COUNCIL OF EUROPE CONSEIL DE L'EUROPE

T-PD(2013)07Rev

31 March 2013

The use of the Internet & related services, private life & data protection:

trends & technologies, threats & implications

by

Douwe Korff
Professor of International Law
London Metropolitan University
London (UK)

with advice from

Dr. Ian Brown
Associate Director (Cyber Security Centre) and Senior Research Fellow (Oxford Internet Institute)
University of Oxford (UK)

(new version)

Douwe Korff
Professor of International Law

The use of the Internet & related services, private life & data protection: *trends & technologies, threats & implications*

About this paper:

This paper was written at the request of the Data Protection and Cybercrime Division of the Directorate-General of Human Rights and Rule of Law of the Council of Europe, by Douwe Korff, professor of International Law at London Metropolitan University (http://www.londonmet.ac.uk/depts/lgir/law/staff/professor-douwe-korff.cfm), with advice from Dr. Ian Brown, Associate Director (Cyber Security Centre) and Senior Research Fellow (Oxford Internet Institute), University of Oxford (http://www.oii.ox.ac.uk/people/brown/). It draws extensively on work done by them together and individually, as well as on the work of others.

1. Introduction

This report seeks to map out and detail emerging trends, implications and threats to the right to private life and to data protection linked to the use of the Internet and related services. The report builds on the discussions held in the context of Internet governance events (IGF and EuroDig in particular) and considers the issues under both a public sector and private sector angle (and in respect of the latter, distinguishes between individuals and groups/user of the Internet and Internet-related services, and companies). It draws heavily on reports by myself and others, by means of direct quotes or as acknowledged in endnotes. Special mention should be made of my regular co-author, Dr Ian Brown of the Oxford Internet Institute, who kindly advised me on many of the technical issues and trends - but I alone remain responsible for any errors. The sources mentioned in the notes (which include many papers and reports written by Ian and me together) may also serve as a basic bibliography.

Section 2 provides the broader context within which the specific subject of the report must be viewed. Sub-sections 2.1 and 2.2 identify general technical and socio-political changes and trends, in the latter case with reference to different actors: individuals and groups of individuals (including criminals and human rights defenders), different kinds of companies, and the State. In sub-section 2.3, I discuss in some details the risks and limitations inherent in the technologies described at 2.1. These are crucial to the purpose of this paper.

I hope that, taken together, the sub-sections in section 2 show the trends and serious challenges to major national, international and European achievements.

On this basis, section 3 seeks to briefly identify the issues most relevant to the work of the Council of Europe in general, and the Data Protection and Cybercrime unit in particular, with reference to the European Convention on Human Rights, European data protection law, European and global international cooperation between police and judicial authorities, and between national security authorities, and to LEA – NSA data exchanges.

In other words, between them, the various sections and sub-sections deal with the trends concerned from various perspectives: from a technical point of view (sub-section 2.1, but with clarification of the limitations of the technologies in sub-section 2.3); from a social-political point of view (sub-section 2.2); and from the point of view of different major areas of focus of the Council of Europe (section 3). This has inevitably led to some overlap, but hopefully makes the complex subject-matter more accessible.

In section 4, I tentatively suggest some areas of possible priority to the Unit. I would of course be happy to discuss any of those further if required.

2. The broader context

2.1 Technological developments[1]

Computers and computing power

Computing technology has grown at an exponential rate since the 1960s, and the Internet has revolutionised societies and the world. Growth in computing processing power and storage capacity will continue to follow "Moore's Law", under which these factors double every 12 – 24 months, leading to a thirty-fold increase by the next decade. Although by then the fundamental limits of silicon engineering will be approaching, it is likely that new devices such as nanotubes or spintronic chips and materials such as graphene, molybdenite and/or other one- or just a few-atoms-thick materials will overcome these.[2] Quantum- and DNA-based computing systems promise even further increases in computing power, but are further on the horizon. [3]

One way or the other, we will move to an era in which "super-computers" with vast processing capabilities will become available "on demand", to many more users (including commercial companies and medical researchers, as well as defence-, law enforcement- and national security agencies), partially through "Cloud computing" (discussed later), but perhaps also involving a grid of peta-scale supercomputers.[4]

The Internet of people

The growth of the Internet is linked to this increase in computing power: communication bandwith has also followed Moore's Law, and the better, faster connections and processes have massively increased uptake, at least in the developed world. In the USA, more than 80% of adults now use the Internet,[5] and Europe is following this trend, with 63% (against 30% in the rest of the world).[6]

However, Internet use is moving away from fixed - and often shared - personal computers in offices and homes that are linked to the Internet by Internet Service Providers (ISPs), to personal mobile devices. We are moving to an "always on" mobile - and personal - Internet.[7] This is seen as a major driver in e-commerce,[8] which is shifting to m-commerce (mobile commerce). e-Government similarly may become m-government, etc. However, this has implications in terms of both users and providers, and their relationships: on the one hand, mobile Internet access is much more directly linked to a specific individual, while on the other hand the platform for the mobile Internet is provided by Mobile Network Operators (MNOs), working with separate application- or value-added service providers. Both MNOs and such other providers tend to exercise more control over their networks' and services' usage and uses, and take a much closer interest in the activities and interests of their clients than traditional ISPs used to do.

Net Neutrality[9]

Apart from the growth in computing power, the spread and importance of the Internet is also made possible by "Net Neutrality": the principle that the network, and the network providers, are agnostic about the use of the network: their only job is to move data, without discrimination between users, content or applications. The principle was an integral part of the original concept of the 'Net, and is still is at core: the whole point of the Internet is to allow users (originally academics and the U.S defence institution DARPA) to freely share their files, without some central control or single node. All data moved, and still basically moves, around the 'Net from sender to recipient through whatever route is most convenient and effective. If an obstacle occurs, the traffic automatically goes around it.

The original goal was convenience and security: the data would always end up with the intended recipient, whatever technical glitzes might occur somewhere on the system, and attackers would find attempts at obstruction of the traffic most difficult.

But it also ensured that when the Internet moved to the wider world, there was a level playing field for all websites and all Internet technologies, offered or used by anyone. Net Neutrality helps innovative entrepreneurs to start up new SMEs offering new products or services, and it enables us, the users, to use any equipment, content, application or service we choose, without interference from the network provider.

Net Neutrality is therefore the greatest strenght of the Internet, indeed a *conditio since qua non* for the Internet as we know it. But it also viewed with suspicion (or worse) by those public and private entities who want to control our activities, and/or increase their profits by discriminating between different users or products or apps. This leads to a struggle over the very nature of, and control over, the Internet, as I shall further discuss in section 2.2, below.

Nanotechnology and the Internet of Things[10]

With the growth of nanotechnology, the spread of miniature sensors that can transmit information is rising fast. RFID (Radio Frequency Identification) chips are increasingly attached, or built into, to consumer products. They are small devices that send information about the product to a receiver, which can be a "Near Field Communication" system built (e.g.) into a shop checkout desk, or into a mobile phone, or a Wifi router.[11] A ubiquitous network of smart packages is being created that track products across the supply chain - but that can also continue this tracking of the products after purchase, when they are in your home or in your pocket. RFID chips are also increasingly included in "e-passports", but with some security built in against "skimming" of the data by unauthorised people. They can also be implanted in animals, as is already done for pets, or included in ankle- or arm bracelets, as is done with babies (to stop them being abducted from hospitals) or people suffering from Alzheimer's disease.[12]

However, smaller - much smaller - sensors are being developed. They could in future be woven into or sprayed onto clothing in the form of nanosheets.[13] In medical science, they can take the form of a "Lab-on-a-Chip" or LOC device, seen as "*an important component*

of e-health".[14] At some stage, sensors or LOCs may be made part of our very cells, report on our biological processes, and switch certain cells off or on, to help in the treatment of diseases.[15]

That may be some time off, though probably not more than a decade. However, a world in which "things" more than people transmit data over the Internet to each other is already coming into existence: the "Internet of Things".[16] This may still be on a small scale: a sensor may note that you are out of the house, and reduce the heating. But it can also be done on a vast scale, e.g., to report on environmental changes. Nano-sensors and –transmittors can also be linked to larger systems: e-Health technologies will include "*health information networks, electronic health records, tele-medicine services, personal wearable and portable mobile devices, health portals and other tools*".[17]

They can be helpful, e.g., by allowing you through passport control more quickly if you have a passport with an RFID chip. Or by allowing tele-medical help to be given quickly.

But nanotechnologies and the Internet of Things can also be highly invasive, as when companies, or state agencies, obtain data on you from a variety of devices directly or indirectly linked to you and create a profile from this. Companies could advise you on better energy consumption, or make you "special discount offers" - or they could charge you more for something they know you urgently need. State agencies - including both health care providers and others with access to your "e-health" data - may "advise" you on healthier lifestyles - or punish you for using your welfare payments "improperly" (the UK Government is already considering banning people receiving such payments from using them to buy cigarettes or alcohol), or deny you treatment because of your lifestyle choices.

Big Data, Smart Data? [18]

The Internet itself, together with nanotechnology and the Internet of Things will generate enormous amounts of data that are directly or indirectly linked to us, or our homes, households or cars. But there are also other major data sources that are increasingly made available online and with little constraint for wider use: population-, company- and land registers, collections of (statistical) data on the environment, crimes or traffic incidents data on an area-by-area or street-by-street basis, statistical health data, etc., etc., etc. Some of these data sources will become "richer" - more detailed, and more personal - because of the Internet of Things.

Increasingly, Governments wish to make these "rich data resources" available for socially beneficial uses, such as determining environmental factors such as street lighting that lead to lower crime rates, or discovering links between social factors and health. Researchers are naturally keen on them; and companies want to exploit them for commercial purposes. What is more, they all want to be able to combine, match and analyse these data, from all these sources. This accumulation of vast and complex information databases, and their exploitation, is referred to as "Big Data".

In theory, from these "big" resources, far-reaching inferences can be drawn, on which business (and government) decisions will increasingly come to rely. However, it is not easy to turn "Big but dumb" data into "Smart Data" (the new catchword):[19]

> Systems of decision have to provide relevant, useful, actionable, intuitive, digestible and interactive information to the right person at the right time. The next generation of analytics are systems of decision that can provide the relevant information to every system user, in work context, to make smart business decisions.

Sometimes, the results of these systems may be straightforward and linear: "*If X occurs, do Y because the [big] data shows that this will [always] lead to Z*". But that will be rare. Much more often, indeed increasingly the norm, will be an output that is in reality a probability: "*If X occurs, do Y, because the [big/smart] data analysis shows that this will probably lead to Z*" (or at least, *Z* will be more probable than if you didn't do *Y*). The conclusion ("... *will probably lead to Z*") is based on the automatic analysis of many factors and data from many sources, i.e., on a (possibly dynamic) algorithm; and the conclusion is used to take decisions, including decisions on individuals.

In that sense, "smart data" in effect create "profiles", as discussed under the next heading - and it suffers from the same built-in - but rarely acknowledged or understood - limitations and dangers as profiles, as discussed in section 2.3. "Smart data" may be less smart than assumed.

Profiling[20]

Profiling is one of the most challenging, and most worrying, developments relating to the use of the Internet, the Internet of Things, and "Big Data", yet is becoming pervasive. It means collecting and using pieces of information about individuals (or that can be indirectly linked to individuals) in order to make assumptions about them and their future behaviour.[21]

For example, someone who buys a pram will often also shortly thereafter buy baby clothes and nappies. In more abstract terms, "*people who did X and Y often also did Z. You did X and Y, so we will treat you as if you are likely to do Z*". But that is a very old-fashioned minimal profile, using obvious factors. In a world of massive "Big Data", innumerable elements can be factored in, and links can be established between factors that no-one would have thought were linked in advance.

> "Big data is not just about lots of data, it is about having the ability to extract meaning; to sort through the masses of data elements to discover **the hidden pattern, the unexpected correlation**" [22]

Moreover, the logic used in the analyses - the profiling algorithm - can either be determined in advance and left unchanged (static), or, as is increasingly the case, be constantly dynamically re-generated and refined through loops linking back to earlier analyses, in theory constantly improving the outcome. Moreover, the refining is increasingly done by the computer itself, using "artificial intelligence".

According to an already-mentioned UK government study, the technologies for "modelling human behaviour", aimed at "understanding complex relationships" are already widespread "*in place of animal testing; use of social identity theory in conflict management, and simulations and gaming in contingency planning; and better informed decisions by individuals and institutions*"; and "*show promise*" in other areas including fighting crime.[23]

There are however serious problems with profiling. As that study acknowledges, in rather under-stated terms:

> "In all cases, the challenge will be to be certain that our understanding of human behaviour (both individual and collective), and our capability to capture that understanding in computer code or in sets of rules, is sufficient for the intended use of the model."

