Statewatch analysis

The “digital tsunami” and the EU surveillance state

Tony Bunyan

“Every object the individual uses, every transaction they make and almost everywhere they go will create a detailed digital record. This will generate a wealth of information for public security organisations, and create huge opportunities for more effective and productive public security efforts." (EU Council Presidency paper)

This analysis looks at the Future Group proposals to harness the “digital tsunami” by European (and national) agencies predicating state surveillance over a very wide range of human activity.

Two of the Future group’s documents are considered here: 1) sections from the final report: *“Freedom, Security and Privacy" - the area of European Home Affairs”* (referred to as the “final report”) and 2) a "Concept" paper from the Portuguese Council Presidency entitled: *"Public security, privacy and technology in Europe: Moving Forward: Concept paper on the European Strategy to transform Public security organisations in a Connected World"* (referred to as the “paper”). As we shall see the obscure language used in the former is firmly embedded in the latter.

Using new technologies and information networks

The final report argues that in the “digital tsunami environment” citizens' expectations of "proactive protection" become "ever more acute", especially as traditional measures to protect privacy "will become less and less effective", thus:

> *“"privacy-enhancing technologies" are absolutely essential to guarantee civil and political rights in the age of cyberspace.”*

The document is silent on how this should be done.

The main emphasis is almost exclusively on the opportunities the "digital tsunami" gives “public security organisations” to:

> *“have access to almost limitless amounts of potentially useful information”*

For "public security organisations" to "master this data tsunami" will require "automated data analysis" to get this through to a "multitude of stakeholders" in the agencies across the EU. "Interoperability" is assumed (being able to access databases across the EU) but what is needed is a:

> *“platform approach to delivering public security”*

A “service oriented” approach means that:

> *“outputs from different parts of the system can be shared (within and across organisations) and to build* ***converged*** *platforms... move to converged networks (or where necessary solutions that ensure all their networks can "talk" to each other) and.. ensure all data streams are digital and capable of being meshed together” (emphasis added)*

For example, the "principle of availability" means that on a "case-by-case" basis, through "interoperable" systems, data and intelligence can be gathered by an agency in one state from a number of other EU states. However, the report argues that:

> *“this is an opportune moment to go beyond the limited perspective of a case-by-case approach and aim for a holistic objective in law enforcement information management.”*

In contrast to an "uncoordinated and incoherent palette of information systems" there would be a:

> *“European Union Law Enforcement Information Management Strategy (EU IMS).. aiming at a professional, business-oriented and cost-effective use of information technology and information networks.”*

The EU "surveillance state”

At its meeting in October 2007 the Future Group was presented with a "Concept" paper from the Portuguese Council Presidency.

It spells out in detail the thinking and intent underneath the obscure language in the full report's section on: "Using new technologies and information networks." The "Concept paper" opens with the statement that:

> *“Technology is not neutral: it must be put at the service of security with respect for the way of life of the citizen in democratic countries and can have a decisive contribution towards making a global world more secure.”*

This statement begs the question of exactly how, if technology is "put at the service of security" it can at the same time "respect" for the way of life of citizens. Surely technology should "serve" the people and "serve" security only in so far as it does not undermine individual and fundamental rights. This paper however assumes the former to reflect the consensus of governments in the EU, “public security” comes first. It can be argued that it is not “public security” that the public want but rather “public safety”. Indeed, if a concept of “public safety”, based on people’s needs, were used instead of “public security”, based on the state’s needs, a whole different set of policies and practices might emerge.

The paper draws attention to the:

> *"development and integration of satellite and airborne monitoring capabilities, the use of GMES technologies, including multilayer mapping with modelling tools and the development of shared, interactive and secure information, communication and analysis tools."*

GMES, Global Monitoring for Environment and Security, is an EU initiative for the implementation of information services dealing with the environment and security. It uses "observation data" from "Earth Observation satellites and ground based information which integrates and makes accessible data from multiple sources. This allows public and private actors to: "anticipate, intervene and control".
The next section in the Portuguese Council Presidency paper is: *"The digital tsunami and its consequences for public security organisations"*. As more and more "people, machines and environments are connected" this vastly increases the amount of:

