeed the emergence of a Big Brother society?), forcing the telecoms industry in particular to get involved in this through onerous, sector-specific legislation.

BT, and the telecoms industry in general, believes that a balance must be struck between protecting the general public and the right of privacy for the private individual. Governments need to consider whether there really is a need to collect and store personal data before legislating.

The Directive obliges telecoms companies in Europe to store and retain customer data relating to: the time and duration of calls (fixed lines and mobiles); caller location (mobiles); details but not the content of Internet Protocols (hence both services like Voice over Internet Protocol (VOIP) and e-mails); and details of unsuccessful calls.

All of this data has to be stored and, upon a request from relevant judicial authorities, handed over within a strict timeline. The Directive stipulates that the data must be retained for a period of no less than six months and no more than two years.

However, as this is a harmonising Internal Market measure, it is up to the Member States to implement the EU Directive in their national law and this may lead to differences in the retention periods as well as diverging approaches with regards to cost recovery for the telecoms industry. (The UK and some
others will seek to reimburse companies, but other Member States will not, thus creating an uneven playing field for European telecoms operators.)

So what is the state of play, at the time of writing, with regards to this Directive? Interestingly enough, not all Member States have implemented the legislation as yet – in fact, only a small number of the 27 Member States have done so, even though the deadline for transposing the Directive was 15 September 2007. This, of course, leads to a tricky situation where telecoms companies have to adopt different strategies and timings for complying with the law across the EU.

As the Directive granted a grace period (up till 15 March 2009) for tackling Internet access, Internet telephony and e-mail, these issues are being elaborated by an expert group comprising telecoms and Internet service providers’ trade associations, and national law enforcement agencies/Member States under the auspice of the European Commission.

As BT and the telecoms industry across Europe strive to track legislation in Member States, seeking to ensure that the right procedures and systems are put in place in order to comply with the Data Retention Directive, this story has taken an interesting twist which could lead to the abolition of the legislation or to it being annulled.

All our efforts to comply with this additional legal requirement pertaining to capture and storage of customer data may be overturned, because of a complaint filed by the Irish government against the Directive with the European Court of Justice in 2006.

The Irish do not disagree with the principles of data retention that the Directive establishes. Rather, the case relates to the procedures used to introduce this new legal instrument. It is argued that the Data Retention Directive should not have been discussed as a harmonising Internal Market Directive under Article 95 of the Treaty but rather under the EU’s ‘third pillar’, which is how other Directives concerning criminal law matters are dealt with.

This would have meant following a different legislative procedure and would have changed the voting requirements for approving the legislation in the Council from qualified majority voting to an absolute majority of all Member States.
In conclusion, regardless of the merits and the effectiveness of this instrument, it is fair to say that the uncertainty over its legal basis, as well as the costs incurred by the telecoms industry and our customers, are not good for business – big or small.

Caroline Persson is a European Policy Adviser at BT.

Endnote

Journalists under pressure in security-conscious Europe

Since 9/11, many countries have adopted laws restricting free speech on grounds of national security. This essay argues that while concerns about potential terrorist threats are legitimate, they have led to substantial and disproportionate attacks on civil liberties which have weakened the scope for investigative journalism, exacerbated by paranoia in the media which is leading to worrying levels of self-censorship.

by Aidan White

In the face of the so-called ‘war on terror’ – although the phrase has fallen from everyday political use – a culture of routine official surveillance of citizens, and particularly journalists, has developed across much of Europe.

The United Nations Special Rapporteur on Freedom of Expression has noted that since the 9/11 terrorist attacks on New York and Washington, many countries have adopted laws that undermine freedom of expression. Restrictions on free speech have multiplied, very often on grounds of national security.

The fear and threats of violence are particularly acute in countries like Denmark, Italy, and Poland – supporters of the United States-led military coalition in Iraq. They fear they may be the next target after Spain and the United Kingdom, following the 2004 Madrid train bombings, which killed 191 people, and the 2007 London bombings, in which 56 people died.

These concerns are legitimate, but there is growing concern that they have led to substantial and disproportionate attacks on civil liberties which have weakened the scope for watchdog journalism.

Evidence of this comes in the findings of the International Federation of Journalism (IFJ) Report Journalism, Civil Liberties and the War on Terrorism, which concludes that: “The war on terrorism amounts to a devastating challenge to the global culture of human rights and civil liberties established almost 60 years ago.”

The report, based upon an analysis of current policy developments as well as a survey of some 20 selected countries in Europe and elsewhere, found that around half of the minimum standards set out in the Universal Declaration of Human Rights are being undermined by the war on terror.
It concludes that the response by governments to the threat of terrorism is out of proportion, noting that journalism suffers in a “pervasive atmosphere of paranoia” which is leading to dangerous levels of self-censorship, while dissent inside and outside media is being restricted.

**Government laws to hobble media freedom**

In this climate, there have been numerous attacks on journalists’ rights. States have put in place new laws concerning “glorification of terrorism,” or “radicalisation of young people” that are vague and potentially harmful to free expression.

In 2006, evidence emerged of systematic spying on journalists by security officials in both the US and Germany. On 15 May ABC News, quoting a senior federal law officer, revealed how the US was tracking the telephone numbers called by the network’s reporters in an effort to root out confidential sources. The scrutiny of US media – which included the New York Times and the Washington Post – was part of a widespread CIA leak investigation following media reports of the secret US prisons in Romania and Poland.

On the same day, Germany admitted that its federal intelligence agency had been spying in news rooms and paying journalists to reveal their sources. The government was forced to pull its agents out of German media after it was revealed that correspondents were under surveillance to stop leaks to the press. Some had even been paid by the security agency, the Bundesnachrichtendienst (BND), to spy on their colleagues.

To many reporters and media support groups, it is unconscionable that journalists in the heartlands of European democracy should be spied upon, that security services should be using paid informants inside the media, and that journalists’ telephones should be routinely tapped.

Reporters need to follow their stories, sometimes putting themselves at risk, and they need to talk to people who can speak with authority for dissident and opposition groups. Without access to diverse sources of information, stories are only half-told and people who run the institutions of state are unaccountable.

In recent years, new laws have been adopted across Europe containing vague and wide definitions of “terrorism” which can be used to stifle political and social protest and legitimate journalism.
The UK provides a good example. The last ten years have seen the introduction of ever-stricter laws, with a broader definition of what constitutes “terrorism”.

A particular problem has been the banning, in the 2006 Terrorism Act, not just of direct incitement to terrorism, but also of anything that can be interpreted as “indirect encouragement” of or “other inducement” to terrorism, including – in some circumstances – glorification. This inhibits valid media-led discussion and has a detrimental effect on community relations.

Although it is fundamental to the guarantee of free expression that any restriction for the purpose of national security, including preventing terrorism, has to be closely linked to preventing imminent violence, these new laws have been used too arbitrarily by the authorities.

The arguments of journalists and civil liberty groups that there are already laws in place to deal with incitement to violence and that new regulation will only encourage further interference in the media’s work were largely ignored.

In 2005-2006, the anti-censorship group ARTICLE 19 cited a number of examples of how the law was being used to curtail rights. Among these was the detention of more than 600 protesters during the 2005 Labour Party conference, including, famously, the detention of an 82-year-old activist evicted from the conference for heckling; the stopping and searching of an 11-year-old girl who participated in a peaceful protest at an RAF base; and the arrest of trainspotters at Motherwell, Reading, Slough and Croydon railway stations.2

Anti-terror legislation in Denmark, France and Spain also criminalises the justification or glorification of terrorism.

Some 40 countries have signed up to the Council of Europe Convention on the Prevention of Terrorism, which came into force on 1 June 2007, requiring governments to criminalise ‘provocation’ of terrorism. This is defined as the “distribution, or otherwise making available, of a message to the public, with the intent to incite the commission of a terrorist offence, where such conduct, whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed”.

Free-speech advocates counter that international standards already limit restrictions to free speech on the grounds of national security to when there is a direct and immediate connection between the expression and the likelihood or occurrence of such violence.
But the rhetoric of anti-terrorism has become ever-more strident and has created a difficult atmosphere for media, who say there is more pressure on journalists to reveal their sources of information, even though the principle of confidentiality is protected by the European Court of Human Rights.

**Journalists victimised**

In many European countries, for instance, reporters have been victimised for publishing information that embarrasses the government. In Denmark, France, Germany, Ireland, Latvia, the Netherlands and the UK, the authorities have used court cases or surveillance – both legal and illegal – to uncover journalists’ sources.

Two Dutch journalists spent two days in jail in November 2006 for refusing to reveal their sources in a case against an agent suspected of leaking secret Dutch intelligence service files.

Bart Mos and Joost de Haas, veteran reporters for the Netherlands’ largest newspaper *De Telegraaf*, were detained – the journalists’ association says they were “kidnapped” – when they refused to name their sources. No one questioned the truth of their information, but the incident led to a widespread protest in the Netherlands led by journalists’ unions and media owners.