In practice, profiles and "human behaviour models" suffer from serious statistical limitations; almost inevitably (but unnoticeably) perpetuate social inequality and discrimination; and tend to become utterly intransparent and consequently almost impossible to challenge. I will discuss these problems in more detail in section 2.3, below. Here, I may already note that profiling poses a fundamental threat to the most basic principles of the rule of law and the relationship between citizens and government or between customers and businesses in a democratic society.

Biometrics, Genomics, Proteomics, and Behavioural Analyses[24]

The recording of personal characteristics of individuals for various reasons - for law enforcement or more general State control (in the form of "mug-shots" etc. of criminals or suspects or "subversives"), or to control access to a place (like a country) or a site (like a workplace), or for other reasons - is nothing new.[25] For a long time, only relatively coarse descriptions, and signatures, were all that was available. In more modern times, from the late-19th Century on, photographs and fingerprints were added.[26] More recently, retinal patterns, facial structure, hand geometry (contour), vein patterns, and basic DNA analysis have been recorded as means of biometric identification; their use has expanded at an incredible rate.[27] However, as will be discussed in sections 2.2 and 2.3, below, there is a dangerous tendency on the part of the bodies or authorities relying on such measures to fail to understand, or to ignore, their limitations, even in that context.

Other technologies go beyond identification, to predict matters about us. First of all, there is genomics, the decoding of a person's entire genome, and the use of the information thus disclosed.[28] This is a "phase change" compared to previous genetic (DNA) analysis, because the full genome of an individual exposes a wealth of very sensitive personal information about that individual, as well as her relatives. The obtaining of full genome data on large sections of the population is increasingly proposed as a "breakthrough" in the fight against many illnesses.[29] Beyond even that, there is the emerging science of proteomics: knowledge about not just the DNA, but the entire protein complement in a given cell, tissue or organism.[30] Both genomics and proteomics can be used to identify markers for a specific disease or trait, and with epigenomical and bioinformatical advances can lead to new understandings and treatments. These new bio-industries depend on

"*increasingly complex analysis of gene, protein and epigenomic function, including pattern recognition, data mining, machine learning and prediction techniques*", facilitated by the already-mentioned increases in computing power, and relying on the availability of "*publicly accessible [genetic and proteomic] databases*", i.e., on Big Data[31]

However, there are serious ethical and legal issues raised by this. I will discuss these in section 2.3, below.

Cloud computing[32]

Finally, I must mention Cloud Computing. In layman's terms, this means using computer services – software or data storage – not at your own computer but somewhere on the Internet, on servers operated and managed by others; examples are web-based email (like Hotmail or Gmail), music and video streaming, photo sharing, social networking, payment services, or online office applications (like word processing or spreadsheets).[33]

Cloud computing itself is not a new technology, but a relatively new way of delivering computing services. It came about because the computing giants (such as Google, Amazon, Microsoft and eBay) built massive data centres with very fast connections to the global Internet to run their own businesses, and then spotted the revenue potential in offering spare data storage and computing services to other companies. These data centres can be located anywhere around the world, inside or outside the EU, but most of the main current ones are based in the USA.

Cloud services can bring many benefits to users, particularly convenience and flexibility, reduced costs, ease of use, improved access to online content, and automatic maintenance and updating. However, there are also important worries which centre on control of the data and their geographical location. Who has access to them? How can they be used? How easy is it to move the data from one cloud service to another? How secure are they? Who is responsible if the data are lost or misused?

Crucially, as it is put in a recent EU study to which I will return later, cloud computing results in:[34]

> "[A] quasi-impossibility for EU [and, one might add, other European and non-European] citizens to know exactly what has been done with their personal data when it is processed by companies either using or providing cloud services."

Current data protection legislation does not provide adequate answers to all these questions. There are ambiguities regarding the role and responsibilities of cloud service providers; when EU or any specific national law applies and when it does not; enforcement and redress; transfers to countries outside the EU; and foreign law enforcement authorities' (including especially U.S. authorities') access to data. If these issues are not addressed in a comprehensive, effective and "future-proof" way in the reviews of the European data protection frameworks, it will be effectively impossible to safeguard the fundamental right to privacy protected by the European Convention on Human Rights, the European Charter of Fundamental Rights, and the more specific European data protection instruments.

The result: an uncontrollable global surveillance monster?

From a 20th century perspective, the technological developments described above - *nanotechnologies and the Internet of Things (but of sensors and things related to and reporting on us), "Big Data" and supposedly "smart" analyses of the data, resulting in "profiles" and behavioural predictions that will increasingly determine how we are treated by companies and State agencies, all happening in a "cloud" that is far from virtual, but in stead consists of servers to which many entities can have access, across borders (but to which some, including U.S. agencies in particular, have more access than others)* - all these create an entirely new, global data environment. While we are promised many gains in terms of medical treatment and health, the environment, commerce, culture, work and private life (cf. section 2.2, below), there are clearly also major threats.

These threats centre around the "tsunami" of data, of personal data, that is being created, and the lack of existing, or even possible, effective controls:

> "The Internet is a surveillance state. ... All of us [are] being watched, all the time, and [the thus-generated] data [are] being stored forever. This is what a surveillance state looks like, and it's efficient beyond the wildest dreams of George Orwell. ... If the director of the CIA can't maintain his privacy on the Internet, we've got no hope. ... Welcome to an Internet without privacy. ..."[35]

The problem is not just the size of this monster: it also stems from socio-political developments, and from the inadequacies of traditional systems of checks and balances and control in this new context. As we shall see in section 2.2, socio-political trends tend to encourage the generation of ever-greater amounts, and ever-more personalised, data and use of data (and of profiles), with ever-less respect for informational self-determination or human dignity. However, policy-makers tend to be ignorant of the serious risks and limitations inherent in the new data uses and analyses; they are discussed at 2.3.

At the same time, as we shall note at 3, international human rights law, mechanisms for mutual assistance between national police and judicial authorities, and European and wider data protection laws are all seriously challenged. At 4, I will try to suggest some priorities for addressing these issues, and for hopefully redressing those imbalances.

2.2 Socio-political developments and effects

The technological developments described at 2.1, above, impact on, and drive, major social and political changes. In this section, I will try to briefly identify those developments and impacts, in relation to various types of actors. The aim is mainly to illustrate where and how the technological developments will show their effects. The descriptions below (like those at 2.1) already mention some risks, drawbacks and limitations of the technologies, but I will return to those in section 2.3.

Individuals, groups of individuals and NGOs:

We as individuals will increasingly come to use and rely on the increased capabilities and speed of the (mobile) Internet, both in terms of our peer-to-peer and group relationships,

but also in relation to our physical environment. We will do so both knowingly and unknowingly (albeit rarely unbeknown to others), in all our endeavours.

Professionally, we will work more from home or otherwise away from a central office, and will have more e-meetings and less physical ones, saving ourselves (and our employers) time and money, and reducing our carbon imprint. But this means more of our communications and data are transmitted over e- or m-communication networks and held somewhere in "the Cloud" - which poses serious professional, personal and commercial risks.

Privately and domestically, we will start using "e-" energy and water meters and "smart" systems for our homes and gardens. Our kitchens and cars will be full of sensors and helpful technologies. If we suffer from serious illnesses, or want to help science, we may have nanosensors on, and in, our bodies.

Socially, we will continue to post and share notes, comments, photographs and video-recordings of ourselves and our friends, by email, on social networks and blogs, in games and virtual worlds, by allowing location-sharing, etc. – although, for the reasons spelled out below, we may well become choosier in this, and exercise our rights of encryption, anonymity and deletion ("the right to be forgotten") and data portability more fully (to the extent that they are really granted and can be effectively exercised in the new, global, Cloud-based environment: see at 2.3, below).[36]

Culturally, we will demand better, less restricted access to the vast store of past human creation, and new products: we want whatever we want, wherever we want it, on any device, at any time. We are willing to pay for this, but unwilling to be ripped off or be subjected to unreasonably constraints. Consumers, once they understand the implications, will demand Net Neutrality and Intellectual Property (IP) and Digital Rights Management (DRM) reform (cf. below: *Companies*).

Politically, we will increasingly use the Internet, and our mobile phones, for activist purposes: to express our views and hear the views of others, to organise meetings and rallies and protests, and to publicise State responses (including "ketteling", arrests, beatings and worse).[37] NGOs already widely use the Internet (including the mobile Internet) to publicise facts and opinions, organise campaigns and coordinate lobbying activities regionally and globally.[38] New types of political groupings are being created, less centrally controlled, based on grassroot participation over the mobile Internet, although it is difficult to predict how this will impact on wider politics.

We may come to merge offline information - the things we see, hear and feel - with online information we will receive, ever more continuously, on our mobile devices, and possibly (if they catch on) even on our virtual reality glasses such as "googles": in our social and work lives. We will increasingly operate in "augmented reality".

However, in all of this, we will increasingly leave, not the just the traces we are half aware of about the things we ourselves do on line, over our mobile phones and on our social networks, but also innumerable hidden traces.[39] The "Internet of Things" will expand the

directly and indirectly identifiable traces on all of us exponentially; and "Big Data" will make them increasingly difficult to de-identify or, even if supposedly pseudonymised or anonymised, will fundamentally undermine protection against re-identification (see below, at 2.3, under the heading "*The end of anonymity*").

Once the ordinary (mobile or fixed) Internet user (or the citizen being recorded on CCTV) starts to realise just how exposed s/he is, this will lead to resistance, in the form of "sousveillance", online protest, distrust and boycotts.[40] We may refuse the more intrusive devices, take our social data from the intrusive sites and try to find (or set up) less intrusive ones, and choose a private doctor or shrink, rather than one who makes all our health data available, in insufficiently de-identified form, to thousands of others: health staff, insurers, administrators and researchers.

As we shall see below, under the headings "Companies" and "The State", this is recognised by the latter two in theory, but not in practice. Companies acknowledge that trust is a fundamental condition for e- (and m-) commerce, and Governments know (or will learn) that trust is equally essential for the maintenance of the social and political contract between the citizens and the State. But when push comes to shove, they ignore this. In the end, the "naked citizen" will not forgive them: he (or she) will evade the global corporations and national and international State institutions' seemingly all-seeing eyes.41

All this applies *a fortiori* to people, in particular politically active people, and more in particular human rights defenders (HRDs), in non-democratic countries. They are already learning to use TOR, the U.S. Government-backed (and 80% U.S. Government-financed) system allowing for anonymous peer-to-peer communication,[42] which in 2011received the Free Software Foundation's Award for Projects of Social Benefit.[43] HRDs are offered training in this and other technologies such as FreedomBox[44] by Western NGOs, again often with government backing. I myself have conducted such HRD trainings in Central Asia, paid for by the UK Foreign and Commonwealth Office.[45]

Criminals and victims of criminals

Criminals use all the means of action and interaction used by non-criminals, but for criminal rather than non-criminal ends. That is the only difference between them and ordinary, non-criminal people. A "cyber criminal" is not a special species, but someone who uses the tools available to any of us for criminal ends. In the offline world, a criminal uses an axe or a crowbar; his online brother uses a computer. In that sense, there is nothing particularly special about a "cyber criminal" (or indeed about "cyber crime" - but see the further discussion below, under the heading "*The State*").

But of course crimes are committed over the Internet, and there are victims of those crimes – including children - that require protection. States are understandably keen to capture the traces and trails left behind by criminals on the Internet and in the Cloud. However, the more organised criminals (like the Columbian and Mexican drug cartels) have extremely sophisticated counter-surveillance technologies (and their own police/informant

surveillance programme).[46] This kind of technology-for-the-criminal will only become cheaper, more readily available and easier to use.

The risk is that while ordinary, non-criminal citizens are increasingly placed under continuous, intrusive, suspicionless surveillance, the really serious criminals and terrorists will have the means to avoid this. Worse, the technologies of political control deployed against serious criminals and terrorists in democratic countries are the same technologies that are used by repressive regimes against political opponents, including non-violent ones. I will return to this, too, below under the heading "*The State*", and in the subsequent sections.

Companies[47]

Network providers

Internet Service Providers (ISPs) provide the traditional portals to the Internet for fixed-based personal computers. They used to see their role as mere providers of just that: a means to move data around the Internet, and nothing more. However, there are increasing pressures on them and other major network providers to take a closer look at those data.