> *"potential information for use in the day-to-day operations of public security organisations.*
>
> *One obvious illustration is the ability to track the location of any active mobile phone (and to know where it was last switched off and last switched on). This is just the beginning. In the next few years billions of items in the physical world will be connected, using technologies such as radio-frequency identification (RFID), broadband wireless (WiFi, WiMAX), satellite and wireless (Bluetooth, wireless USB, ZigBee). This means it will be possible to trace more and more objects in real-time and to analyse their movement and activity retrospectively.... In the near future most objects will generate streams of digital data about their location and use - revealing patterns and social behaviours which public security professionals can use to prevent or investigate incidents."*

The "objects" referred to also include people who could be tracked through their car, mobile phone or the clothes they are wearing.[1]

The paper goes on to look at digital transactions, use of biometrics and online behaviour:

> *"All credit or debit-related purchases already generate monitorable and searchable real-time information; but more and more transactions will be of this kind as we move towards a cashless society...*
>
> *These trends will be reinforced as biometric measurements are used to enhance security at more and more locations - whether public places such as town halls or train stations; private locations such as amusement venues; or places of work."*

This assumes the widespread use of peoples' biometrics (fingerprints, facial scans or iris scans) in everyday life once they have been collected by national EU states for passports and ID cards:

> *"Most large cities have already seen a significant increase in the use of closed circuit television (CCTV), and usage (by public and private sector organisations) is likely to increase further and to shift from the current analogue technologies to more easily storable and searchable digital technologies.*
>
> *Further accelerating the tsunami of data is online behaviour. Social networks such as My Space, Face Book and Second Life - and indeed all forms of online activity - generate huge amounts of information that can be of use to public security organisations."*

Next generation "searchable digital" videos of public and private places suggests life-time databanks with the ability to conduct historical searches based on a person's image.[2]

The paper suggests that the capacity now exists, or will very soon, where the state will be able to combine data from different sources on every individual - financial transactions, train journeys, visits to a town hall, a fairground, images from "searchable digital technologies", internet usage and social habits together with state records, citizen registration, National Insurance details, schools, universities, criminal records, tax record, health record, driving licence and motoring offences, insurance details and more which could be used to monitor and control social, economic and political life. If this seems an extreme view just read what the Portuguese Council Presidency goes on to say:

> *"These trends have huge implications for public security. Citizens already leave many digital traces as they move around. What is clear, however, is that the number of those traces (and the detailed information they contain) is likely to increase by several orders of magnitude in the next ten years.*
>
> *Every object the individual uses, every transaction they make and almost everywhere they go will create a detailed digital record. This will generate a wealth of information for public security organisations, and create huge opportunities for more effective and productive public security efforts."*

Is "privacy enhancing technology" a non-starter?

The final report mentioned that "Privacy enhancing technologies" were essential if people were to be convinced of the need for this development. Here in this background paper, however, this is recognised but is also fatally undermined. The paper says that fundamental privacy issues are raised on "how much information about the behaviour of citizens should be shared" There is no reference to terrorism or even crime but simply "information about the *behaviour* of citizens" being hoovered up. It then goes on to say:

> *"Paradoxically, those same tools can also be used by terrorists and other criminals. Thus, if data are automatically anonymised, after a certain lapse of time, that procedure may erase evidence of crimes; encryption tools prevent hacking when information is transmitted over the Internet and protect personal data against unlawful processing but may also help conceal criminal plans; cookie-cutters enhance compliance with the principle that data must be processed fairly and that the data subject must*

> *be informed about the processing going on, but may also make ineffective police efforts to gather information on illegal activities."*

Indeed, when it comes to "balancing" the first need against the second it is "security" that has always won since 11 September 2001. Just look at the draft Framework Decision on data protection on police and judicial cooperation – covering the exchange of data/intelligence between member states and outside the EU about to be adopted by the Council. The Commission proposal was thrown out and rewritten by law enforcement officers and officials. [3]

Three "Challenges"

The Portuguese paper says that there are three "Challenges", the first of which is presented under the heading: "Automate and master data analysis" is that with the "digital tsunami":

> *"data monitoring and analysis will become much more automated"*

Drawing on the practice of financial traders, brokers and credit card companies who use sophisticated programmes to analyses changes and trends the paper says that:

> *"**machines** are able not just to analyse records of transactions, but also to analyse visual information as well. Current systems can already identify individuals by their gait or flag up particular types of image, eg: unattended luggage or a person lying on the ground, apparently injured. Next generation systems are likely to be able to watch for, find and follow even more tightly defined objects, behaviour patterns or events.*
>
> *These developments mean routine data monitoring and analysis will increasingly be handled by machines; the system will then flag up exceptions (unusual behaviour and anomalies) for human investigation. Some law enforcement agencies are already familiar with this approach in their suspicious transaction monitoring activities carried out by specialised agencies tasked with anti-money laundering activity. But this approach will need to be much more widely understood. (emphasis added)"*

When put together "automated monitoring and analysis" with "machines" determining unusual or unacceptable behaviour the next step is easy, you get "machine" driven responses. Thus "networked systems" will not just monitor live situations but the "machine":

> *"will start to respond to it intelligently"*

So now we have "intelligent" machines. Moreover, the systems or "machines" will:

> *"work across multiple data streams and multiple types of data stream. For example, if someone in an airport starts making a series of unusual mobile phone calls, the system might monitor the video streams of the areas where that person is more sensitively than it would normally. Or it might*

> *check passenger travel information to see if that person or someone related to them is due to arrive or depart in the next couple of hours."*

Who or rather what (if it is a machine) will determine if a mobile phone call is "unusual"? What if you are doing your neighbour a favour by picking up their grandparents from the airport - you are not related to them and are a bit anxious that you will not recognise them?

The second "Challenge" is "Making decision-making more distributed" which is making sure that everyone in the chain of public security organisations can get instant and real-time information.

The third "Challenge" is to "Transform Decision support". Employing "Mashups" ("Web applications that combine data from two or more sources into a "single tool") means that:

> *"in the near future public security organisations will be building portals that aggregate a huge range of data sources into personalized cockpits for different decision-makers."*

Which means, in turn, that:

> *"IT systems will increasingly have automated policies that perform actions on decisions and/or destinations.."*

It is not hard to imagine a scenario where a person is picked up by CCTV running in a tube station: is this person running because they have attacked someone, running away from their attacker, or just running for the train?

Echoing the final report the Council Presidency paper says that EU member states "individually and collectively" should take a "platform" approach to "delivering public security". They need, it says to move beyond interoperability to a "services-oriented approach" and "converged platforms" so that all the networks "can "talk" to each other". After all, in an increasingly connected world:

> *"public security organisations will have access to almost limitless amounts of potentially useful information."*

Conclusion

The papers referred to and the final report were drawn up by high-level officials and agreed by EU Ministers. They, frighteningly, really do believe they have, and are, "balancing" the demands of security and civil liberties; they embrace the new technology, if it is technologically possible why should it not be used; they assume that the "digital tsunami" should be harvested by public security organisations, simply because it is there; and assume too that everyone accepts that the "threats" they proclaim require such a gargantuan, and undiscussed, leap. There is no recognition that people not only want to live and travel in safety also want protection from an all-mighty state.

The creation of an surveillance state, for that is what is being proposed, will take the EU further down the road to authoritarianism, a path which looks less and less likely to be reversible.

In the aftermath of 11 September 2001, and for the next three or four years, the rationale for new powers, databases and agencies in and across the EU were presented as if they were "exceptional", initiatives needed to meet the terrorist threat. We know now what was termed "exceptional" is the norm, that unthinkable (and politically unacceptable) uses of technology just seven years ago are almost upon us.

Footnotes

1) During the Portuguese Council Presidency a Conference was held on "RFID - The next step to The Internet of Things" (15-16 November 2007), EU doc no: 14681/07.

2) Under its Communications Data Bill the UK government is proposing to create one, massive, database of all communications including phones, mobiles and internet usage in perpetuity.

3) See: Observatory on Data Protection in the EU:
http://www.statewatch.org/eu-dp.htm

This Analysis was first published in Statewatch Journal, Vol 18 no 2, April-June 2008

NB: The subsequent in-depth analysis (60 pages) , *The Shape of Things to Come* by Tony Bunyan was published in September 2008, see:

http://www.statewatch.org/future-group.htm