Two cases in Denmark and Germany tellingly expose the growing unease in relations between government and media.

The prosecution in Denmark in 2006 of three journalists accused of breaching national security by publishing information about the government’s handling of policy related to the invasion of Iraq was unprecedented and shocked the media establishment in a country rightly proud of its free press traditions.

In a series of articles published in February 2004, the daily newspaper *Berlingske Tidende* quoted excerpts from Danish military intelligence reports which denied the availability of credible information on the existence of weapons of mass destruction in Iraq before the March 2003 invasion by British and American troops. The existence of such weapons was the principal argument vigorously put forward by Prime Minister Anders Fogh Rasmussen to justify Danish support for the war.

The journalists who broke the story, Jesper Larsen and Michael Bjerre, were first arrested in April 2004 and charged under the Criminal Code.
What press freedom groups and journalists found curious about the investigation was that there was no suggestion that the information itself was inaccurate or, indeed, that its publication posed any credible threat to Danish citizens or the country’s military. But the story embarrassed the government by exposing the paucity of arguments to justify going to war.

In the event, the court cleared the journalists in 2006, but the question remains whether this prosecution would ever have happened were it not for a new order of politics which has lowered regard for fundamental liberties in favour of political self-interest.

In Germany, too, journalists have the courts to thank for reaffirming the rule of law and old-fashioned democratic values in the face of press violations by the authorities.

The German Federal Constitutional Court intervened to shield media from the security services after the 2005 raid on the editorial offices of the monthly news magazine Cicero in Potsdam. In April 2005 the magazine had published an article on the Islamist terrorist Abu Musab al-Zarqawi which quoted a top-secret report from Germany’s Federal Criminal Police Office (BKA). Not long afterwards, the magazine’s offices were raided and searched.

The magazine filed an official complaint that the search had violated press freedom as guaranteed in the German Constitution and argued that when BKA officials searched the magazine’s editorial offices, they were on a fishing expedition to figure out who passed on the top secret document – in clear violation of the reporters’ right to protect their sources.

House searches and seizures like the one at Cicero have increased in recent years, according to the German Journalists Association (DJV), which has reported 187 cases since 1987. The charge, says the DJV, is always “inciting or participating in the disclosure of secrets”. This line of attack intimidates and deters the press.

Despite a number of rulings designed to firm up the boundaries of press freedom in Germany, laws on the country’s statute books still make it possible to leverage journalists to reveal their sources. The authorities now feel confident in using these rules to put pressure on media.

As a result, journalists face the prospect of prosecutors and investigators roaming around their newsrooms demanding to know who they have been
talking to and about what. In this way, the law becomes a tool for intimidating journalists.

In February 2007, the Constitutional Court came down on the side of press freedom in the Cicero case, finding that “searches and seizures in investigations of members of the press are unconstitutional if their sole or chief purpose is to ascertain the identity of an informant”. Nor is it justified, said the judges, to search newsroom offices solely on the grounds that official secrets have been published. The case for exempting journalists from section 353b of the Penal Code appears to be unanswerable.

Nevertheless, this changing mood has forced journalism onto the defensive across Europe. Journalists insist that it is not their job to help the state keep its secrets. Indeed, a free press should make it more difficult for the government to keep secrets, particularly when – as in the Danish and German examples – there is an overriding public interest at stake.

But governments increasingly beg to differ. The increased surveillance of journalism by reinvigorated security agencies comes as new anxieties emerge within communities over immigration and failing economies contribute to weakening the public attachment to rights. Surveys last year found that 80% of Danes supported new laws to combat terrorism and control immigration and, in Britain, 73% of people polled by the Guardian newspaper said they were willing to give up some civil liberties to improve security.

Media themselves, though, have not helped themselves in this changing climate of opinion. Too often, the images and words used by television and the popular press follow a pattern of sensationalism and opportunism that undermines public confidence. They often reinforce stereotypes and prejudice rather than encouraging notions of engagement and value-based dialogue.

The current existential crisis of media – caused by the advance of the Internet, changing consumer habits and the breakdown of traditional market models – has led to widespread cuts in editorial spending, and quality journalism in Europe has suffered as a result.

The responses to these worrying developments have come from within journalism and other civil society groups. In 2005, the European Civil Liberties Network was launched, bringing together groups working on associated issues, such as, legal rights, media freedom, refugee and migrants' rights, globalisation and peace.
In November 2007, the European Federation of Journalists led a coordinated series of actions in European capitals to protest over new threats to journalism. During 2008, media organisations and journalists’ groups were sufficiently concerned about governmental attitudes to bury their differences and to prepare a joint statement in defence of media freedom in Europe.

They argue that freedom of the press is not a right to be enjoyed only in calm and tranquil times; it must be tested in the turbulence and anguish of stormy events, and particularly when democracy and its institutions are under fire. Contrary to what many political leaders think, independent journalism and press freedom are an advantage, not a handicap, in a crisis, as the history of conflict in Vietnam, Algeria or even Northern Ireland demonstrates.

So long as governments seem focused on monitoring and limiting the scope of journalism in Europe, they make matters worse. They lower morale and create an atmosphere of secrecy and uncertainty in society, and they encourage self-censorship – a pervasive and self-denying process. They make the seeking of solutions more difficult, not easier.

Aidan White is General Secretary of the International Federation of Journalists.

Endnotes

III. WHERE DO WE GO FROM HERE? THE IMPLICATIONS FOR FUTURE POLICY-MAKING

Warm words and colds acts: the future of policing and judicial cooperation

The Lisbon Treaty includes reforms to ‘communitarise’ policy-making in the justice and home affairs arena. But this essay argues that there is unlikely to be an outburst of legislative activity in this area, with or without the Lisbon Treaty, and that any proposals will continue to spark fierce political battles, not least because of the highly sensitive nature of the security versus liberty debate.

by Damian Chalmers

The Lisbon Treaty was meant to be all about institutional reform rather than policy innovation or competence creep. Its predecessor, the Reform Treaty, was even identified as such by its title. Yet the Lisbon Treaty was also about unfinished business – and the great unfinished business since the final moments of the Maastricht negotiations has been the unification of the first and third ‘pillars’ of the Treaty on the European Union.

This was partially realised in the Amsterdam Treaty with the transfer of immigration, asylum and visas to Title IV of the EC Treaty, but has only been fully accomplished in the Lisbon Treaty.

The excited pitch of both advocates and opponents of this extension of the ‘Community method’ to policing and judicial cooperation in criminal matters assumes it is just that: i.e. that this policy area will be legislated and adjudicated upon in precisely the same manner as pre-existing Community fields, be they agriculture, transport or the Single Market, if and when the Lisbon Treaty comes into force.

After discussing the formal changes, this essay will suggest that this ignores the politics of this policy area. Issues of civil liberties, public security and administration of justice do not lend themselves as easily to the same institutional alignments, policy communities and deals as the regulatory politics that are the Community’s bread and butter.
As if this were not enough, deal-makers will find the process a great deal more hog-wired than they would like. Courts police this field particularly intensely and, unlike other initiatives, institutional reform in this area is not taking place to realise a new policy agenda but rather to pursue the well-established one set out in the 2004-2009 Hague Programme for Justice and Home Affairs.

What does this mean? If the Lisbon Treaty does come into force, the politics in this field are likely to be more contested and bitter than in any other area of EU law-making. The saliency of the issues, the heterogeneity of the parties – intelligence agencies, courts, supranational institutions, and national ministries – and the constraints on what can be easily agreed will lead to a polarisation which might prove particularly intractable.

The reforms introduced by Lisbon provide for the current co-decision procedure to be the central law-making process for policing and judicial cooperation in criminal matters. It will cover, among other things, rules on:

- the mutual recognition of judgments and evidence;
- the rights of victims in trials;
- the definition of criminal offences and sanctions for ten serious types of crime;
- the regimes governing both Europol and Eurojust;
- policing facilities involved in the collection and storage of data, common investigative techniques and training.

Alongside these, there are areas in which the European Parliament is not just given a veto, but also has actively to consent before a measure can be adopted, most notably for the establishment of a European Prosecutor’s Office, and the definition of criminal offences other than those outlined above. Parliamentary powers are only marginalised in relation to rules governing operational activities of law-enforcement agencies.

This is a far cry from the intergovernmental pattern currently pervading this field. It lends itself to the aspiration of the legislative settlement which pervades much EU law-making, whereby the Parliament rarely exercises its veto but has established significant influence over the process through the dominance of its power to amend Commission proposals and its involvement in joint trialogues.

These hopes are likely to be frustrated. The Parliament’s success has lain in part in industry, civil society and national governments dissatisfied with a
Commission proposal beating a path to its door. These are not available in the same way in this area. To be sure, there are civil liberties’ groups, but otherwise one does not find the same array of policy communities or advocacy coalitions that can supply expertise or wider support to the European Parliament.