First of all, as discussed later, States, also acting through the EU, want to enrol the ISPs in their efforts to spot Internet traffic related to crime (including in particular child pornography), terrorism and wider "extremism".

Second, companies that provide goods and services in the form of data (which covers a great many things, from audio, e-books, music, images and video to software) want to retain control over their intellectual property rights (IPR) (and extend those rights), and use "digital rights management" (DRM) technologies to that end. They too want ISPs and other providers to monitor the use of the devices that access the Internet - which in practice can only be done by highly intrusive Deep Packet Inspection (DPI) of all traffic (i.e., not just of traffic in relation to some activity that gives rise to a reasonable suspicion of unlawful actions) - which the European Court of Justice has now ruled to be disproportionate and contrary to human rights law.[48] The excessive demands of major companies pushing for draconian - and privacy-destroying - enforcement of IPR has led to massive opposition from civil society and the European Data Protection Supervisor, but major companies are continuing their efforts to sustain outdated business models nonetheless.[49]

Third, providers could increase their profits if Net Neutrality were ended and they could charge different users of the Internet (companies and consumers) differently depending on their uses. Mobile network operators (MNOs) and search engines, who are becoming the leading providers of access to the Internet and online services, are often especially opposed to Net Neutrality, and in favour of being allowed to introduce differential pricing for different "service" or access levels. In 2010, Google and Verizon published a "*Joint policy proposal for an open Internet*" that was in fact aimed at creating a separate, priviliged premium 'Net.[50] This was strongly criticised by U.S. digital rights groups.[51] However, similar proposals continue to be made, also in Europe. Although several countries have

adopted laws enshrining Net Neutrality as a fundamental principle, and although the European Data Protection Supervisor too has criticised the idea of ending Net Neutrality because it implies the use of DPI in order to be effective,[52] the EU Commission continues to prevaricate.[53]

Social network providers

As noted, many people are extremely active on social networking sites, as social, cultural, political and professional activities. As result, these networks accumulate enormous amounts of highly sensitive personal data. It is becoming impossible to truly de-identify those data: a recent report showed that "*easily accessible digital records of behavior, Facebook Likes, can be used to automatically and accurately predict a range of highly sensitive personal attributes including: sexual orientation, ethnicity, religious and political views, personality traits, intelligence, happiness, use of addictive substances, parental separation, age, and gender*."[54]

Prospective employers, and insurance companies, are already looking at individual Facebook and Twitter accounts of individual job applicants and claimants. But the "mined" data would be even more valuable - albeit far from error-free, as discussed at 2.3, below.

This is likely to give rise to several parallel trends. First, as already noted, once individuals become aware of how exposed they are on these sites in respect of past and present activities (and shortly, also in terms of predicted future behaviour), they are likely to exercise their right to withdraw from them and have their previous data deleted (the "right to be forgotten"/*le droit à l'oublie*). Or they may start to deliberately make misleading entries, to enhance their "scores". They may also ask for more privacy-friendly networks, and there are likely to be new companies being created to cater to that demand. Whether Facebook (*et al.*) will rise to the challenges remains to be seen.

Companies offering other goods and services online

For companies, the amount of data they can obtain on their customers and potential customers in the new environment offers previously unheard-of possibilities. They can tailor their products and services much better to the right categories of individuals, improve their customer care, and find new possible clients. In addition, the data they hold on their customers or visitors to their websites is itself a major resource, that companies often want to exploit: they wish to monitise "their" data (meaning really: the data on their customers and visitors), by selling them or sharing and matching those data with other data. That can be data held by sister-companies or third parties, but can also include data from publicly or commercially available "big Data" databases.

Personal data is thus the fuel that powers the digital transnational e-economy. However, the break is trust.

Lack of trust has been repeatedly identified by the EU Commission as one of the main barriers to a fully-functioning internal market, and the development of pan-European e-

commerce. Concerns about the abuse of consumers' personal data, and of security breaches, form a large part of this distrust.[55]

Hopefully, companies will wake up to these challenges, and will make and offer products incorporating "privacy-by-designs", or "privacy-by-default", certified by demanding, a high-quality European privacy seal.[56] This could be stimulated by offering offering benefits to products and services that have such a certified seal, e.g., in terms of public procurement.

Globalisation and the Cloud

Finally, I should note that commerce, and especially online commerce, is increasingly global: we visit foreign and indeed non-European (especially U.S.) websites and buy goods and products (including software) online. Moreover, company data from companies everywhere (including Europe) is increasingly held and processed in the Cloud - which in practice often means on servers based in the USA. And data from European companies held in such non-European jurisdictions, and data from companies established in such non-European territories, may be subject to the jurisdiction of the relevant foreign country. This is especially true of European data that end up on U.S.-based servers, and of data on anyone (including Europeans), held by U.S.-headquartered companies.[57] I will return to the challenges this poses in section 3.

The State[58]

The technical developments described at 2.1, above, feed into the major social and political trends of the day. We all worry about terrorism, child pornography and serious international organised crime. The State also worries about exploding budgets for health care, education and social welfare. Governments want to encourage "good" behaviour, and discourage "bad" behaviour (in a much wider sense than "non-criminal" vs. "criminal"). In some countries – in the EU, in particular, the UK – the authorities believe that the more information its officials can get, and share, the better it can tackle social ills, be this teenage pregnancy, obesity or "extremism" that may lead to terrorism.[59]

e-Government systems typically contain large quantities of sensitive personal data on entire populations, shared between government departments using specific "gateways" contained in legislation. "Back office" systems focus on the more effective processing of data and the enabling of new services (including fraud detection and prevention related to benefit payments and tax returns) out of the citizens' gaze. "Portals" enable citizens to interact online with the government, supplying information such as tax returns and applying for services without the cost to either party of face-to-face or telephone conversations and manual form processing.

Electronic Health Records (EHRs), digital versions of medical records, are being nationally specified in countries including France, the USA, Canada, Germany and the UK. Plummeting costs mean that the sequencing of patients' genomes is likely to become routine. The ageing of the baby boomer demographic in North America and Europe is likely to produce strong cost pressures for the out-patient treatment of chronic health

conditions in older citizens, and we are therefore likely to see much more detailed information automatically gathered on physiological indicators and more general lifestyle data for the elderly and the less well.

Law enforcement and intelligence agencies have been eager to gain access to the wide range of personal information that has become available from information systems created for very different purposes. This trend has intensified since 2001 under the rubric of "national security" and anti-terrorism purposes – including monitoring of financial transactions to reduce money laundering. Many governments have taken powers to require that Internet Service Providers make their networks "wiretap-capable" and retain data about customers' communications for later access by officials. Compulsory data retention on everyone, without any specific indication of criminality, is officially required in the entire EU under the Data Retention Directive - but this has been found to breach the constitutions of several EU Member States, and is being challenged in the ECJ as in violation of fundamental European human rights law. Yet in other countries - again, specifically the UK - the authorities remain keen to access all communications data for preventive monitoring purposes, through DPI. Data protection is seen as an obstacle to State policies of this kind.

This leads to the absurd situation in which the U.S. Government on the one hand develops or promotes the development of surveillance systems, while on the other hand it supports and finances TOR and other tools to help human rights defenders evade them; and in which certain European Governments similarly simultaneously try to have "black boxes" installed in their domestic communications networks, while training HRDs in other parts of the world in surveillance evasion.[60]

Indeed, the ubiquity of personal data and data gathering means that the default position is shifting from state and private bodies having to decide to collect data to one in which they have to make an effort not to collect (increasingly sensitive) data.

There are three further issues to be mentioned in this respect, in relation to law enforcement and national security in particular. First of all, the lines are being blurred between law enforcement and other ordinary State functions. In the UK, this is often referred to as making the State's activities more "holistic": social workers, teachers, medical professionals and the police should (so it is argued) work more smoothlessly together to tackle the major social evils of our time, from obesity to drugs abuse to "extremism". This leads to calls for wide and easy data-sharing between the different agencies, without too much regard for data protection.[61]

Second, in particular in the fight against terrorism, the lines between law enforcement and national security activities are increasingly blurred: law enforcement agencies (LEAs) and national security agencies (NSAs) are increasingly working hand-in-glove. This may be desirable from the perspective of efficacy of the anti-terrorist efforts, but it is highy problematic in some respects. In particular, it means that domestically, the special rules created for NSAs, which often depart from the normal ones to allow them to operate "in the shadows", are being extended to LEAs, who were traditionally subject to strict rules and

close (judicial) supervision. The police increasingly use undercover agents, infiltrators and inside collaborators, often in highly unethical ways.[62] LEAs are also increasingly themselves using malware and hacking tools, both domestically and transnationally, and are increasingly specifically authorised to do so by their domestic law:[63]

More problematic still, given that much of Europe's data protection rules are based on EU law, is the fact that **the EU has no competence over matters of national security**. Indeed, it has been argued with reference to a (rather unfortunately phrased) ECJ ruling, that even the disclosure of data that are subject to EU data protection law to NSAs, even NSAs abroad, for national security purposes, is outside EU data protection law.[64] That interpretation may be wrong (it is in my opinion),[65] but it merely serves to underline the problem.

This must be seen as linked to the third issue: the treaty arrangements between many States relating to (i) mutual cooperation in law enforcement (in particular Mutual Legal Assistance Treaties or MLATs), and quite separate from that (ii) intelligence sharing between NSAs. MLATs in particular are increasingly by-passed by some LEAs: the U.S. authorities are increasingly seeking access to data held abroad directly, by requiring U.S.-headquartered companies to hand over any data they can access, including data held in Europe. This clearly contravenes a fundamental principle of international law, unambiguously stated by the Permament Court of International Justice in the *Lotus* case:[66]

> "Now the first and foremost restriction imposed by international law upon a State is that - failing the existence of a permissive rule to the contrary - it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention." (pp. 17-19)

By contrast, the German LEAs apparently do rely on MLATs - i.e., on a convention in the sense used by the Court - when seeking access to Cloud data outside Germany, in particular in the USA.[67]

The illegal practice of U.S. LEAs by-passing MLATs means that there are no guarantees (such as can be required under MLATs, or the Cybercrime Convention) that the data are not passed on to U.S. NSAs. In fact, U.S. law - more specifically the PATRIOT Act - provides almost no protection against this.

Worse, another U.S. law, the Foreign Intelligence Surveillance Amendment Act (FISAA) of 2008, give U.S. authorities virtually unrestricted power to conduct political surveillance on foreigners' data accessible in U.S.-based Cloud servers;[68] and the Grand Chamber judgment on the EU – USA PNR Agreement of 30 May 2006[69] can be read as suggesting that neither this issue nor the issue of data sharing between EU Member States' LEAs and NSAs, can be addressed in EU law.

In other words, there are major holes in at least the EU's otherwise quite comprehensive framework for data protection, most glaringly in relation to data that are

held on U.S.-based Cloud servers, but also in relation to data sharing between EU Member States' LEAs and EU Member States' NSAs, and between EU Member States' NSAs and non-EU ones, including in particular U.S. NSAs.[70]

The Council of Europe's Convention No. 108 does, in principle, apply to processing of personal data by the State Parties for national security purposes, and thus also to the making available of personal data by LEAs to NSAs, whether within a country or across borders (subject to a limitation provision, but one that is at least on paper aligned with the usual ECHR tests of lawfulness, necessity and propoprtionality). However, in practice not enough attention has been given to this issue.

I will return to these matters in section 3.

2.3 Risks, limitations and defects of the technologies

As noted above, unless restrained, the technological developments listed at 2.1, combined with the social and political trends noted at 2.2, are likely to result in an historically unprecedented surveillance environment, in which we will all be judged and dealt with on the basis of ubiquitously-generated data, both on us individually and in aggregate form on us all as citizens, or transport- or energy users, or patients or customers, etc.. However, there are risks and limitations inherent in the technology, and the data, and the uses of those data, that those who do use the data to make decisions about us or to take measures that affect us are often either unaware of or deliberately ignore. This section tries to briefly describe those risks and limitations, as before with reference to more in-depth studies and materials.

The end of anonymity?[71]

Anonymisation means removing or obscuring information from data sources that would allow direct or indirect identification of a person.

One of the big advantages of anonymisation is, for example, to allow research that would otherwise not be possible due to privacy concerns. For instance, using everyone's medical records to find disease patterns could improve health care, but would also seriously infringe on people's privacy. It is claimed that the solution is to remove direct identifiers such as names, birth dates, and addresses, so that the data cannot be traced back to individuals. Governments, industry and researchers tend to claim that effective anonymisation of personal data is possible and can help society to ensure the availability of rich data resources whilst protecting individuals' privacy.