The other feature of this field is that agenda-setting has traditionally been governed by dense cooperation between interior and justice ministries. The formal power of proposal may now lie with the Commission, but one would expect these ministries to exert strong influence over its initial consultation and impact-assessment procedures and over its relations with the Council. Indeed, by the time a proposal reaches First Reading in the European Parliament, coalitions and majorities in the Council may be very firmly entrenched.

If proof of this is required, one only need look at the Prüm Treaty, agreed in 2005 between Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Spain, to allow their police forces easier and more wide-ranging access to each other’s databases – which was, in 2007, cut and pasted verbatim into a Council Decision.

If the Parliament’s influence over legislative content might be diminished by its institutional position, a further factor curbing its power has to do with the politics of criminal justice and policing.

This is a policy area where it is less easy to ‘cut the difference’ than in market regulation and where any attempt to do so would be poorly viewed by the public. One cannot, for example, spilt differences through backroom deals on whether a man has to be aware of a woman’s lack of consent for it to be rape. As such, Commission proposals have a much stronger ‘take it or leave it’ quality.

All this will lead to a greater oppositional politics in which the avenue for the Parliament to exercise its power will be, increasingly, through use of the veto or litigation against a measure. Indeed, there is some evidence of this already happening in the field of Justice, Liberty and Security, where the Parliament has already challenged a number of high-profile measures before the European Court of Justice (ECJ).\(^1\)

Political context will also matter. The mood music is not propitious and suggests that agenda-setting will have a lowest common denominator tone rather than being characterised by proactive collective problem-solving.
First, the Lisbon Treaty places a number of constraints on decision-making. A feature which differentiates this Treaty from the Constitutional Treaty is that national security is stated to be the exclusive preserve of the Member States. Alongside this, the brake procedures set out in the Constitutional Treaty are retained. These provide that where any Member State feels that an EU measure touches on a fundamental aspect of its criminal justice system, the matter is to be referred to the European Council.

To be sure, there is a lack of clarity about what these concepts mean and purists will argue that both caveats could be subject to possible erosion before the ECJ. However, their insertion both casts the shadow of a veto over any measure and provides a bulwark for a national government to argue against any measure.

Secondly, it is not clear that Lisbon would prevent the development of intergovernmental arrangements outside the Treaty when Member States wish to go down this road. They have institutional exit clauses when its procedures do not suit them. This has been formally recognised in the new Treaty, which both leaves this possibility open to them and in some ways encourages it by establishing a Standing Committee (COSI) within the Council to secure operational cooperation on internal security.

Finally, there is question of political timing. If there is no political initiative to advance legislation, little will be put forward. It took the Tampere Agenda to activate law-making within the field of immigration and asylum after the Amsterdam Treaty, and the White Paper set out a template for the Single European Act. There is no such equivalent here.

Measures to realise the Hague Programme have largely been adopted. More significantly, it is clear that national governments see this as being the reference point for some time to come. The Transitional Protocol provides that the considerable body of existing measures adopted under the third pillar are to remain in force until repealed or amended, and that the Commission will have no power to commence enforcement proceedings against Member States which have not implemented these measures.

Viewed in this light, the new legislative procedures set out in the Lisbon Treaty could be seen as possibly no more than default procedures. They are to be deployed only when the existing acquis is thought to be unworkable, and when there is a clear consensus on how to replace it and for it to be replaced by EU legislation – a set of circumstances that might not occur very frequently.
All this suggests that there is little early likelihood of an outburst of legislative activity, with or without the Lisbon Treaty. Yet there will be public debate. The discussions surrounding the European Arrest Warrant and the European Public Prosecutor give a flavour of what may follow.

The debate has taken place in many fora. It has pitched supranational institutions against each other, with the European Parliament positing itself at the vanguard of civil liberties and the concerns about the new European security architecture. At a national level, constitutional courts have been extremely proactive, as have national parliamentary committees. Debate on the Internet has flourished. It is, in short, everything one would want from a public sphere – contested, open and usually informed.

Yet there is still a concern, and it is this. This public sphere is a sphere of protest and opposition. It is centred around concerns about what has gone wrong. This is certainly necessary, but it leaves a deficit in two senses.

One is that it can curb and possibly change legislative and administrative activity, but the extent to which it informs it is very uncertain. There is no evidence that it challenges or shapes the view of justice ministries or security agencies.

Equally seriously, a sphere of opposition is precisely that. It sets out a discourse of binary oppositionalities – liberty versus security, justice for the victim versus justice for the accused – and such a discourse is necessarily too simplistic and reductivist to meet the challenges for which this policy area was established.

Damian Chalmers is Head of the European Institute at the London School of Economics.

Endnotes

3. Article 83(3) Treaty on the Functioning of the European Union (TFEU).
4. Article 71 TFEU.
5. Article 71 Treaty on the Functioning of the European Union (TFEU).
The use of intelligence data by European agencies – misplaced concerns?

The growing number of EU agencies storing, sharing and analysing intelligence data has fuelled concerns about potential threats to civil liberties. But this essay argues that as the personal data these agencies use is collected by national authorities, concerns over the way this is done (and whether the information is accurate) need to be addressed at national, not European, level.

by Björn Muller-Wille

Cooperation between different countries’ security services has intensified significantly in recent years. This trend has also affected the EU itself, which has expanded its own intelligence agencies, created other bodies supporting law enforcement, and further developed telecommunication systems and procedures for exchanging information.

It is clear that the continuing internationalisation of security challenges requires unified action, and thus cooperation and adaptation on the part of security services. Nevertheless, concerns remain about the effects of all this on civil liberties.

Who uses what data?

The Union’s ‘security’ agencies can be divided into two basic categories based on the types of decision-making they support and what type of information this requires.

The first group, which operates at the strategic level and serves the EU’s political decision-making, includes the Satellite Centre (SatCen), the Joint Situation Centre (SitCen) and the Intelligence Division of the EU Military Staff (IntDiv). Due to the nature of these bodies’ tasks, the ‘granularity’ of the data used is rather coarse, posing no threats to civil liberties. This is rather obvious in the case of the SatCen, which analyses satellite images, but also applies to the others.

Both the IntDiv and SitCen are tasked with serving the EU’s Political and Security Committee (PSC), the General Affairs and External Relations Council (GAERC) and the Security General/High Representative (SG/HR). As
none of these ‘customers’ engage directly in any form of law-enforcement operations or other activities requiring information on individual citizens, they would not have any use for such data. Rather they are interested in trends and aggregated figures that can inform strategic and political decision-making.

That said, they may, of course, collate information on individual leaders outside of the EU, be they dictators, warlords, military leaders or other influential actors. However, any concerns about infringements of the civil liberties of the likes of Robert Mugabe or Omar al-Bashir and their followers are clearly outweighed by the need to inform decisions on the Union’s collective response.

The second group of agencies is significantly different from the first. Although they occasionally support strategic decision-making, for example by producing threat assessments, they are unique in that they support law enforcement at the operational and tactical level. This group includes Frontex, Europol, Eurojust and the European anti-fraud office OLAF.

Frontex stands out in this group in the sense that it focuses on developing national border control capabilities and on improving the allocation of national capacities to the places in the Union where they are most needed. Hence, just like the agencies in the first group, Frontex does not need information on individuals or objects and is not connected to any IT network sharing such information. Rather it focuses on general developments at European borders and the availability of Member State capabilities.

In contrast, Europol and Eurojust seek to help national officials to draw the right conclusions and undertake appropriate action in very specific cases. By pooling expertise, they can support investigations directly. Although this support can be very useful, their efforts merely complement those of national authorities, which retain full responsibility for law enforcement on their own territory. One could therefore argue that their main contribution lies in acting as central hubs connecting various national agencies.

OLAF supports national authorities too, but also conducts its own fraud investigations in areas where national authorities do not have any competences – for example, within the European institutions. Hence, only the latter three agencies use personal data.
Who collects what data?

In general, European bodies neither have the resources nor a mandate to collect data on their own. All are in the business of analysis, not collection, and draw on information provided by national authorities, open sources or, as in the case of the SatCen, commercially available material.

If it is useful, staff can, of course, complement the material provided with knowledge gathered through interviews, etc. However, none of these bodies has the right to collect information in a more intrusive manner than any ‘normal’ European citizen. Hence, personal data used by the Union’s agencies is provided by national authorities.

OLAF is an exception to this rule, when it conducts internal EU investigations. Europol officers can also investigate illegal activities on the Internet (open sources) or be authorised by Member States to investigate or collect data if they participate in so-called Joint Investigation Teams.

How is data stored and shared?

In the first group, SitCen and IntDiv staff access information from national agencies via their own national telecommunication systems. Drawing on these national contributions, they produce collated EU material that is disseminated to the SG/HR, PSC and GAERC and, via them, back to the Member States.

At present, there is no centralised European information system connecting the SitCen or IntDiv with their national counterparts or other agencies within the Union. Some communication takes place via the European Security and Defence Policy net (military) or Cortesity (diplomatic), which connect the Council, Commission and national authorities, but their function is limited as information posted on them is made available to all terminals and they are not used for secret information.