Unfortunately, this is simply not the case – as scientists have known for a long time. For example, in 1997, researchers were already able to re-identify individual patients from a large set of medical records reduced to post code and date of birth. In 2006, a study found that if you know how a user rated just six films, you can identify 99% of the users in the Netflix (an online video rental service) database.

How is this possible? The main problem is that effective anonymisation does not just depend on stripping away direct identifiers (name, address, national identification number, date of birth) from a data set. Instead, the relevant measure is the size of the "anonymity set" – that is, the set of individuals to whom data might relate. If you're described as "a man" the anonymity set size is three and a half billion, but if you're described as "a middle-aged Dutchman with a beard" it is maybe half a million and if you're described as "a middle-aged Dutchman with a beard who lives near Cambridge" it might be three or four.

Pseudonymisation, that is replacing the name and other direct identifiers with a new identifier, – e.g. "John Smith, 1 High Street" becomes "person 45684231" – does not resolve this problem either, irrespective of whether, or how well, the pseudonym is encrypted. Suppose we gave everyone in the world an ID card with a unique number. What will happen? You start with a single pseudonymous incident, such as a drug prescription: "human no. 45684231 got penicillin on 3 Feb 2009". The anonymity set size just shrunk from seven billion to a few hundred thousand. Then along comes a second incident: "human no. 3,265,679,016 got codeine on 14 May 2009". Now it's down to a few hundred or even a few dozen. A couple more incidents, and the individual is uniquely specified.

As more and more "Big Data" data sets are released, the possibility of identifying people in any single "anonymised" data set by using data from other large data sets increases greatly.[72] With current – and foreseeable future – technology, it is safe to say that anonymisation no longer works when identities are actively sought. This poses major challenges, in particular in relation to "Big Data", that are insufficiently acknowledged or addressed to date.

As we have seen, we cannot rely on anonymisation to be completely secure. In this context, transparency regarding the technologies being used, open peer review by security engineering experts and responsible disclosure procedures will at least provide early warnings over compromised databases and raise standards.

Profiling and the baserate fallacy

As noted earlier, profiling - also more euphemistically referred to as "social sorting" - is increasingly used in many context, to predict something about individuals. In marketing, the aim is merely to identify a potential customer. In epidemeological research (such as breast cancer screening), the purpose is to identify targets for further examination. In the (near) future, they are likely to be used, indeed to some extent they are already used, to try and identify *potential* criminals or terrorists. As it is put in the UK Government Technology and Innovation Futures report:[73]

> "Analysis of live data streams by 'artificial intelligence' agents will allow more proactive surveillance, potentially alerting operators to crowd control problems or [**to] identify persons of interest.**"

But that are three main problems with profiling:

1. The base rate fallacy[74]

The first problem arises when profiles are used to identify rare phenomena, and is referred to in statistical literature as the "base rate fallacy". This phrase is used to refer to the mathematically unavoidable fact that if you are looking for very rare instances in a very large data set, then no matter how well you design your algorithm, you will always end up with either excessive numbers of "false positives" (cases or individuals that are wrongly identified as belonging to the rare class), or "false negatives" (cases or individuals that do fall within in the rare, looked-for category, but that are not identified as such), or both. It is important to stress the mathematical inevitability of this: you cannot improve the data set, or the algorithm, to avoid these debilitating results.[75]

Statisticians know this. Epidemiologists know this: they know that it is effective to screen all women over the age of 50 for breast cancer, because in that group there is a sufficiently high incidence of that affliction. But it is not effective to screen all women over the age of, say, 15, because that would thrown up enormous numbers of "false positives", which would deplete hospital resources. Exactly the same applies in anti-terrorist screening based on profiles: there are (thank God) simply not enough terrorists in the general population, or even in smaller populations (say, all Muslims in the UK of Pakistani or Saudi origin), to make the exercise worthwhile. The police and the security services would be chasing thousands of entirely false leads, while some real terrorists would still slip through the net.

The conclusion must be that profiles should never be used in relation to phenomena that are too rare to make their application reliable, such as trying to identify (real, let alone potential) terrorists from a large dataset.

2. Discrimination by computer

Apart from the base rate fallacy (which is well-known to statisticians, albeit ignored by too many others), the wider implications of algorithm-based decision-making have not been as widely researched as they should be. However, the leading research in this area, by Oscar Gandy, shows that (in David Barnard-Wills paraphrase):[76]

> predictive techniques and 'rational discrimination' – statistical techniques used to inform decision making by 'facilitating the identification, classification and comparative assessment of analytically generated groups in terms of their expected value or risk' – perpetuate and enforce social inequality.

This built-in risk - that profiles will perpetuate and reinforce societal inequality and discrimination against "out-groups", including racial, ethnic and religious minorities - grows dramatically with the massive, almost explosive growth in data described at 2.1, above, and the pressures to use this "Big Data" and data generated by people and things for commercial or social purposes, described at 2.2.

Crucially, this can happen even if the algorithms used are in their own terms perfectly "reasonable" and indeed rational. In practice (as Gandy has shown) the results will still reinforce the inequalities and discrimination already perfidiously embedded in our societies. Crucially, this discrimination-by-computer does not rest on the use of overtly

discriminatory criteria, such as race, ethnicity or gender. Rather, discrimination of members of racial, ethnic, national or religious minorities, or of women, creeps into the algorithms in much more insiduous ways, generally unintentionally and even unbeknown to the programmers.

But it is no less discriminatory for all that. Specifically, it is important to stress that in international human rights law, the concept of discrimination does not imply some deliberate discriminatory treatment. Rather, in the words of the Human Rights Committee established under the UN Covenant on Civil and Political Rights:[77]

> the term "discrimination" as used in the Covenant should be understood to imply **any distinction, exclusion, restriction or preference** which is based on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status, and which has **the purpose <u>or effect</u>** of nullifying or impairing the recognition, enjoyment or exercise by all persons, on an equal footing, of all rights and freedoms.

Only by constantly evaluating the results of the decisions based on profiles can one avoid these effects. It takes serious effort. As Gandy concludes:[78]

> these systems must be subject to active and continuous assessment and regulation because of the ways in which they are likely to contribute to economic and social inequality. This regulatory constraint must involve limitations on the collection and use of information about individuals and groups.

In Europe, this "regulatory constraint" - this protection against discrimination-by-computer - takes the form of data protection rules.

<u>3. The increasing unchallengeability of profiles - and of decisions based on profiles:</u>

Profiles are becoming increasingly sophisticated and complex. As already noted, these days they tend to be dynamic, in the sense that, in the more developed "artificial intelligence" or "expert" systems, the computers operating the relevant program create feedback loops that continuously improve the underlying algorithms - with almost no-one in the end being able to explain the results: the analyses are based on underlying code that cannot be properly understood by many who rely on them, or even expressed in plain language.[79]

This ties in with both earlier topics. First of all, such sophisticated profiles will have been tweeked in the direction of either higher "false positive" or "false negative" rates. Without understanding this, a user can seriously misinterpret the results.[80]

Secondly, it is especially in such dynamic systems that the risk of reinforcing engrained biases is greatest: feedback loops have a tendency to amplify such biases. Yet again, the very complexity of the algorithm tends to mask such effects: many users will not be able to detect such discrimination, or may be uninterested in it as long as the systems work to their benefit.

At the same time, the data subjects - the individuals included in or excluded from profile-based selections - are less and less able to challenge those results, at least in their individual cases. If a company says it will not give you a loan because your income is too low, or you have a history of bad debts, you can challenge that if the figures or facts the company used are incorrect, or outdated.

But increasingly, a company (or State agency) will tell you it will not give you a loan, or will not invite you to an interview (or has placed you on a terrorist "no-fly" list, or worse), "***because the computer said so***": because the computer generated a "score" based on a profile, that exceeded or did not reach some predetermined basic level. If you ask for an explanation (if, that is, you actually find out that such an automated decision has been made on you), the company or agency (or at least the person you are dealing with) is likely to be unable to explain the decision in any meaningful way. They might provide you with examples of some of the information used (age, income level, whatever), but they will not give you the underlying algorithm - partly because the respondent him- or herself does not know or understand that algorithm, which is in any case constantly dynamicaly changing, and partly because the algorithm is a "commercial secret".

Even at a higher level, it will be effectively impossible to verify the risks inherent in those profiles: i.e., to assess the level of "false positives" and "false negatives", or the possibly discriminatory effect of the profiles on certain groups, without the full, in-depth cooperation of the company or agency generating the profiles. Yet the latter are likely to be unwilling to be so helpful, unless compelled to do so by law.

Profiling thus really poses a serious threat of a Kafkaesque world in which powerful corporations and State agencies take decisions that significantly affect their customers and citizens, without those decision-makers being able or willing to explain the underlying reasoning for those decisions, and in which those subjects are denied any effective individual or collective remedies.

That is how serious the issue of profiling is: it poses a fundamental threat to the most basic principles of the Rule of Law and the relationship between the powerful and the people in a democratic society.

The fallability of biometrics[81]

As Bohm and Mason have pointed out:[82]

> … identifiers (such as names and other attributes) represent attempts by society to provide an infrastructure for referring tolerably unambiguously to a person in the context in which that person moves.

Note the "tolerable unambiguity". It is crucial.

Names are not very good identifiers: there are many people called "John Smith" (and there is probably even more than one person called "Douwe Korff", although I seem to be the only one on the Internet so far); and single individuals may be known by different names in different contexts ("Dad", "Jim", "Mr Smith"). Even with other information, such as an

address or a birth certificate, the identifiers are far from conclusive: one person with one particular name may have been the person who lived at a particular address at a particular time (according to the records), but the fact that he no longer lives there does not prove it is not him; nor does the fact that a person with that name who can show that he lives at that address now conclusively proves that he is the person to whom an earlier record joining that name and address relates. In the real world, Bohm and Mason suggest:

> Instead of seeing 'identity' as a collection of more-or-less verifiable attributes of a person, … it is much more productive to see it as a relationship.

A person is (sufficiently) identified in a particular context if the party that wants the "proof of identity" is given information that suggests that the person in question is the supposed person, adequate to the purpose and context. Most often, that party is in any case not really interested in a person's "real" identity: all he wants to establish is that the person presenting him- or herself (in flesh and blood or in the virtual world) is entitled to what he or she demands: access to a transport system, or the purchase of a good or service, etc.. This is why Privacy Enhancing Technologies (PETs) can play such an important role: they can avoid the disclosure of identifying details altogether.

Here, we must note that for *all* identifiers, the level of identification they allow is limited and relative. We try to identify a person "tolerably unambiguously" for the specific context. A shop will gladly sell me things if I pay using my wife's bank card; and the bank will pay without demur, even though its standard Terms amd Conditions tell my wife she is not allowed to let me use her card. London Underground will let me use the "Tube" with someone else's travel card (called the "Oyster Card"). Etcetera. In many circumstances, the identifying instrument is relied on in a way which is not very demanding in terms of identification. Usually, we happily live with the "ambiguity" mentioned by Bohm and Mason.

In any case, the supposed identifiers are also inherently far from conclusive. We know this of names. We should know it also, if we think about it, of most ordinary, "old-fashioned" documents, such as pre-biometric passports and driving licenses. In most case, it matters little - but sometimes it matters a lot: just think of the use of falsified passports by the Israelis in the recent assassination of a Hamas official in Dubai. In that case, the "ambiguity" turned out to be not "tolerable".

We tend to think that the personal features and attributes that we have started to record more recently are devoid of such limitations: that they really do conclusively identify individuals. In practice, if one takes into account the actual ways in which the technologies that deal with them are applied, this is simply not true.

Fingerprints are said to be unique to each individual; they even differ between identical twins.[83] However, in practice the police and the security services do not use complete fingerprints: instead, they compare "points of comparison", places wher ridges whirl and split: it is this very reduction in comparison, developed by Sir Francis Galton in the late-1900s, that allowed for the development of the science of fingerprint matching. But of course, this very reduction also introduces an amount of imprecision, ambiguity.[84]

A "match" is declared when a "sufficient" number of points on the examined print correspond to the same points in a print held in a collection or database. But what is "sufficient"? Some police departments require 10, others 12, matches; some are satisfied with eight. Ultimately, "*the decision to declare a match is a subjective one*". [85] In other words, a "match" means a likelihood, not 100% certainty - although such certainty is regularly, falsely, claimed by the authorities - and even the experts - in court.