However, the Secured European System of Automated Messaging (SESAME), which might replace the two systems, will offer both a selective ‘e-mail’ function and allow for secure communication.

Currently, much information must therefore be shared in physical printed form or by transporting data storage facilities within the Brussels institutions.
Given that the tasks of the agencies in the second group require an exchange of detailed information on people and objects, it is not surprising that the technical support tools used by Europol, Eurojust, OLAF and national authorities have been widely debated.

While most people support the principle that authorities collect, store and share information on people known to pose security threats, entering details on innocent, law-abiding people into European databases and searching them in order to identify ‘villains’ is controversial.

Europol, Eurojust and OLAF are all connected to national authorities via an array of systems containing data on individuals. These are the Schengen Information System (SIS), the Prüm databases, Eurodac, the Visa Information System (VIS), the Customs File Identification Database (FIDE), the Customs Information System (CIS), the Europol Computer System (TECS) (including the Europol Information System, the Europol Analysis System, the Analysis Work Files (AWF) and the AWF index system).

### Network linkages between EU agencies

<table>
<thead>
<tr>
<th>Network</th>
<th>Europol</th>
<th>Eurojust</th>
<th>OLAF</th>
<th>National Authorities</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIS (SIS II)/SIRENE</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Prüm</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Eurodac/Dublinet</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>VIS</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>FIDE</td>
<td>Envisaged</td>
<td>Envisaged</td>
<td>Yes/partially</td>
<td>Yes/partially</td>
</tr>
<tr>
<td>CIS</td>
<td>Envisaged</td>
<td>Envisaged</td>
<td>Yes/partially</td>
<td>Yes/partially</td>
</tr>
<tr>
<td>Europol Info. System</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes/only Europol national units</td>
</tr>
<tr>
<td>Europol Analysis System</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes/only Europol national units</td>
</tr>
<tr>
<td>Europol AWF</td>
<td>Yes</td>
<td>Envisaged</td>
<td>No</td>
<td>Yes if liaison officers/national experts participate in analysis group</td>
</tr>
<tr>
<td>AWF index system</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes/only Europol national units</td>
</tr>
</tbody>
</table>
The first three – the SIS (containing information on people or property sought by authorities, with about 23 million entries, of which 1.1 million relate to people); the Prüm databases (allowing all participating states to search all national databases containing DNA profiles, fingerprints, and vehicle registration data); and Eurodac (containing the fingerprints of around 300,000 asylum seekers and illegal immigrants) contain much data but are the simplest systems and most limited in their function. They are ‘alert databases’ and work on a ‘hit-no-hit’ system, which means that an enquiry results in an alert if another authority holds more information on the item. To get more details, for example, if a person is reported missing or wanted for a crime, officials have to contact national authorities via specially established national points of contact, for example through SIRENE in the case of the SIS or DubliNet in the case of Eurodac.

The next group display all (albeit limited) information held on the database in case of a hit. The Visa Information System (which will contain data on visa applications when operational), FIDE (containing data on people or businesses that have been or are subject of customs investigations), the Customs Information System (containing data on smuggling activities), and the Europol Information System (a register of persons connected to serious crime) all belong to this category. The envisaged European Criminal Records Information System (ECRIS) would probably do so as well.

As these offer a bit more information, operators may draw some conclusions and take action based on the details provided, although they would have to contact the authority responsible for the entry for any further information.

Europol’s AWF and Analysis System fall into the category of ‘analysis and investigation databases’, and are the most comprehensive in terms of the detail and applications offered. The former supports ongoing investigations directly and contains most of the information relating to the themes addressed by Europol’s analysis groups, and is therefore much broader in terms of content. The latter is a ‘data warehouse’ system, a tool that helps to link the data included to, for example, generate alerts or to identify patterns. The AWF is further supported by an index system that allows members of the analysis group and national units to find entries on a ‘hit-no-hit’ basis.

Finally, the last ‘database’: FIU.net is not a database at all. Rather it is a secure computer network designed to allow EU Financial Intelligence Units
(FIUs) to request financial information from each other and to answer such requests in a standardised format.

**Misplaced criticism?**

While some concerns about European databases are justified, they tend to focus on what is tangible and easy to criticise.

Rather than focusing on the intrusive ‘investigation databases’, most criticism is directed at the ‘alert databases’, which are easy targets due to their simplicity and transparency. In principle, ‘hit-no-hit’ searches should be the least controversial. Their use by law enforcement authorities for other purposes is also acceptable, possibly even to the extent that third countries could be told about the availability of further information.

Hence, it is not primarily the range of entries nor the fact that they are accessible to a large number of officials that is worrying. The main problem is that too many entries appear to be inaccurate and can lead to unwarranted alerts.

A 2005 inspection by the Joint Supervisory Authority (JSA) of entries into the SIS may serve as an example. According to a source involved, up to 40% of national entries were false/incorrect. The effects of false entries can be exacerbated by further linkages between existing databases and result in cross-contamination. If, for example, Europol requested more information concerning an alert through SIRENE, false details could be passed on, entered into the AWF and possibly communicated to third parties. Correcting false entries in all places where the information is held could prove very difficult.

Another area to which little attention is paid concerns information exchanged outside the Union’s databases. Neither European nor national analysts can rely solely on the information held in databases. They also need to communicate and cooperate with sister agencies in other countries that hold more detailed information. Thus a large amount of, and potentially far more detailed, information is exchanged between authorities outside of the databases and in a far less controlled environment.

The Union has facilitated these contacts by design, firstly by establishing a series of national points of contact (SIRENE for the SIS, national contact points for the Prüm treaty, Dublin Units for Eurodac, Europol’s national units and liaison officers and the national contact points of the European Judicial Network) that offer a first point of call, and can direct enquiries to relevant authorities.
Moreover, the Union provides secure networks that can be used to exchange information. TESTA, the European Community's own secure network, is an example of this. Isolated from the Internet, it allows officials from different ministries to communicate at a trans-European level. Other networks include the FUI.net that interconnects national financial intelligence units, and the two e-mail systems – DubliNet between authorities dealing with asylum applications, SIRENE for the SIS, as well as the envisaged connection within the European Judicial Network that enables direct communication between the national contact points and Eurojust.5

Only exchanges through SIRENE are clearly regulated. In addition, the use of temporary secondments and rotating contracted staff from national authorities, as for example practiced by Europol, systematically exposes experts from different countries to each other, builds trust, and develops a network of contacts that staff employ once they return to their national unit.

**Conclusion: national responsibility**

Although exchanging and saving data at the European level raise valid issues in their own right, critics do not seem to focus on the main challenges; i.e. the potential for inaccurate data, and more detailed and intrusive bilateral communications. Clearly both issues must be addressed at source, which requires national rather than European solutions and action.

European bodies have neither the resources nor a mandate to control the accuracy of national entries. Nor can they ensure the quality of entries emanating from third parties, even when tasked with doing so.6 As long as national data-protection legislation varies, it is also impossible to hold European institutions responsible for bilateral exchanges outside of their databases. Again the problems and responsibilities lie with national authorities.

While it is easy to criticise what entries the SIS II should contain, such worries avoid the more substantial threats to civil liberties. Concerns about excessive and arbitrary exchanges of personal information would be better directed against the more intrusive analysis and investigation databases, and above all against bilateral exchanges between Member States.

*Björn Muller-Wille is Senior Lecturer in the Department of Defence and International Affairs at the Royal Military Academy of Sandhurst.*
Endnotes

2. See http://ec.europa.eu/anti_fraud/fidei_en.html, See also Council document no. 3616/2/08.
4. This is even explicitly mentioned in Article 12(4) of the Council Decision establishing the European Police Office, which states that Europol and national units may exchange additional information held on persons appearing in the Europol Information System.
6. There is no way Europol could certify that information provided by third parties is correct even if this falls within its responsibilities. See Article 15(1) of the consolidated Europol Convention. See also document no. 706/08, ‘Council Decision establishing the European Police Office (Europol)’, 24-06-2008, Article 29 (1).
The securitisation of EU policies: trends and comparisons

Heightened concern about the threats to our security, particularly since 9/11, are having an impact on an increasing range of policy areas, from policing and intelligence and the defence industry to energy and migration. This essay tracks these trends and considers the questions they raise about the respective roles of EU and national policy-makers.

by Robert Dover

Millions of gallons of ink have been spilled trying to understand the nature of the EU beast: is it a super-state, a quasi-state or a club of states? Can it be seen as a state unless and until it ‘does’ security and defence ‘properly’?

Europhobes hold a paradoxical position: they fear that the EU is already too state-like, whilst suggesting that a fully functional security and defence identity is the only way to complete the job. Europhiles suggest that a regional organisation of the EU’s size and wealth really ought to exert some competence in the security sphere. But on the question of what really counts as a ‘security issue’, academics and policy-makers have moved as one to expand the definition ever wider.

This paper tracks the trend towards securitisation across a range of policy areas: defence manufacturing, policing and intelligence, and energy and migration. In doing so, it highlights the often counter-intuitive observations that individual states have been emboldened and empowered by increasing levels of EU activism, and that the European polity is neither a state nor a quasi-state but rather a governance network built on a watertight confluence of governmental and business interests.

An inflationary peace dividend

The EU’s adoption of the arms trade as a pet project took many commentators by surprise. This was an area that seemed destined to remain solely within the remit of national governments and private manufacturers, despite the success of the two flagship pan-European defence projects of the last 30 years – the Panavia Tornado and the Eurofighter Typhoon.
National governments have been reluctant to cede much ground on weapons procurement because of a historical mistrust of their neighbours, the prestige of a self-sufficient military and the potential to sell their military equipment to non-EU countries.

However, there is a strong Europeanising pressure on military equipment. Defence equipment inflation runs at a compound interest rate of 11% a year, and defence budgets – even in this time of ‘wars of choice’ – have failed to keep up as financially-pressed governments opt to focus scarce resources on budget lines which bring greater social benefits.

The rational choice has therefore been to share the research and development costs with partner countries and, as with the Eurofighter, allow the partners to sell the end-product to third countries on the open market. Nearly all European governments have played with shifting the risk of projects onto private industry – creating large off-balance sheet debts – and nearly all have ended up underwriting the risk anyway.

Under European law, the EU was technically barred from getting involved in the development of military equipment. But it managed to find a way around this via the Lisbon Agenda for growth and competitiveness, allowing it to establish the European Defence Agency (EDA) in 2004.

The EDA helps coordinate the development and procurement of European defence equipment and now provides some funding to manufacturers – a good result for the companies, which sought to influence the agency’s creation through lobbyists and their strong insider positioning within governments.

What the arms trade tells us about the Europeanisation of security is complicated. National positions have been strengthened – through common procurement and expanded European markets – resulting in larger order books for manufacturers and the protection of jobs. But Europeanisation has yet to result in savings for governments, as defence manufacturers seem exceptionally good at preserving their cash flows. However, it has resulted in the EU becoming proficient in coordinating military activity, albeit in a limited way.

National governments have yet to feel the impact of the EDA in their everyday activities. Insofar as they are influenced by the revolving door network of officials, military personnel and manufacturers, the EDA presents
merely another promising market. In time however, it may begin to fundamentally change the way that European militaries are equipped.

**Feeling spooked yet?**

The Europeanisation of intelligence and policing – again, a traditional security concern – has proceeded fitfully. The EU has taken on board some coordinating roles (Europol, SitCen, etc), but the majority of the efforts are still vested at the national level.

Cooperative arrangements across Europe have proved useful on occasion – for the British authorities, this was particularly so in the case of the capture of convicted terrorist Hussein Osman in Rome in August 2005. But old enmities die hard and, for the British intelligence agencies, the transatlantic link is still particularly durable.

If the ‘Islamist’ threat persists into the medium term, national policing and intelligence agencies will improve their liaison with other European states, but this will still be done bilaterally, and will not involve a change of institutional culture – put simply, they do this already.

The main driver for future policy in this area of security will, I think, be in the interplay between private companies and government intelligence, and will happen in three clear ways.

First, the brain drain out of government agencies in the 1990s following the end of the Cold War has resulted in the establishment of hundreds of private intelligence firms across Europe, replete with the methodologies of official espionage but without the same accountability.

Second, private firms are becoming important intelligence assets. The universality of mobile phones, commercial reward cards and high-speed Internet means that we are all now laying down far heavier data trails. In most European countries, mobile phone operators are required to keep details of who we have called and from where for up to two years.

It is currently possible to subscribe commercially to a service to locate someone, based on their mobile phone signal, showing the potential of this technology. Similar provisions exist for Internet Service Providers (ISPs) to keep data on e-mails and sites visited, and also more recently in tracking
behavioural trends through companies like ThorpeGlen, which have created profiling software to alert intelligence and policing agencies to ‘problematic’ patterns of behaviour.

The new reliance on technology and private companies has been a response to Islamic terrorism, but has also had the effect of transforming the relationship between European governments and their citizens. The passive collection of large quantities of usable data (about communications, travel and lifestyle choices) have placed citizens in a deeply supplicant position to their governments. It is highly unlikely we will ever see a revolution in Europe again, and it is lucky for us that such technology did not exist in Eastern Europe in the late 1980s, or movements like Solidarity would have been crushed before they began.

The third critical change is that since 1991, European intelligence agencies have been focused – even with the terrorist threat – on economic espionage against their allies, with business, economics and jobs becoming security issues.

If the current economic difficulties persist, we are likely to see (or perhaps, more precisely, not see) a heightened level of economic intelligence and counter-intelligence, and the blurring of the lines between government intelligence and private interests. This belatedly raises some question about the extent to which the two can be seen as distinct spheres.

**We were all cooking on gas…**

The securitisation of energy has been rapid and vigorous. Tied to fears of global warming, the availability and cost of energy (typically oil and gas) has become a topic of great concern. The recent and ongoing tensions with Russia highlight the precarious nature of Europe’s energy needs; a disruption to the flow of oil or gas to Europe will put out our lights in more than one way.

Yet, in typical European fashion, the interplay between gas companies, third countries and European actors has been disjointed to the point of farce. Energy firms have rightly tried to lever profits from their investments, and governments have recognised the loss of pricing controls as a downside of privatisation. Russia, for example, has played a very astute game of avoiding European-level negotiations on gas and picking off individual EU Member
States, like Portugal, to create bilateral agreements. This has been a boon for those which have them, but less positive for the collective good.

What can be concluded is that this swirling interplay between energy companies, third countries, and the European and national level, has created an uneven energy playing field across Europe and seriously compromised the EU’s ability to present a unified front on issues such as Russia and Georgia today.

For individual governments, energy prices have been a tricky problem, with the cost of petrol causing civil unrest in France, Spain and the UK – but again, the ability of governments to do anything other than alter taxation rates seems limited. It may take something like the $150 barrel of oil, and further conflicts in the Middle East, to convince European governments that they need to invest more political capital at the EU level to strengthen their national hand, through the collective might of the Union.

**Fortress Europe – a problem of immigration?**

Immigration became a securitised issue in Europe because of the perception of a post-9/11 terrorist threat from Europe’s ‘near-abroad’, namely the transit routes through Morocco and Algeria; the correlation between migrant communities and levels of crime in European cities; and a zero-sum game equation of increased populations and the availability of food, housing, energy and financial resources.

The European Commission’s Directorate-General for Justice, Freedom and Security has been pushing for a common approach to immigration, but, as it stands, individual governments still have a great deal of leverage over their self-determined policies, and can therefore shape their own destinies. This creates a very patchy experience for migrants coming from outside the EU’s territory.

From a security perspective, the fear of Islamic migration (in particular) outweighs the reality of any threat it might present. The atrocities on mainland Europe have been largely committed by second-generation Muslims radicalised within Europe, rather than first-generation ‘imports’.

The pressure that has been placed on social cohesion within parts of Belgium, France, Germany, Italy, Spain, and the UK has created its own low-level security problems as disaffection spreads within what might be termed the indigenous and immigrant populations, faced with employment glass ceilings and poor social conditions.
The EU has, however, taken ownership of helping its members to police the Union’s external boundaries and, in the case of Africa, has placed processing centres outside the EU’s boundaries to try to discourage dangerous attempts to land on European soil.

What the issue of migration ultimately challenges is the answer to the question: what does it mean to become a citizen of Europe – is Europe a place where people can come and make their fortune, or is it a closed club? This debate is yet to be had, and the tensions between the European drive to formulate common approaches and the national practice of jealously guarding policy primacy means we should not necessarily be optimistic that it will be neatly resolved any time soon.

Conclusions

This paper focuses on four policy areas that I felt represented recent European security trends and brings out what I believe is the complicated and problematic nature of Europeanisation.

We cannot neatly track the ‘uploading’ and ‘downloading’ of preferences depending on the issue, nor can we easily suggest that the growing list of issues covered by the term “security” is due to a bureaucratic land-grab.

The main trends have been to see a pronounced role for private companies in all of these areas, and for them to successfully pursue the profit motive through lobbying and insider-advocacy simultaneously at the national and European levels. This can be viewed either as a pincer movement, or as I prefer to see it, as a broader set of questions about the extent to which the distinction can be made between government and private interests.

Another trend has been to see a positive-sum game emerging out of this securitisation agenda, with governments and the EU becoming emboldened by new measures and policy developments. This is something that the European governments should bear in mind when they retreat into nationalistic policy bunkers.

Ultimately though, all of these developments have contributed to a recalibration of the social contract in Europe – what it means to become and be a citizen of Europe. These are no longer ‘our’ governments, but entities that govern ‘us’, and this is important because it places an emphasis on
these governments and businesses to act with proportionality, and to project a positive vision of what it means to be a citizen in their space.

Robert Dover is a Lecturer in International Relations in the Department of Politics, International Relations and European Studies (PIRES) at Loughborough University.