Unsurprisingly, therefore, in spite of the claim of complete uniqueness, there have been cases, such as that of Scottish police detective Shirley McKie and U.S. lawyer and Muslim convert Brandon Mayfield, in which fingerprint identification was shown to have been wrong. [86]

Another problem is that fingerprints can be "planted", by corrupt policemen or others. Last year, the "Chaos Computer Club" (CCC) in Germany captured a fingerprint of the Interior Minister, Wolfgang Schäuble, who supported the use of biometrics in identity cards. CCC may now be able to "leave Schäuble's fingerprints" in embarrassing places - which could lead to a "match" that in normal circumstances might suffice to implicate the person whose prints were found in nefarious activities. Not everyone will be given the "benefit of the doubt" that will now of course be extended to Schäuble's fingerprints.

The other biometrics mentioned suffer from the same, or worse, defects. Whenever we rely on records of retinal patterns, facial features, hand contours or vein patterns, we really rely on an abstract of the full record: from the original - or rather, from the image of the original - an algoritm is created, based on a number of marked points or similar comparable features; and retinal, facial, or hand contour or vein patter comparisons are, in reality, comparisons between the algoritm derived from one such image and the algoritms held in a database.

By the very nature of these technologies, a "match" indicates a "tolerable unambiguity", an acceptable, relative level of certainty - not absolute certainty.

The systems also inherently suffer from limited tolerance: they only work (reasonably) well under certain conditions. Face- or gait recognition in particular suffer from this: they work reasonably well in the laboratory or in other tightly-controller circumstances, such as when a person can be made to stand in a particular position at a particular spot, in pre-designed lighting (as in airport checkpoints). Even then, they are not that reliable: standing in the queue for passport control at London Stansted airport, one can often see fellow passengers who have enlisted in a programme that is supposed to allow them through by looking into a camera, without a human check, being rejected by the system.

The systems are even less reliable when used "in the field". The idea that a "drone" (or even a satelite) flying high up in the sky over Afghanistan can adequately identify a specific individual from his facial or other features or gait, is fanciful - and in circumstances in which the "drone" can shoot as well as observe, potentially lethal.[87]

The above is also true when it comes to the use of DNA samples for identification purposes (I will come later to the use of DNA and genomics in risk prediction). In practice, not the

complete DNA of a suspect (or dead body) is matched, but an extract, based on the identification of selected strings of nucleotides.[88] Just as with fingerprints, there are variations between jurisdictions as to what should be regarded as a "sufficient" match, for the purposes of criminal proceedings: Bianchi and Liò note that in the UK, a match is only regarded as sufficient for forensic purposes if 13 out of 14 loci (STRs) are matched, in three individual examinations. However, they say that by contrast, "German courts generally consider five or six STRs to be sufficiently strong evidence of identity".[89] Not surprising, there are mistaken identifications by means of DNA:[90]

> In 2000, Raymond Easton, a 49-year-old man living in Swindon was charged with a burglary in Bolton, 200 miles away. His DNA matched some found at the crime scene. The problem was Easton was in the advanced stages of Parkinson's disease, and could barely dress himself. Only after an advanced DNA test was the initial match proved to be a 'false-positive': this is when innocents are identified as guilty, for whatever reason – 'false-negatives' are when the guilty slip through the net.

In criminal cases such as this, there is the time and there are the resources (one hopes) for the more elaborate, more advanced check to be carried out (although a misidentified suspect is still likely to spend time in jail, and to suffer other serious effects). Even then, the police, the prosecuting authorities and the "official" experts are often reluctant to admit to the possible weaknesses in their assessments, unless faced with unsurmountable evidence of the innocence of the accused.

One of the greatest dangers of the introduction of new technologies for the identification of individuals is the excessive belief in their infallability on the part of the general public (and judges and juries), culpably brought about by the exaggerated claims of the developers of the product and the willingness of politicians and other policy-makers to rely on such claims, also for political ends ("*we are installing the most advanced, the most expensive, the most sophisticated system ever designed, in our efforts to fight [whatever they want to be seen to be tackling, but find hard to do in practice]*" - in the light of such propaganda, how can the layperson fail to believe?).

In addition to these limitations on the analyses, there are other factors that affect the probability of a "match". In particular, the match must again be seen in context. Often, claims are made about the probability of "false positives": these are generally said to be extremely unlikely: "*one in a million*" or even "*in 10 million*". One should be extremely wary of such claims. How are these figures arrived at? For instance, if the incidence of a particular STR in the general population of the UK is indeed one in 10 million, one may be tempted to conclude that the presence of that STR in the DNA of a particular suspect shows with that kind of accuracy that that suspect is the person who left the sample at the crime scene. However, within the UK, there are smaller populations that share a much smaller gene-pool. In some towns, there are high concentrations of immigrants from small geographical areas in India, Bangladesh or Pakistan. In those cases, a particular STR may well be a 1,000 times more prevalent in such populations than in the general population of the UK. One in 10 million then quickly becomes one in 10,000. And that may mean that

in the particular town where the crime was committed, there may well be five, or ten, or twenty people whose DNA, in this respect, would match the sample.

One thus has to be careful in one's reliance on DNA evidence, even in court. But if it is proposed to use DNA samples and –records (read: selected abstracts of the real, full strain) for identification purposes in other contexts, the matter gets worse. The time and resources for more in-depth analysis are unlikely to be available. Indeed, such other contexts may well requiring a considerable lowering of the standard. Yet at the same time, the officials using the technology are still most likely to be seduced by the systems' reputation for absolutely certainty.

The Article 29 Working Party, in its Working Document on the concept of "personal data", referred to "features" of individuals that "are both **unique** to [an] individual and **measurable**". However, most of the supposedly-unique biometric "features" that are brought to mind, when used in the real world, are not as unique as they are made out to be. ***Even supposedly straight-forward biometric identifiers have built-in limitations, or are subject to limitations in the way their measurements are used in practice, that mean they should be treated as probabilities, subject to error.***

As we shall see under the next heading, the matter is (much) worse for even more new-fangled technologies presented as almost magically infallible.

The dangers of computerised behavioural assessments[91]

So far, we have dealt with more-or-less factual, more-or-less easy-to-measure "features" of the individual: his or her fingerprints, face-structure, hand contour, or basic DNA - and we have noted the limitations in those.

However, some systems (some existing, some under development) go further: they look at the actions of individuals, at their behaviour, and seek to identify the individuals, or aspects of the individuals, from those. (Some even go beyond that, and try to *predict* a person's future behaviour: we will look at that later). The actions in question - the actions that are analysed in order to identify a person, or something about a person - arise in a range of contexts. They include the use of language, stress and "abnormal" behaviour.

There have been reports on supposedly scientifically-validated "Paedophile Detectors", "Lie Detectors" and "Abnormal Behaviour Detectors". Such systems are not necessarily used to identify a person immediately by name, but they still try to see if a singled-out person should be identified as a paedophile, or as a "liar", or as someone who behaves "abnormally".[92] Once that happens, further identification, and further measures, are likely to follow: The aim is first to assign some attribute to the person, and then, indeed, to "do" something to that person: exclude him from a chatroom, not appoint him or her to a certain job, or even dismiss him, perhaps even to arrest and interrogate the person as a suspected criminal or terrorist.

The claims of accuracy for these products are fancilful. The developers of a "paedophile detection" system claimed "94% accuracy" in distinguishing adults from children on a

website, which is blatant nonsense. The very validity of the claims made for "lie detectors" has been comprehensively de-bunked (even if the research showing they are snake oil has been partially suppressed).[93]

Yet the proven uselessness of "lie detector" systems has not only not deterred security agencies from employing them, they have also not hesitated to go beyond them, to try and develop supposedly even more sophisticated detection systems.

Thus, there were attempts in the post "9/11" US "Total Information Awareness" programme to develop systems that would identify dangerous individuals, people who posed some kind of security risk: these include programs with acronyms like HTID ("Human Threat Identification at a Distance") and TARM ("Threat Activity Recognition and Monitoring"). In July 2002, EPIC obtained documents under the US Freedom Of Information Act showing that NASA was developing so-called "non-invasive neuro-logic sensors" - a kind of brain scanner which its proponents claimed would be capable of detecting the state of mind of a person (the report does not mention the undoubtedly catchy acronym for this program).[94] In 2005, the US scientific community, in cohort with the intelligence agencies, was again actively peddling this line of research.[95]

This seems to have paid off: a few years later, it was reported that the US Department of Homeland Security had launched a call to security companies and government laboratories to develop a "Hostile Intent" project aimed at: [96]

> build[ing] devices that can pick up tell-tale signs of hostile intent or deception from people's heart rates, perspiration and tiny shifts in facial expressions.

Part of the scientific work is apparently carried out in the American Psychological Association's Social and Behavioral Research (SBR) Program.[97]

These ideas appear to have been also taken up in Europe, in particular in the EU's "7th Framework Programme" (FP7), under the heading "*Automatic Detection of Abnormal Behaviour and Threats (ADABTS)*".[98] FP7 also included a project called SAFEE ("*Security of Aircraft in the Future European Environment*"), which is supposed "*to detect unlawful interference onboard aircrafts*". This turns out to be based on:

> "the assumption that an algoritm can distinguish the nervousness of a passenger who is afraid of flying from the nervousness of a terrorist about to attack an aircraft."

The reviewers of the programme rightly called this "challenging" and of "uncertain" practical application, and found the proportionality of this detection system to the right to privacy "questionable". However, they - and we - should stop beating about the bush: these things are not just "challenging", or even (as they say in a brave moment) "beyond challenging" - they are impossible and a nonsense. It is not "challenging" to defy gravity - on earth, it is impossible. And it is seriously misleading to suggest otherwise.

The very first question that should be asked, of all proposed new biometric and similar technologies, is: can they work, even in theory? Are the underlying assumptions, and is the underlying design, valid in straightforward scientific terms? I suggest that the answer, at least in respect of the typically ridiculously named "ADABTS" and SAFEE systems, is a

resounding no. What is more, the onus should be on the developers to show otherwise (which they will not be able to do).

I might add that, even if these technologies could detect some of the things they claim to detect - like "nervousness" - they would still be useless in practice, because of the enormous numbers of "false positives" they would throw up, and the unacceptable number of "false negatives", in the form of undetected, calm terrorists. See the section on "profiles", above.

If such mad ideas will not work, indeed cannot work, and can be shown to be unworkable, then it is madness to pursue them. Madness in terms of money, but above all madness in terms of data protection and fundamental rights. We don't want or need "safeguards" to ensure that such systems will only be used in an "appropriate", "proportionate" manner - we want and need to make sure that they are never used, ever, in Europe (or if we could help it, elsewhere)!

The dangers of genomics and proteomics[99]

There is a fundamental, qualitative difference between genomics and proteomics on the one hand, and the other biometrics used for identification, discussed earlier: ignoring the fact that the genome or proteome of an individual contains enormous amounts of private medical and ancestry-related information about its owner and his or her family leads to a grossly inaccurate and dangerous underestimation of the privacy problems involved.

Specifically, as noted at 2.1, above, both genomics and proteomics can be used to identify markers for a specific disease or trait, and with epigenomical and bioinformatical advances relying on "Big Data" and super-computing, can lead to new understandings and treatments.[100]

However, there are serious ethical and legal issues raised by this. For example, the genomic information on a relative can reveal many intimate and sensitive details about you, and can be obtained and made available without your knowledge or consent. The data thus released may perhaps help you avoid an illness to which you were (statistically) prone, but it is also certain to lead to discrimination in health insurance (unless expressly prohibited by law, as in the USA under the U.S. GINA law), or even denial of a job.

In a forensic context, the availability of such data is likely to lead to a "driftnet" approach of comparing scene-of-crime samples against the DNA of the whole population or large sub-sets of the population, rather than just against that of chosen suspects.

There are two major issues in this respect. First of all, one may feel that it is inappropriate and unfair for an honest citizen to have his or her genome or proteome forensically inspected - and before that, compulsorily obtained - even when there is no evidence whatsoever of the individual having committed a crime. In that sense, the creation of full-genome/proteome databases on all who live in a country is similar to, but even more intrusive than, compulsory suspicionless retention of everyone's communication data, as currently required by EU law (but, as already noted, as also having been found to be

contrary to fundamental rights in several EU States and subject to human rights challenges in the ECJ).