Endnotes

1. Bar the Danish, who opted out.
Protecting the right to privacy: why the EU must stand by its principles

The 1995 EU Data Protection Directive set out clear principles of protection based on privacy as a right. This essay argues that while the legislation may need adapting to take account of new technology and changing business methods, raising complex and difficult issues, this must not be used as a pretext to weaken its core principles.

by Jim Murray

Regulation is often criticised as lagging behind developments in the market place. However, the fundamental EU law on privacy – the 1995 Data Protection Directive – and later associated measures, might more accurately be described as being far ahead of developments in the market place.

When the Directive was first mooted, it was certainly seen as a response to new challenges posed by information technology. But few foresaw the full potential of that technology to expand and make the collection and processing of personal data easy, almost without limit and at little cost. Indeed, some would argue that this is the problem with the Directive, and that it should now be amended (i.e. softened) to adapt to the impact of new technology and business methods.

I would argue the contrary. I think it was fortunate that the Directive was enacted when it was. It was easier then to articulate clear principles of protection based on privacy as a right, when the impact on existing business practices was not as extensive as it would have been later.

It might be argued (but not by me) that industry initiatives would have adapted and improved data-protection regimes in line with evolving technologies and business methods. We have only to look at what has happened in advertising and marketing to see the weakness of that argument.

It was once a cardinal principle of advertising self-regulatory codes that all advertising should be recognisable as such. The early crude techniques of subliminal advertising were universally condemned – but not so many of the more modern techniques of integrated marketing (especially online) and viral marketing (strategies that encourage e-mail recipients or ‘influence
leaders’, including children sometimes, to pass messages on to others to generate added exposure. These techniques are hidden advertising (viral marketing especially), but nowadays they win advertising awards instead of condemnation.

Faced with criticism that it has abandoned a long-held principle, the industry simply responds that “times have moved on”, as if the process was somehow inevitable and outside anybody’s control. The same would certainly have happened to data protection if we had not had the mandatory principles of the 1995 Directive.

The Directive does lag behind the market place, however, in relation to enforcement. The explosion of new techniques and technologies for data gathering and processing has raised numerous challenges in applying its core principles.

For example, how should it apply to search engines, online social networks, behavioural profiling, ambient intelligence, radio frequency identification technology (RFID), CCTV, child protection, electronic tolls, cross-border data flows, security and crime prevention, interactive media and biometrics?

These are some of the issues currently being studied by the data-protection authorities of the EU Member States, in the committee and working party set up under Article 29 of the Directive. It will take time and (more) resources to work through these issues, but the difficulties and complexities involved are no argument for weakening the Directive’s core principles.

Briefly, if simplistically, stated, these are that personal data should be gathered only with the consent of the subject, that they should be used only for the purpose for which they were collected, that the gathering, processing and storage processes should be necessary and proportionate to the object for which the data were collected, and that subjects should always have the right to access and correct their personal data.

From the beginning, it was clear that there had to be an extra-territorial aspect to EU law on data protection – data can flow across borders almost instantaneously at the click of a keyboard. The Directive therefore applies to processing by any data controller exporting information from the EU who is established or using equipment in the Union. Data may not be sent to another country where there is not an equivalent level of data protection – the country concerned must be a “safe harbour”.
Protecting EU data in the US?

This principle has raised problems in relation to the US, which has different and sectoral sets of data protection regimes, as distinct from the more unitary EU regime that applies to all sectors across the board. Problems have also arisen in relation to the post-9/11 US policy of extensive data collection, including airline Passenger Name Record (PNR).

A first agreement between the EU and US was annulled by the European Court of Justice and replaced by a new accord. This new agreement is apparently less onerous, although that has been disputed and is still a source of serious concern to privacy advocates and regulators. Among other issues, doubts remain as to the extent to which the agreement is binding on the US.

More recently, further tensions arose when the US sought to conclude a bilateral deal under which the Czech Republic would provide more information than required under the revised EU/US PNR agreement. In return, the Czech Republic was to be included in the US visa waiver scheme.

Passenger Name Records were not the only source of EU/US tension on data protection and privacy. In 2006, it was revealed that US intelligence and law enforcement agencies, on foot of a subpoena, had had access for some years to the data recording millions of international financial transactions carried out by Belgian-based SWIFT (Society for Worldwide Interbank Financial Telecommunications).

For the European data protection authorities, this arrangement was in clear breach of the 1995 Directive since, inter alia, the data transfer was secret, intrantransparent and without adequate (or perhaps any) limit on the period for which the data might be kept or the uses to which it might be put. The point was made that even in the fight against terrorism and crime, fundamental rights must be respected.

Subsequent negotiations between the EU and US led to an understanding regarding future transfers from the SWIFT database. This understanding (it can hardly be called an agreement) has also been criticised for appearing to rely more on US goodwill than on any legally binding commitments.
New challenges to privacy continue to emerge. To meet these challenges, the US and EU will need to work together as closely as possible, despite the problems posed by the disparate US privacy regimes and the US response to the 9/11 outrage.

The Transatlantic Consumer Dialogue (TACD) has called on the US and EU to develop a set of standards for the use of radio frequency identification technology (RFID) pre-emptively.

In the words of the Article 29 Working Party, “the ability to surreptitiously collect a variety of data all related to the same person; track individuals as they walk in public places (airports, train stations, stores); enhance profiles through the monitoring of consumer behaviour in stores; read the details of clothes and accessories worn and medicines carried by consumers, are all examples of uses of RFID technology that give rise to privacy concerns. The problem is aggravated by the fact that, due to its relative low cost, this technology will not only be available to major actors but also to smaller players and individual citizens.”

**Keeping personal information personal**

A different set of problems is posed by the increasing use of search engines and social networking sites. Google, for example, collects, retains and processes a vast amount of information about the search history of its users – information from which personal details such as religion, political beliefs, sexual orientation, income range, etc. may readily be deduced.

Just recently, Google has decided to anonymise personal data after nine months, down from up to 24 months at first, although then reduced to 18 months under pressure from the Article 29 Committee. The nine-month period is obviously an improvement, but still seems very long.

The popularity of social networking sites, especially among young adults, has huge implications for privacy. The consent of the subject is an essential pre-requisite for the collection and processing of personal data, and the data must be used only for the purposes for which it was collected.

What is the level of consent and understanding of those who seem to present their (perhaps embellished) private life to the world, including their youthful indiscretions to be seen by everyone – including perhaps police, parents and prospective employers? The Wall Street Journal recently reported on a survey
by Career.com of more than 3,000 hiring managers: 22% of respondents said they checked social networking sites to screen job applicants and of these, 34% found content that made them drop the candidate.

The issue of data protection is also arising in competition policy. In a merger case, for example, what are the implications of the fact that the personal data held by one company will be transferred to the new merged entity? Should this transfer be a factor in the assessment of consumer welfare in a regulatory review of a proposed merger?

In approving the Google-Double Click merger earlier this year, the European Commission said the decision was “without prejudice to the merged entity’s obligations under EU legislation in relation to the protection of individuals and the protection of privacy with regard to the processing of personal data and the Member States’ implementing legislation”.

This would seem to suggest that the Commission currently feels that issues of privacy are a matter for data protection legislation rather than factors to be considered in competition policy.

The protection of intellectual property is a battleground for privacy rights on both sides of the Atlantic. Intellectual Property (IP) rights holders are struggling in various ways – unfortunately with some success – for the right to require Internet service providers to disclose personal details of users who may be assisting in the downloading of music or audiovisual files without proper authorisation to them directly.

The Commission and the right to privacy

The Commission seems sympathetic to the rights holders’ position, even including a provision in a proposal (currently on hold) to give them the “right to assist” the police or other public authorities in the investigation of suspected breaches of IP rights. In effect, this could give rights holders the right to accompany police on raids on private property (including a competitor’s property) and the right to inspect documents seized in such raids.

Of course, authorities in Europe also collect and process personal data for many other reasons. Many Member States have a population register and ID card system – a practice viewed with much misgiving in those countries that have not gone down this road. A Passeport Name Recognition system is being introduced for flights in and out of the EU. There is much sympathy in
the Commission and among some national authorities for the efforts by IP rights holders to weaken certain privacy provisions.

Perversely, the Commission also hides behind so-called privacy concerns to try to justify its own lack of transparency, refusing at times to disclose the identity of lobbyists or the content of what it was told by them.

This is disingenuous because the solution is in the Commission’s own hands: it only has to announce that from a certain date, it will publish all submissions on issues of public policy and their source, subject to a few limited and narrowly defined exceptions including a (genuine) need for commercial confidentiality.

As technology develops, there will continue to be new strains and challenges in preserving privacy. It may be necessary to adapt existing legislation to better meet some of these challenges, but the core principles must not be changed. Privacy is a right, not a preference.