Secondly, even if a State were to limit the collection of genomic/proteomic data to certain categories of people, e.g., to everyone arrested by the police, this could - indeed will - lead to distortions in detection rates: people with relatives with criminal records, or indeed people belonging to ethnically-defined sub-groups with higher criminal conviction rates, would be more likely to be singled out for "special attention" than people who are not so marked.

From a purely actuarial point of view, the denial of health insurance (or the demand for higher premiums), or the higher arrest (and conviction) rates would be perfectly defensible: it keep the health care premiums for "ordinary" people down, and may lead to an overall better detection- and conviction rate. However, just like profiles, in this, the use of genomic/proteomic data can reinforce societal inequalities and discrimination.

The use of these new technologies is dangerous. They should not be widely used, and not used at all in certain contexts, without previous extensive, informed debate, and without the setting of clear rules and limitations.

3. The challenges

The trends and technologies, and the risks and limitations, described above, pose serious challenges to major national, international and European achievements. This section seeks to very briefly identify the ones most relevant to the work of the Council of Europe in general, and the Data Protection and Cybercrime unit in particular. In section 4, I will go on from these to suggest some areas of possible priority to the unit. However, both this and that section must at this stage be seen as very tentative and a basis for discussion rather than in any way finally-formed.

There are four main causes for the challenges:

- the ocean of digitalised data being created and becoming available for analysis, and the resulting "tsunami" of personalised data and "profiles", coupled with the near-impossibility of retaining anonymity, which will fundamentally change the relationship between the individual and those with access to those data and profiles, be those States or corporations, i.e., between the ordinary people and the powerful;
- the globalisation of everyone's activities: civil, political, social, economic and cultural; the transmission of (almost all of almost) everyone's data to the "Cloud"; and the consequent in-principle availability of those data to Cloud companies and to the state authorities of the countries where the Cloud servers are located, in particular U.S. authorities;
- the likely failures on the part of the users of the data and of the profiles to recognise or acknowledge the risks and limitations inherent in them; and
- the fact that the digital-global environment described in section 2 is controlled more by private entities than by States.

Challenges to European human rights law generally[101]

There are three main challenges to European data protection law, arising from the developments described in section 2:

The problem of the margin of appreciation[102]

The European Court of Human Rights applies the European Convention on Human Rights (ECHR) with considerable flexibility. In particular, depending on certain factors, it grants State Parties a certain "margin of appreciation" in the application of the Convention requirements. One can say that this doctrine makes the case-law of the Court often rather unpredictable, or indeed that it has bedevilled the Court's case-law. But this doctrine becomes near-impossible to maintain in a global, and for data borderless, Internet-based society. Unless, in its case-law, the Court urgently addresses this issue, in particular in relation to transnational freedom of expression (which it unfortunately failed to do in the *Perrin* case), it will be unable to deal with the new, emerging world.

The question of companies and human rights[103]

Another major issue under international (not just European) human rights law, is the focus of the relevant treaties (ICCPR, ECHR, etc.) on the responsibilities of States. The ECHR as currently applied is insufficient to regulate the actions (and refusals to act) of private entities involved in the maintaining of the Internet - who are, in fact, the main actors maintaining the Internet. It should not be left to the very indirect, haphazard application of the doctrine of horizontal effect to secure the rights to communication, expression and association of everyone, including political activists, on the Internet *vis-à-vis* ISPs, search engines, blog hosts, etc..

The need to regulate the actions of coporations that affect human rights is increasingly strongly recognised, in particular in the Ruggie Principles developed by the UN, and in civil society initiatives such as the GNI Principles on Freedom of Expression and Privacy. These (or similar) principles should be given greater legal backing as a vital precondition for the protection of human rights in the new context - either through ECHR case-law or through new European instruments.

The principle of legality[104]

The Rule of Law (also referred to as the principle of legality), as applied by the ECtHR, requires that all interferences with the freedoms to communicate, express views and organise on or via the Internet shall be based on clear, specific and accessible rules; that there should be strict limits on interferences with these rights, which should be "necessary" and "proportionate" to recognised "legitimate aims"; and that there be "effective remedies" against undue interferences. All of these criteria are challenged in the new contexts, in particular also given the problems of corporate control and control exercised.

Challenges to European data protection law

There are five main challenges to European data protection law:

- Data protection law to a large extent rests on the concept of "identifiability": if data are related to an identified or identifiable person, they are "personal data" and their use is subject to many important rules and constraints. But if they are not, they tend to be regarded as outside the scope of data protection law. However, in the new digital context I have described in section 2, we may get close to the end of anonymity. The implications have not yet been addressed.

- In view of the complexity of corporate-, intra-corporate-, State- and inter-State arrangements relating to (the processing of data over) the Internet, it is becoming impossible for individuals to know what is being done with their data or to give meaningful consent to the processing of their data, i.e., to have any kind of "informational self-determination".

- "Profiles", aggregate data (including "Big Data") and possibly even genomic/proteomic data that may in themselves not constitute "personal data", will increasingly be used in relation to individuals, to take action with regard to them and adopt decisions or measures on them that may (fundamentally) affect them But trying to tackle this issue only at the stage when the action, decision or measure is taken - or worse, *ex post facto* - will not protect the individual, especially not if it is left to him or her to seek a remedy.

- There are a many different data protection regimes for different contexts, even in Europe, especially within the EU, and the new post-Lisbon structure of the EU will not eradicate this. Moreover, as noted at 2.1, above, the EU has no competence or jurisdiction over matters related to national security. It will be crucial to clarify urgently that when data are transferred from one data protection regime to another (e.g., from the private sector to law enforcement agencies, or from law enforcement agencies to national security agencies, or *vica versa*), the <u>disclosure</u> is subject to the rules applicable to the disclosing party, and the <u>obtaining/collecting</u> is subject to the rules applicable to the receiving party. In particular, it cannot be acceptable that disclosures by private entities or LEAs to NSAs are regarded as not subject to the normal rules on disclosures, or on transborder data transfers, by the disclosing party.

- There is no global data protection regime (even though Council of Europe Convention No. 108 offers such a regime). But the rules on transborder data flows between countries with good data protection and other countries (without data protection, with inadequate protection, or with protection that is somewhat adequate) are incapable of being sensibly applied or enforced in the new environment. "Cloud" processing, in particular, is (almost?) impossible to be subjected to meaningful data protection constraints, in particular in the light of U.S. obstructions to the creation of a strong global (or at least wide/Western) Internet privacy regime.

Challenges to European and wider international police and judicial cooperation

There are four main challenges to current arrangements for European and international police and judicial cooperation (and the relationship between those arrangements and national security activities by national NSAs), arising in the new environment:[105]

- There are increasing problems of substantive (criminal) jurisdiction in relation to the Internet. E.g., in general terms, speech that is protected under the constitutions of some States can be regarded as criminal (pornographic, blasphemous, racist, etc.) in other States - but the expressions are readily available in all. As noted above, in the *Perrin* case, the European Court of Human Rights failed to give guidance on how such conflicts can or should be resolved.

- There are also increasing problems in terms of enforcement jurisdiction. In spite of the *dictum* of the PCIJ in the *Lotus* case, quoted earlier, some States (notably the USA) are demanding that companies whose headquarters or mother companies are registered in their territory hand over data to them from servers in other countries, including in Europe, without informing (let alone involving) the LEAs of the latter countries: MLATs are increasingly by-passed.

- The notions of "law enforcement", "protection against serious threats/disasters" (which can be brought under the more general rubric of "internal security") and "national security" are ill-defined, and the demarcations, such as there were, are increasingly blurred in the fight against international terrorism (which is in any case linked to organised crime). Moreover, as noted under the previous heading, the rules on the transfer of data obtained for internal security, by LEAs, to NSAs, for national security purposes, or *vica versa*, are unclear, both at the national State level, and at European and global level. This poses a serious threat to the maintenance of the Rule of Law in these regards.

- The CyberCrime Convention leaves States considerable discretion in relation both to the substance of the crimes to be created and to important elements of these crimes (intent, damage, seriousness, etc.). Similarly, crucial concepts relating to communications data - which in the new environment are absolutely central to law enforcement and national security - are ill-defined. Thus, it is not clear whether the term "traffic data" includes "location data" (or not), or whether, in an Internet context, "destination data" refers to data in a URL up to the first back-slash, or also to file names (i.e., to search data). The Convention also does not address the (compulsory or "voluntary"/"self-regulatory") involvement of ISPs and other Internet providers in law enforcement, or even more contentious, State security and other surveillance. And the human rights safeguards in the Convention are also ill-defined, and indeed may not apply at all in some contexts,[106]

4. Tentative suggested priorities

The discussions earlier in this paper, and the challenges (tentatively) listed in section 3, should be taken into account by the Council of Europe, and specifically its Data Protection and Cybercrime Unit, in the setting of their priorities. It is not up to me to dictate them, but on the basis of this paper, I would suggest that the following could be high on the list of such priorities:

I. Human Rights/ECHR generally:

As noted, there is a serious lack of guidance on how to apply human rights law, including the ECHR, to transnational contexts/the Internet. The Court may develop such guidance in cases in the near future. However, if this does not happen, the DP & CC Unit could consider issuing guidance itself, on matters within its remit, or work with the Commissioner for Human Rights in seeking an advisory opinion from the Court.

II. Data protection generally:

The biggest challenges to data protection in the next 5 – 10 years will undoubtedly come from what I have already referred to as a "tsunami", not just of data, but of identifiable data; and the increasing uses of "profiles" and "behavioural predictions", based on data generated by us, on data otherwise related to us and on things related to us (The Internet of Things, brought about also by the spread of nanotechnologies and genomics/proteomics), and on broader "Big Data".

- *In this regard, I would suggest that a priority should be to think about how to fend off this tsunami, and specifically: how to affirm and protect **the right to anonymity** on the Internet and in the wider, global digital environment; and, linked to this, how to regulate and strictly limit the creation and use of **profiles**, in all kinds of different contexts. There must especially be strict rules to counter the serious threat of profiles and predictions leading to social exclusion and **discrimination**.*

This is related to the use of surveillance technologies, in all kinds of devices and networks, including the generating and retention of communcation- and location data and Deep Packet Inspection:

- *It should be a COE priority to draft guidelines on the restrictions that should be imposed on **surveillance technologies**; on the international trade in such technologies; and on the responsibilities of corporations in this regard. This should include a declaration that compulsory suspicionless mass surveillance/data retention/DPI violates the ECHR.*

The above should be placed in a global context:

- *The COE should continue to strongly promote **Convention No. 108 as the "gold global standard"**, and should in particular (in cooperation with the EU and others) try to convince the USA to become a full (!) Party to the Convention.*

III. Data protection and cybercrime:

The complete lack of competence and jurisdiction of the EU in matters relating to (ill-defined) "national security", means that in that regard the requirements of the most fundamental European human rights instruments, including even the ECHR and Convention No. 108, are not ensured by the Union. Only the COE can provide appropriate standards in relation to this area, and in relation to the interstitions between areas of various competences and national security. This is crucial, especially in the light of the serious blurring of lines between law enforcement and national security. Consequently:

- *The CDP & CC Unit should issue a strong clarification to the effect that **when data are transferred from one data protection regime to another** (e.g., from the private sector to law enforcement agencies, or from law enforcement agencies to national security agencies, or vica versa), the **disclosure** is subject to the rules applicable to the disclosing party, and the **obtaining/collecting** is subject to the rules applicable to the receiving party. In particular, such a clarification should stress that it is not acceptable that disclosures by private entities or LEAs to NSAs are regarded as not subject to the normal rules on disclosures, or on transborder data transfers, by the disclosing party.*

- *In addition, the COE and the Unit should urgently consider issuing guidance on cooperation between LEAs and NSAs, and amongst NSAs, in terms of data exhanges/data sharing. In Europe, only the COE can do this, and as recent abuses have shown, such guidance is urgently required.*

Another matter of concern is the extraterritorial application of national enforcement jurisdiction by U.S. national security (and law enforcement?) agencies in particular, in contravention of basic international law (*Lotus*):

- *The COE should strongly condemn this violation of the sovereignty of the (European) States affected, and reaffirm in strong terms that **transnational law enforcement- and national security activities should at all times be undertaken within the constraints of international treaties**, i.e., MLATs when dealing with police and judicial cooperation, and national security treaties when dealing with data sharing between NSAs; and that in any case, at all times, all such data exchanges must be in accordance with the ECHR and with Convention No. 108.*

As concerns the more general by-passing of MLATs in the relations between LEAs, the COE should review the problems with the operation of these treaties:

- *The aim should be **to revise MLATs** to make them more efficient, but always in accordance with the ECHR and Convention No. 108. By-passing of the Rule of Law should be anethema to law enforcement.*

- o – O – o -

Douwe Korff
Cambridge/London March 2013

NOTES:

[1] This section draws on Ian Brown, *Working Paper No. 1: The Challenges to European data protection laws and principles*, produced for the Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, carried out by Douwe Korff and Ian Brown for the European Commission in 2010, available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_1_en.pdf

[2] See, e.g.:
http://bits.blogs.nytimes.com/2012/10/28/i-b-m-reports-nanotube-chip-breakthrough/
http://www.cam.ac.uk/research/news/3d-microchip-created
http://www.wired.co.uk/news/archive/2011-02/03/atom-thick-nanosheets
http://actu.epfl.ch/news/first-molybdenite-microchip/

[3] See the UK Government report on Technology and Innovation Futures: UK Growth Opportunities for the 2020s – 2012 Refresh (meaning the updated version of the 2010 report, issued in 2012), section 2.3(8), on pp. 37-39:
http://www.bis.gov.uk/assets/foresight/docs/horizon-scanning-centre/12-1157-technology-innovation-futures-uk-growth-opportunities-2012-refresh.pdf

[4] *Idem*, section 2.3(2), on pp. 32-33.