Jim Murray was formerly Director of BEUC and President of the Transatlantic Consumer Dialogue (TACD). He writes here in a personal capacity.
Keeping the Internal Market together in the knowledge economy

Personal data is becoming an ever-more important and valuable commodity in today’s increasingly knowledge-based economy. This essay argues that different rules on data retention and Internet surveillance from Member State to Member State are already making life more difficult for companies operating across Europe, and the EU must act to prevent the fragmentation of the Internal Market.

by Hans Martens

The EU’s Internal Market was created to boost Europe’s economy, creating economies of scale by breaking down barriers and opening up a huge European home market.

The challenge now is to ensure that the successes of the past can be continued into the future by updating the Internal Market to cope with the realities of today’s increasingly knowledge-based economy, in which personal data is clearly becoming an ever-more important and valuable commodity.

Failure to address this issue would raise the spectre of an increasingly fragmented Internal Market, with the development of different data protection regimes from Member State to Member State.

Looking back, it is obvious that the manufacturing sector was uppermost in policy-makers’ minds when the Internal Market was being created and that, in effect, most of the 1992 ‘package’ was about market-opening for industrial products.

The services sector had already grown considerably by then, and was overtaking manufacturing in terms of economic importance quite rapidly. However, when proposals to modernise the Internal Market through the Services Directive were launched by the European Commission in 2004, the process did not go nearly as smoothly and enthusiastically as in the years leading up to 1992.

The result of this is that, today, the EU has an imperfect Internal Market in services. The risk is that we are going to get an even more imperfect Internal Market for knowledge-based services and products in the future.
That would be damaging to Europe’s economic development. There is a wide consensus that Europe’s future welfare depends on integrating more and more knowledge into economic activity, and that productivity must be raised by integrating knowledge-based, ‘smart’ solutions into the way we do things. This is essential to meet the big challenges of the future: global competition and demographic developments in Europe.

The Lisbon Process is a framework for structural reforms in Europe, and includes a very strong focus on pushing for more innovation and a deeper development of the knowledge-based economy in Europe. But a well-functioning Internal Market is also a pre-condition for the Lisbon Process to work, and will be a pre-condition for the development of Europe’s knowledge-based growth in the future.

It should also be noted that substituting 27 sets of national rules with one common European set of rules or regulations makes a significant contribution to administrative simplification, which could further boost the development of knowledge-based services and products.

However, the knowledge-based economy is not ‘in the future’ and therefore something that we can deal with later. We are already living in it, and there is a risk that we will lose the opportunity to bring the successes of the existing Internal Market with us into this new economy if we do not act to create a real Internal Market for the knowledge society.

This is the main reason why the European Policy Centre has set up a Task Force to work on proposals in this area, with the aim of coming up with a set of concrete recommendations on steps to be taken to maintain the great advantages of an Internal Market in the knowledge society.

Links to the past

There are obviously strong links between the 1992 Internal Market and the knowledge-based Internal Market, not least the fact that the knowledge economy is not separate from more traditional economic activities: knowledge-based solutions are already increasingly being ploughed into the industrial or service sectors.

One such example of a great success in the 1992 Internal Market was the GSM standard for mobile telephony. In the preceding years, there were several standards for mobile telephony in European countries and regions,
and this resulted in fragmented markets which offered very few economies of scale. This, in turn, meant handsets were very expensive and operational costs very high.

As a common European standard, GSM created the necessary economies of scale, and the rest is history. It became established as a world standard – a feat which would have been impossible for any of the national European standards.

Integrated networks across the world, and in particular across Europe, have provided a tool for transferring knowledge with technologies derived from the 1992 Internal Market; and the increased focus on roaming charges could lead to an even more seamlessly integrated European communications’ market.

**Links to the future?**

However, while we may have successes from the past to build on, there are many examples of missing links to the future; i.e. a lack of initiatives to prepare for the free movement of knowledge.

The discussion on this often focuses on the issue of the free movement of researchers, but although there could be improvements in this area, the basic requirements have already been provided for in the existing Internal Market and the free movement for people principle enshrined in the Treaty of Rome. The real fifth freedom to be added to the existing four (free movement of goods, services, people and capital) is free movement of knowledge and knowledge-based products and services.

There are already many examples of the lack of a coordinated European approach in this area.

One such example is the different rules concerning copyright protection for digital services: the recent high-profile protest in Brussels backed by celebrities like Sir Paul McCartney centred on a dispute over the lack of European legislation in the area of copyright and royalties for the electronic use of music across national borders.

Another example is home banking. This has become very popular in many parts of Europe but, while there do not appear to be many limits to the range of banking services on offer within the national borders, there are certainly limits to what can be done across borders. Even within the euro area, cross-border transfers cannot be made without involving the bank (and its charges). So while
all transfers from Seville to Barcelona can be done from home without incurring additional costs, this cannot be done to cover the much smaller distance between Barcelona and Perpignan.

Electronic signatures are another example of how the lack of a real Internal Market is hampering the use of digital services across Europe’s borders. Most countries have invented their own systems and, despite efforts to create European common rules and standards in this area, the uptake is virtually zero. Nor has enough been done to promote a Europe-wide regime for electronic signatures. This creates problems in relation to private transactions across borders and in dealing with public authorities, including electronic bidding in response to Europe-wide tenders under the EU’s public procurement laws.

Different rules on data retention and surveillance of the Internet from Member State to Member State are already making life more difficult for companies operating across Europe, which are required to comply with different sets of rules and regulations in each country.

Data-protection laws in Europe also appear to be out of line with ‘real life’ requirements, with UK Information Commissioner Richard Thomas telling the Financial Times in July 2008, that: “Europe’s data-protection laws are no longer fit for purpose.” He warned that the regime is showing its age and is failing to meet new challenges to privacy, such as the transfer of personal details across international borders and the huge growth in personal information online.

The big risk is, of course, that if European legislation in such areas is seen as outdated, Member States will be sorely tempted to introduce ‘improved’ regulations at the national level, leading to precisely the sort of fragmentation of the market that should be avoided. Europe therefore must take the lead and make proposals for updated legislation in order to keep the Internal Market intact and ensure it continues to function effectively.

This issue of Challenge Europe highlights other examples of a trend towards a fragmented European market in areas directly linked to data protection, but the main point here is that if EU does not take the lead in a very fast-changing environment, it runs the risk of national standards and rules emerging.

This would deny e-traders, telecoms companies, airlines and many other operators the opportunity to benefit from economies of scale at the European level, and this in turn would mean that Europe deprives itself of opportunities
to take full advantage of the developments in the knowledge-based economy of the future.

A more homogenous Europe

Finally, it is also important to note that Europe is far from homogenous when it comes to use of the knowledge society and digital services. Again, if there is a consensus that the future of wealth creation lies in the knowledge economy, it is important to get everyone on board.

Statistics for 2007 (Internet World Stats) show the wide variations in Internet use: only 30% of Bulgaria’s population has access to the Internet, with similarly low figures for Hungary (35.2%) and Greece (35.5%), compared to 77.3% in Sweden and 73.1% in Portugal.

This indicates that a major effort is required in the area of investing in physical infrastructure, particularly broadband (fixed line or mobile). Although a significant proportion of EU Structural Funds are being used for this purpose, it is far from enough to get the whole of Europe online.

A major effort, using both public and private money, is required at national and regional level to create a more inclusive knowledge society in Europe. It is equally important to invest in education and to demonstrate the clear benefits of the knowledge economy to the broader public.

This is especially important in countries with low Internet and broadband penetration, not only to create the demand for such services, but also to include a larger part of the population in the knowledge economy, where important sources of welfare creation are to be found.

A sound and well-designed environment for data – and consumer – protection can do much to eliminate the fears of the digital world that many people still have.

Hans Martens is the Chief Executive of the European Policy Centre.
Constructing a Europe of asylum in a securitised world

Governments maintain that collecting increasing amounts of information on people entering and leaving EU territory, and tracking the movements of third-country nationals, boosts security. But this essay argues that increasingly sophisticated border controls are just one example of the over-riding emphasis EU Member States now place on security and control, which is undermining the Union’s reputation as a haven for those in need of asylum.

by Nicolas Beger

For many good reasons, the EU regards itself as a beacon of human rights and, reflecting Europe’s own (patchy) record as a territory open to those who face serious persecution, EU Member States will remain a magnet for those seeking to escape persecution, violence or poverty.

However, with security increasingly becoming the paramount concern for Member States, many argue that men, women and children seeking international protection today are being seriously failed by the repressive approach to irregular migration. Asylum-seekers and refugees face new obstacles that arguably circumvent the international ‘obligation to protect’ by preventing them from ever reaching EU territory.

Strengthened border controls are becoming increasingly sophisticated, with an ever-greater volume of personal data being collected as part of efforts to track the movements of third-country nationals, and the EU is engaging with third countries – some of which are gross human rights’ violators – to actively curb migration and facilitate repatriation.

This scenario is fuelled at home by a dangerous blurring of language which mixes asylum, migration and terrorism. The overriding emphasis on control and security is the key element preventing the EU from developing a more comprehensive approach to addressing the reasons why people flee their countries.