[5] Source: the Pew Internet & American Life Project, chart on trend data for adults, at:
http://pewinternet.org/Static-Pages/Trend-Data-%28Adults%29/Internet-Adoption.aspx
This website is also a great source of more general data and statistics on the Internet and the use of Internet-related services, etc..

[6] Internet Usage in Europe, June 2012, at:
http://www.internetworldstats.com/stats4.htm
In several European countries more than 90% of the population uses the Internet; the statistic for Monaco is even 100.6% ☺ . In Asia, there are wide differences, with some countries or areas (such as Japan, Hong Kong, Singapore, South Korea and Taiwan) reaching 70-80%, mainland China is at 40%, and Turkmensitan at 5%, see:
http://www.internetworldstats.com/stats3.htm

[7] See:
http://phys.org/news/2013-03-teens-mobile-internet-survey.html

[8] *The global rise in 'always-on' mobile and tablet shoppers driving e-commerce, says WorldPay*, InternetRetailing, 14 May 2012, at: http://internetretailing.net/2012/05/the-global-rise-in-always-on-mobile-and-tablet-shoppers-driving-e-commerce-says-worldpay/

[9] See the webpage on net neutrality on the "*savethenet*" coalition's website, hosted by Free Press:
http://www.savetheinternet.com/net-neutrality

[10] See Technology and Innovation Futures (note 3, above), section 2.2(1), on p. 24ff, and section 2.3(5), on pp. 35-36.

[11] *How RFID works*, at http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid.htm/printable, with reference to RFID Journal.

[12] The main producer of such chips is a U.S. company that used to be called VeriChip, but has now been renamed PositiveID. It has been heavily criticised, see: http://www.antichips.com/. Possibly as a result, no information on VeriChip/PositiveID can be obtained from its website unless you register, see: https://www.myphrinfo.com/PositiveID/Default.aspx.

[13] See:
http://www.wired.co.uk/news/archive/2011-02/03/atom-thick-nanosheets
See also Technology and Innovation Futures (note 3, above), section 2.2(7), on "*smart interactive textiles*", on p. 16. Note in particular the reference to location monitoring.

[14] See: Technology and Innovation Futures (note 3, above), section 2.1(7), on p. 16.

[15] See:

http://www.independent.co.uk/news/science/biological-computer-that-lives-inside-the-body-comes-one-step-closer-as-scientists-make-transistor-out-of-dna-and-rna-8553915.html

[16] See the introduction and report on a recent BCS/OII event on the Internet of Things, at: http://www.bcs.org/content/ConWebDoc/49225
See also the video presentations and the paper at: http://www.bcs.org/content/ConWebDoc/49148

[17] See: Technology and Innovation Futures (note 3, above), section 2.1(1), pp. 18-19.

[18] See the section on Big Data in a booklet on data protection by EDRi, written by Privacy International, UK, available at: http://www.edri.org/files/paper06_datap.pdf

[19] See: http://smartdatacollective.com/mfauscette/50705/big-data-smart-data-supporting-critical-business-decisions

[20] This sub-section draws on a section on Profiling in the booklet on data protection by EDRi (note 18, above), written by Douwe Korff of the Foundation for Information Policy Research, UK.

[21] For a more detailed analysis, see http://protectmydata.eu/topics/limitations/ and Douwe Korff, Comments on Selected Topics in the Draft EU Data Protection Regulation (September 18, 2012), see http://ssrn.com/abstract=2150145.

[22] The quote is from Art Coviello, executive chairman of RSA, the security division of EMC, see: http://www.computerweekly.com/news/2240178641/Embrace-big-data-to-enable-better-security-says-RSA (emphasis added)

[23] Technology and Innovation Futures (note 3, above), section 2.1(11), p. 19.

[24] The first part of this sub-section draws on "*The recording of personal characteristics*", in: Douwe Korff, Automated Processes of Identification, Behavioral Analysis and Risk Detection (Including Technologies for the Use of Images and Airport Security Control) (2010). Presented at Spanish Data Protection Agency Seminar, Madrid, Spain, 9-11 June 2010. Available at SSRN: http://ssrn.com/abstract=1977874

[25] *Biometric Myths: Six Of The Best*, by Russ Davis, CEO of ISL Biometrics, 13 July 2004, at: http://www.net-security.org/article.php?id=711.

[26] On fingerprints, see: http://health.howstuffworks.com/search.php?terms=fingerprints.

[27] The following is from 2007 and probably already outdated:
"*FBI Prepares Vast Database Of Biometrics - $1 Billion Project to Include Images of Irises and Faces*", Washington Post, 22 December 2007, available from: http://www.washingtonpost.com/wp-dyn/content/article/2007/12/21/AR2007122102544.html
See also Technology and Innovation Futures (note 3, above), section 2.3(11), on pp. 41-42.

[28] This part of the subsection draws on Frank Stajano, Lucia Bianchi, Pietro Lio & Douwe Korff, Forensic Genomics: Kin Privacy, Driftnets and Other Open Questions at: http://www.cl.cam.ac.uk/~fms27/papers/2008-StajanoBiaLioKor-genomics.pdf

[29] See: http://www.guardian.co.uk/science/blog/2013/mar/27/prostate-cancer-breakthrough-douglas-easton

[30] See Technology and Innovation Futures (note 3, above), section 2.1.

[31] *Idem*, p. 10.

[32] This sub-section is largely taken from a section on Cloud Computing in the booklet on data protection by EDRi (note 18, above), written by Privacy International, UK. See also Technology and Innovation Futures (note 3, above), section 2.3(3), on pp. 33-34.

[33] Cloud Computing, How the Internet Works http://www.edri.org/files/2012EDRiPapers/how_the_internet_works.pdf
For a more technical definition, see NIST: The NIST Definition of Cloud Computing, 2011, p. 2 http://carc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[34] Fighting cyber crime and protection privacy in the cloud, study for the European Parliament Directorate-General for Internal Policies, February 2013, PE 462.509, p. 13, available at:

http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050

[35] *Our Internet Surveillance State*, Bruce Schneier's blog on security and security technoogy, 25 March 2013, at:
http://www.schneier.com/blog/archives/2013/03/our_internet_su.html
Julian Asange and his colleagues effectively make the same point in their book Freedom and the Future of the Internet, OR Books, 2012. The reference to the Director of the CIA is about the exposure of an affair he had by FBI agents, in spite of the director and his lover taking quite elaborate precautions to hide their activities.

[36] See the section on Privacy & Data Protection on Social Networks in the booklet on data protection by EDRi (note 18, above), written by Access Now.

[37] See Douwe Korff and Ian Brown, *Social Media and Human Rights*, chapter in: Human Rights and a Changing Media Landscape, Strasbourg, Council of Europe Publications, 2012, pp.175-206. Available at SSRN: http://ssrn.com/abstract=1860060

[38] The best recent regional example was the Europe-wide non-governmental opposition against the Anti Counterfeit Trading Agreement, ACTA, which was in the end defeated by this new form of grassroot activism. Cf.: http://action.ffii.org/acta/

[39] Most ordinary people involved in the "Arab Spring" who used their mobiles and Internet access for activist purposes were unaware of their exposure. They were lucky the uprisings succeeded; if they had not, many would be in jail, at risk of torture or even death. In future (indeed, even current) upheavals, people are likely to be more cautious. See the discussion of protective technologies for political activists and human rights defenders (HRDs) in section xxx, below.

[40] See Ian Brown, How will surveillance and privacy technologies impact on the psychological notions of identity?, paper for the UK Government *Foresight* project, February 2013, available at:
[ADD]

[41] See the lecture on "*The Naked European Citizen*" by Douwe Korff at the University of Maastricht, the Netherlands, in 2007, at:
http://vimeo.com/3956469

[42] See:
https://www.torproject.org/
http://en.wikipedia.org/wiki/Tor_%28anonymity_network%29

[43] See:
http://www.fsf.org/news/2010-free-software-awards-announced

[44] FreedomBox is described as "*a personal server running a free software operating system, with free [open-source] applications designed to create and preserve personal privacy*". See:
http://freedomboxfoundation.org/
http://en.wikipedia.org/wiki/FreedomBox

[45] See:
http://www.londonmet.ac.uk/research-units/hrsj/training-and-consultancy/$human-rights-defenders.cfm (FCO HRD Training in Tashkent, Uzbekistan, 2007);
http://www.londonmet.ac.uk/research-units/hrsj/training-and-consultancy/$human-rights-defenders-training-in-kyrgyzstan.cfm (FCO HRD Training in Kyrghystan, 2008).

[46] See:
http://www.wfaa.com/news/world/Mexicos-cartels-build-own-national-radio-system-136234073.html and
http://www.geek.com/articles/news/outclassed-by-technology-in-the-drug-war-20020711/

[47] I am using the term in the loosest possible way as referring to any entity involved in commercial or quasi-commercial activities, aimed at consumers.

[48] [ADD ref to SABAM rulings].

[49] See note 38, above.

[50] See:
http://googlepublicpolicy.blogspot.co.uk/2010/08/joint-policy-proposal-for-open-internet.html

[51] See:
http://technorati.com/business/article/net-neutrality-under-attack-google-verizon/

[52] See:
http://ec.europa.eu/bepa/european-group-ethics/docs/activities/peter_hustinx_presentation_%281%29_15_rt_2011.pdf

[53] See:
http://www.edri.org/edrigram/number10.20/edri-answers-net-neutrality-consultation

[54] See:L *Private traits and attributes are predictable from digital records of human behaviour*, at:
http://www.pnas.org/content/early/2013/03/06/1218772110

[55] See in particular the EU Commission staff working document "Bringing e-commerce benefits to consumers", produced in the context of the preparation of the Commission Communication on "A coherent framework to boost confidence in the digital single market of e-commerce and other online services", available at:
http://ec.europa.eu/internal_market/e-commerce/docs/communication2012/SEC2011_1640_en.pdf (working document);
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0942:FIN:EN:PDF (Commission Communication)
The working document showed that the main concerns stopping consumers from using online transborder services was fear over their payment card data and over their private data. On the question of security breaches, and the need for disclosure of such breaches to maintain consumer trust, see the section on Data Security & Data Breaches in the booklet on data protection by EDRi (note 18, above), written by Privacy International, UK.

[56] On PbD, see the section on Data Protection by Design & by Default in the booklet on data protection by EDRi (note 18, above), written by Access Now, international. There is already a European Privacy Seal in existence (see *https://www.european-privacy-seal.eu/about-europrise/fact-sheet*), but new certification mechanisms are likely to emerge under the new EU data protection regime currently under consideration.

[57] See Fighting cyber crime and protection privacy in the cloud, note 34, above.

[58] The first five paragraphs of this sub-section essentially repeat paras. 8 and 9 of the Final Report on an EU Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, which in turn summarise relevant parts of the *Working Paper* for that study, referred to in note 1, above. The reader is referred to that *Working Paper* for further details and references.