Constructing a ‘Europe of Asylum’

In October, EU leaders adopted the ‘European Pact on Immigration and Asylum’, which explicitly includes the commitment to “construct a Europe of Asylum” – a welcome step. The chapter on asylum does not, however, contain
any new or innovative thinking. It merely reconfirms the roadmap drawn up by the European Commission in its June 2008 ‘Policy Plan on Asylum’.

Although it states that strengthened European border controls should not prevent access by those who are entitled to international protection, the Pact does not detail how it will ensure that the EU’s external border-control mechanism effectively meets this obligation; nor, indeed, how a ‘Europe of Asylum’ will be constructed in reality, bearing in mind that two other commitments underlying the Pact are somewhat contradictory to this aim. They focus on making border controls more effective, and firmly endorse the principle that “illegal (sic) immigrants on Member State territory must leave that territory”, 1 whether returning to their country of origin or a transit country.

Asylum policy cannot be a political football. It is a vital tool of human rights’ protection that imposes legal obligations upon governments. States are entitled to control the entry of non-nationals into their territory, but this right must be exercised in accordance with international human rights’ law and refugee law and standards. The EU’s Common European Asylum System could be based on the highest standards possible (currently it is not), but it would be of no use unless refugees can actually gain access to the Union’s territory and admission to procedures.

The EU’s obsession with securing its external borders fits with the logic of abolishing internal border controls and creating an Internal Market. However, in turn it puts migrants and asylum-seekers at risk and, as recent figures show, it is not curbing the ever-increasing numbers.

Moreover, the process of creating more and more obstacles that prevent access to EU territory is no longer limited to the Union’s actual physical external borders. Indeed, the EU and its Member States are now engaged in effectively shifting the external borders further South and further East, with Member States increasingly carrying out sea patrols not only in their own territorial waters, but also in the territorial waters of third countries from where asylum-seekers and migrants start their perilous attempts to access EU territory.

Operations carried out in the framework of FRONTEX have been taking place in the territorial waters of countries such as Senegal and Mauritania, with a view to preventing people from embarking on a very dangerous journey. As much as these measures may effectively save lives, such interception/rescue-at-sea practices may also prevent access to protection by those in need.
‘Containment’ is not even working

Ironically, the EU’s own data show that the Union and its Member States’ control-oriented approach and their policy of ‘containment’ are not even successful.

Ever-more sophisticated border controls in the Mediterranean do not seem to have reduced, let alone stopped, irregular migration. Migration flows have just shifted in consequence and the many operations carried out at land and sea borders have so far not prevented migrants and refugees from risking their lives at sea or paying enormous amounts of money to unscrupulous traffickers to smuggle them into Europe.

Migrants are simply forced to travel on longer, and therefore more dangerous, migration routes, but as long as their actual plight – persecution, violence, poverty – is not addressed, the numbers will never decrease.

In a remarkable interview recently, the executive director of FRONTEX even pointed out that operational activities in the Mediterranean may have been counter-productive in so far as they may be “serving as a pull factor for traffickers”. According to FRONTEX, traffickers are forcing migrants to sink their boats when they sail close to the coasts of Malta and Lampedusa so that they will be saved by EU Member States’ vessels and taken ashore.

The EU and its Member States must address the negative and potentially life-threatening side-effects of this predominantly control-oriented approach. The phenomenon of the Mediterranean Sea crossings presents a formidable challenge for the EU as well as for human rights’ advocates. The imperative to prevent further loss of lives at sea must be reconciled with the obligation to offer international protection to those in need of such protection and to ensure that no one is subjected to refoulement (i.e. being returned to a territory where they would face persecution).

With this dilemma in mind, and recognising the EU’s right to manage its own borders, its increased cooperation in the field of migration control with a number of transit countries nonetheless raises a number of questions.

Firstly, is it legitimate, and indeed in accordance with Member States’ international legal obligations, to prevent asylum-seekers from leaving countries with highly problematic human rights’ records? Amnesty International has reported a range of human rights’ violations, including long-term arbitrary
detention, collective expulsions and indeed *refoulement* of migrants and asylum-seekers from such countries as Morocco, Libya and Algeria.

Secondly, is it legitimate to pursue a policy of preventing onward migration of asylum-seekers through so-called capacity building with transit countries in North Africa, when we know that asylum systems in such countries are either non-existent or in a very early stage and clearly not ready to offer effective protection in line with international law? And how does this affect the responsibilities of the EU Member States and indeed the EU institutions under international human rights’ law?

None of this suggests that the EU should stop its efforts to support transit countries in creating a functioning protection system or to encourage them to adopt a legal framework at national level to ensure respect for the fundamental rights of asylum-seekers and migrants. The more ‘protection space’ that is created, the better. However, the approach should be balanced and acknowledge the differences in protection capacity and the need for more solidarity in the international protection regime.

**Is technology really the ultimate solution?**

A predominantly security-driven approach is also reflected in three recent European Commission communications on the future management of the EU’s external borders which propose increasingly sophisticated technical measures.

The Commission’s vision is to create an entry/exit system similar to that which has been installed in the US. Based on a more efficient use of biometric identifiers and the creation of yet another database at EU level (the European Electronic Travel Authorisation System), it aims for total control of the Union’s external borders.

Technology is increasingly seen as the ultimate solution that will provide us with information about who enters and who leaves, and thus should be able to prevent those third-country nationals who apparently pose a threat to national security or public order from entering the EU.

A system of registered *bona fide* travellers who have sufficient means of subsistence, have never overstayed before and do not pose a threat to security, will be added to the entry/exit system replacing the current visa system. All third-country nationals would be subject to increased and more
thorough pre-entry screening both at consulates and embassies and at the physical border. Those who do not currently require visas would, as a result, also be targeted.

Within the over-arching frame of the ‘war on terror’, it is argued that collecting increasing amounts of personal data about the whereabouts of third-country nationals should increase security. Indeed, an alert system should automatically inform competent authorities throughout the Union of those third-country nationals who overstay their visa or authorised stay in the EU.

Science fiction or reality? That remains to be seen. In any case, the Commission’s vision is to shift control away from the physical borders of the Union.

Important questions arise with regard to who exactly will be considered as a *bona fide* traveller. Will it really be about facilitating travel for businesspeople who regularly travel into the EU, or is it rather about keeping out those who fit a generalised profile of potential risk to internal security or public order? Will the alert system with regard to those overstaying be an effective method of managing migration in a way that respects human rights, or will it add to the witch-hunt of those who have not complied with the entry regulations?

Creating security in Europe is not achieved by eroding human rights. Measures should remain in proportion to what they are trying to achieve.

In this securitised world, perhaps the most worrying trend is the suggestion that somehow there is a link between asylum, migration and terrorism. The right to asylum, as a fundamental commitment to human rights’ protection, has somehow become entangled in the wider security debate. The result is a political climate in which governments are no longer inhibited about attempting to change or effectively undermine existing international standards.

There are manifold examples that show how the ‘politics of fear’ takes over, to the detriment of upholding fundamental rights and values upon which the EU is built.

One is the opening up of EURODAC, the EU’s database on fingerprints of asylum-seekers, to law enforcement agencies which may share them with third countries – potentially those governments whose violations of fundamental rights cause asylum-seekers to flee in the first place.
The other is the constant push by certain Member States for an increased use of diplomatic assurances to facilitate the removal of alleged terrorist suspects. Nothing less than the principle of non-refoulement is at stake here.

International law is very clear that the ban on torture and other ill-treatment is absolute, and prohibits transferring people to a place where they would be at risk of torture or other ill-treatment. Yet there have been attempts by a number of Member States to seek political backing at the European level for a practice that clearly undermines international human rights’ law.

How successful these attempts have been so far is hard to assess. But there is little doubt on the position the EU should take in this debate. If the Union wants to maintain its credibility as a global actor for the protection and promotion of human rights, it cannot but strongly reject any use of diplomatic assurances.

The ‘politics of fear’ will undermine the EU’s reputation as a beacon of human rights. The initial few who pointed to the dangers we all face vis-à-vis the safeguarding of fundamental rights in Europe have now been proven right in their predictions.

It is high time for the tide to change again towards a more human rights-oriented climate that seemed untouchable not that long ago. The recurrence of xenophobic attitudes, this time under the cover of ‘security’ at the highest political levels in EU Member States, does not go unnoticed. The criminalisation of migrants on their status alone, as recently seen in Italy, is a dangerous move that Europe cannot afford.

Nicolas Beger is Director of Amnesty International’s EU Office.

Endnotes

2. Using the term ‘illegal’ for irregular migrants is more than a question of political correctness. It aggravates the tendency towards criminalising migrants on their status alone – while acts can be illegal, no human being can be illegal per se.
Mission Statement

The European Policy Centre (EPC) is an independent, not-for-profit think tank, committed to making European integration work. The EPC works at the ‘cutting edge’ of European and global policy-making providing its members and the wider public with rapid, high-quality information and analysis on the EU and global policy agenda. It aims to promote a balanced dialogue between the different constituencies of its membership, spanning all aspects of economic and social life.