[59] In the UK, the Conservative Party and the Liberal Demorat Party when in opposition criticised the Labour Government for creating a "Database State" (cf. the FIPR report referred to in note 55, below), but now in government, the Conservative-Liberal coalition is essentially maintaining the policy. See:
http://www.techweekeurope.co.uk/news/how-the-government-is-lying-about-fighting-the-database-state-112021

[60] On the major challenges this poses to both States and companies, see Ian Brown and Douwe Korff, Digital Freedoms in International Law, Global Network Initiative, 2012, available at:
http://ssrn.com/abstract=2085342

[61] For details, see two FIPR studies, one for the UK Information Commissioner on Children's databases (2006), and a wider one on all the main national governmental databases for the Rowntree Reform Trust, The Database State (2010); available at:
http://www.ico.org.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_issues_paper_protecting_chidrens_personal_information.pdf
http://www.cl.cam.ac.uk/~rja14/Papers/database-state.pdf.

[62] Cf. the follwing recent UK reports:
http://www.guardian.co.uk/uk/2013/feb/03/police-spies-identities-dead-children
http://www.guardian.co.uk/uk/2013/mar/01/police-spy-fictional-character
http://www.guardian.co.uk/uk/2013/mar/01/spy-mark-kennedy-number-relations

[63] See "Dutch gover http://www.guardian.co.uk/uk/2013/mar/01/spy-mark-kennedy-number-relationsnment proposes cyberattacks against... everyone", at: https://www.eff.org/deeplinks/2012/10/dutch-government-proposes-cyberattacks-against-everyone. Similar issues have arisen in Germany ("online search") and the UK.

[64] Grand Chamber judgment on the EU – USA PNR Agreement of 30 May 2006 in Joined Cases C-317/04 and C-318/04, para. 58:

"[Although] the PNR data have been collected by private [EU-based] operators for commercial purposes and it is they who arrange for their transfer to a third country [i.e., the USA], [this does not mean that] the transfer in question is not covered by [Article 3(2), first indent of the DP Directive, which excludes public security from its scope]. The transfer falls within a framework established by the public authorities that relates to public security."

[65] See Douwe Korff, Note on the applicability of the EC Data Protection Directive to disclosures of personal data from entities covered by the Directive to entities not subject to the Directive, November 2012, at:
[ADD]

[66] Available at:
http://www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf

[67] See:
http://www.huntonprivacyblog.com/2013/03/articles/german-law-enforcement-access-to-cloud-data-in-foreign-jurisdictions-including-the-u-s/

[68] See Fighting cyber crime and protection privacy in the cloud (note 34, above), pp. 33-35, for details.

[69] Note 62, above.

[70] See Douwe Korff, The Hole in the Wall: EU (in)competences in relation to security matters & the protection of privacy and personal data, presentation at the EU SURVEILLE project meeting, EUI, Florence, April 2013; slides and charts available at:
[ADD]

[71] From a section on Anonymisation in the booklet on data protection by EDRi (note 18, above), which in turn draws heavily on advice to a major EU study, provided to the authors of the study (Prof. Douwe Korff and Dr. Ian Brown) by Prof. Ross Anderson, quoted on p. 50 of Working Paper No. 2, produced for that study, and on the FIPR submission to the UK Information Commissioner's Office (the UK Data Protection Authority) on the latter's draft Anonymisation Code of Practice, also drafted by Prof. Anderson.
http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_working_paper_2_en.pdf
http://www.fipr.org/120823icoanoncop.pdf

[72] There are techniques to limit queries to a specific single database to ensure that re-identification of individuals from that single database is (almost) impossible. This includes in particular "differential privacy", designed by Cynthia Dwork and others. However, this does not work if one can make cross-reference searches in several large datasets. See:
http://research.microsoft.com/en-us/projects/databaseprivacy/ (with references).

[73] Technology and Innovations Futures, note 3, above, section 2.3(12), p. 42.

[74] From Douwe Korff, Comments on selected topics in the Draft EU Data Protection Regulation, prepared for EDRi, November 2012, available at:
[ADD]
See also the section on this topic in: Douwe Korff, Automated Processes of Identification, Behavioral Analysis and Risk Detection (note 24, above).

[75] For a detailed discussion of the analysis of personal characteristics and risk identification, and profiling, see: D. Korff, Technologies for the Use of Images: Automated Processes of Identification, Behavioural Analysis and Risk Detection Control at the Airports (note 24, above). The paragraphs on the baserate fallacy in the text draw on this. See in particular also the "security blog" on the issue, by Bruce Schneier, referred to in this paper (and in many other papers): *Why Data Mining Won't Stop Terror*, 3 September 2006 on http://www.schneier.com/blog/.

[76] Review of Gandy's main book on the topic, Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage, 2009, in *Surveillance & Society* 8(3): 379-381, at: http://www.surveillance-and-

society.org/ojs/index.php/journal/article/viewDownloadInterstitial/gandy_chance/gandy_chance. For the book itself, see: http://www.ashgate.com/isbn/9780754679615

[77] UN International Covenant on Civil and Political Rights, Human Rights Committee, General Comment No. 18: Non-discrimination, 10 November 1989, para. 7, emphases added, available at: http://www.unhchr.ch/tbs/doc.nsf/%28Symbol%29/3888b0541f8501c9c12563ed004b8d0e?Opendocument. The HRCtee's definition draws directly on the definitions of discrimination against women, and discrimination on the basis of race, in the major UN Conventions against discrimination against women (CEDAW) and against people on the basis of race (CERD) (and, we might add, in the UN Declaration against discrimination on the basis of religion).

[78] Oscar Gandy, Engaging rational discrimination: exploring reasons for placing regulatory constraints on decision support systems, J Ethics Inf Technol, Vol 12, no. 1, pp. 29-42, 2010, at: http://academic.research.microsoft.com/Publication/41860489/engaging-rational-discrimination-exploring-reasons-for-placing-regulatory-constraints-on-decision.

[79] See the discussion of the (then) most sophisticated systems used by the U.S. national security authorities in Korff & Brown, Privacy & Law Enforcement, FIPR study for the UK Information Commissioner, 2004, and in particular the technologies developed in the so-called "Total Information Awareness" program, discussed in *Paper No. 3: TIA & PNR*, by Douwe Korff, available from: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/tia_and_pnr.pdf.

[80] See F Kraemer et al., Is there an ethics of algoritims?, Ethics Inf Technol (2011) 13:251–260, at: http://purl.tue.nl/605170089298249.

[81] From a section on *The limitations and relativity of identification* in: Douwe Korff, Automated Processes of Identification, Behavioral Analysis and Risk Detection (note 24, above).

[82] Nicholas Bohm and Stephen Mason, Identity and its verification, in: *Computer Law & Security Review*, Vol. 26, Number 1, January 2010, pp. 43 – 51.

[83] "Although identical twins share the same genes they do not have identical fingerprints. That's because the shape of the whorls and arches on our fingers are determined both by genes and the local environment around the dividing skin cells. So a twin's individual position in the womb will cause slight differences." Editor's answer to a reader' question, New Scientist, 1 October 2005, at: http://www.newscientist.com/article/mg18825191.100-twin-fingerprints.html.

[84] This is what leads to what Angell and Khanna call "The Fallacy of the "Residual Category": see note 11, below.

[85] David Feige, *Printing Problems: The inexact science of fingerprint analysis*, 27 May 2004, quoting Simon Cole, the author of Suspect Identities: A History of Fingerprinting and Criminal Identification, at: http://davidfeige.com/fingerprintpage.htm.

[86] On McKie, see: *The Fallacy of the "Residual Category"* by Ian Angell and Ash Khanna, 19 April 2008, available from:
http://ianangell.blogspot.com/2008/04/fallacy-of-residual-category.html.
The facts of the McKie case are also summarised on the official inquiry website:
http://www.thefingerprintinquiryscotland.org.uk/inquiry/21.html.
The Government made the out of court settlement without admission of liability: that is almost standard procedure and can itself breach human rights, but I will not go into that now.

On the Mayfield case, see David Feige, *Printing Problems: The inexact science of fingerprint analysis* (note 85, above).

[87] The idea may be fanciful, but that of course does not mean that it is not peddled by the snake-oil salesmen of the companies that seek to develop the systems, or taken up by governments. See Douwe Korff, *TIA & PNR*, Paper No. 3 in: Ian Brown and Douwe Korff, Privacy & Law Enforcement, study by FIPR (the Foundation for Information Policy Research) for the UK Information Commissioner, 2005. The letters TIA stand for "Total Information Awareness", a massive anti-terrorist programme developed by the US Government and now supposedly stopped (but parts of which continue under different names, in different other programmes). This paper gives an overview, *inter alia*, of the DARPA programme to develop "biometrics-based human identification to recognize individuals and activities" and to capture the relevant

data, in whatever format it is found: video, audio, photographic or whatever, with new technologies being used to link such data seamlessly with more traditional (text) formats of information. Available from: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/tia_and_pnr.pdf. Cf. also the programmes developed by IARPA, discussed in relation to "data mining" and "profiling" under the latter heading, later in this section (with references).

[88] Originally, five locus matches were used in the matching of DNA fingerprints. More recent systems used "variable number of tandem repeats" (VNTRs), and the most modern systems use "short tandem repeats" (STR). For details, see Lucia Bianchi and Pietro Liò, o.c. (note 4, above), p. 2.

[89] Lucia Bianchi and Pietro Liò, o.c. (note 4, above), p. 3.

[90] *The Fallacy of the "Residual Category"*, o.c. (note 11, above).

[91] From a section on *The analysis of personal characteristics and risk identification* in: Douwe Korff, Automated Processes of Identification, Behavioral Analysis and Risk Detection (note 24, above).

[92] For details of these detector systems, see the paper mentioned in the previous note, and the references given there.

[93] See Anders Eriksson and Francisco Lacerda, Charlatanry in forensic speech science: A problem to be taken seriously (2007). Note that this article was removed from the online version of the journal in which it was originally published under pressure from the detector vendors, but it can still be found elsewhere quite easily, e.g., at:
http://www.cs.columbia.edu/~julia/papers/eriksson&lacerda07.pdf.

See endnote xx to *The analysis of personal characteristics and risk identification* in: Douwe Korff, Automated Processes of Identification, Behavioral Analysis and Risk Detection (note 24, above) for further details of the suppression of the research.

[94] This latter technology was not mentioned in the TIA documentation: it was (is?) apparently being developed in connection with airline passenger screening: see http://www.epic.org/privacy/airtravel/nasa.

[95] "*National security intelligence organizations should monitor advances in cognitive neuroscience research*", press release of the US National Academies, 13 August 2008, available from:
http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=12177.

[96] "*Security firms working on devices to spot would-be terrorists in crowd*", Guardian, 9 August 2007, at: http://www.guardian.co.uk/science/2007/aug/09/terrorism.

[97] Testimony of the American Psychological Association to the US House Appropriations Subcommittee on Homeland Security Regarding Funding for Fiscal Year 2007, March 16, 2006, available from: http://www.apa.org/about/gr/science/advocacy/2006/dhs.pdf. The other "product" to be produced in this area is "an integrative model of the ideological, organizational, and contextual factors associated with a group or radical movement's likelihood of engaging in violence."

[98] *Human Rights Risks of Selected Detection Technologies - Sample Uses by Governments of Selected Detection Technologies*, in: Collaborative Project DETECTER (Detection Technologies, Terrorism, Ethics and Human Rights), Work Package 09,FP7-SECT-2007-217862, 11 December 2009, p. 15.

[99] This subsection again draws on Frank Stajano, Lucia Bianchi, Pietro Lio & Douwe Korff, Forensic Genomics: Kin Privacy, Driftnets and Other Open Questions (note xx, above).

[100] See note 31, above.

[101] This section draws on the discussion in sections 3.1 and 3.4 of the paper on *Social Media and Human Rights*, written by Douwe Korff and Ian Brown for the COE Commissioner for Human Rights in 2011, which was the basis for a (rather shorter) chapter with that title (Chapter 6) in the latter's publication Human Rights in a Changing Media Landscape, 2011, and on Digital Freedoms in International Law, a report by the same authors for the Global Network Initiative, available at:
[ADD]

[102] See the detailed discussion of this impossibility in section 3.4, sub-section (a), of the full paper mentioned in the previous note, with reference to the *Handyside* and *Perrin* judgments in particular.

[103] See section 3.4, sub-section (b), of the full paper mentioned in note 101.

[104] For further detail, in particular on the application of this principle to the blocking/filtering of data and wesbites on the Internet, with reference to detailed UN standards, see section 3.4, sub-section (c), of the full paper mentioned in note 101, and Digital Freedoms in International Law, also mentioned in that note.

[105] This section draws on

[106] See Douwe Korff, Note on some main issues [relating to the CyberCrime Convention and Human Rights], Council of Europe CyberCrime@IPA Conference, Baku, Azerbadjan, November 2012.

- o – O – o -