Statewatch

Detection technologies and democracy

“The quality of democratic life is too important to be decided by multinationals and the law enforcement and security agencies”

This analysis looks at the European Commission’s Green Paper on "detection technologies in the work of law enforcement, customs and other security authorities"

The European Commission has published a Green Paper on "detection technologies in the work of law enforcement, customs and other security authorities" (COM 474, 1.9.06), which is open for "consultation" until 10 January 2007.

It opens with the statement that "Security is a cornerstone of Commission policy" and a "crucial dimension" of security policy is "crime and terrorism". Throughout the paper "terrorism", "crime" or "terrorism and other forms of crime" are conflated as if to suggest there is an equal "threat" from “terrorism”, which may kill or maim, and all “crime” however minor. By doing so it uses the “politics” of fear” to justify the introduction of a surveillance society.

The green paper, resulted from a conference (“Public-Private Security Dialogue: Detection Technologies and Associated Technologies in the Fight against Terrorism”) that took place in November 2005, attended by “major European business and industry associations” and the users (”stakeholders”) members of the law enforcement, customs and “other security authorities”. [1]

The Commission paper’s intention is to:

“find out what role the Union could play in order to foster detection technologies in the service of the security of its citizens.”

The whole premise, however, is not about citizens’ needs as these are to be defined by the parameters of the “private” sector (the multinational

[1] Presumably “other security authorities” is a euphemism for internal security agencies – though later there are references to “security authorities” seeking to suggest that policing, immigration and customs are “security” agencies[1].

suppliers) to meet the needs of the "users" (stakeholders), the "public sector" (law enforcement, customs and "other security authorities").

Thus the assumption throughout is:

"to further enhance interaction between public and private sectors in an effort to focus investment on standardisation, research, certification and interoperability of detection systems and to transform research results into useful and applicable tools. A virtuous circle has to be established in which the private sector is guided in its research effort and expenditure by a public sector that knows what it wants and what the private sector can offer. This should help to develop an advanced market in detection products and security solutions, which in turn should lead to greater availability of products and services at lower cost."

There are standard references to the EU Charter of Fundamental Rights and the ECHR even though the former has not been legally adopted. The 1995 Directive intended to protect people's personal data covers the "first pillar", that is, it affects the multinationals (the suppliers of technologies). The real test is the proposed Framework decision on data protection for police and judicial matters – which will affect the "users", the law enforcement agencies. The Commission put forward a draft proposal which the European Parliament is considering – but the parliament is only being "consulted" as this is a "third pillar" measure. In the Council's, secret, deliberations the draft proposal is being torn to shreds in order to give priority to the so-called "principle of availability" over any meaningful data protection for the individual.[2]

The paper addresses the following issues:

a) "Standardisation" of:

"the public sector (needs) and the private sector (solutions)"

however as:

"for security reasons, the development of standards cannot be openly discussed"

So they should, the paper says, only focus on to what extent "common standards may be desirable".

This avoids the obvious question: the technical details of standards might need to be secret but their *purpose and interoperability* should be a matter of public, open debate.

---

[2] The "principle of availability" was in the Hague Programme agreed by EU governments on 5 November 2004 – there was no parliamentary or public debate on its contents prior to adoption. The "principle" means that any data or information held by any agency in one member state must be accessible to all other agencies in the EU.

b) "Security research": the paper refers to the European Security Research Advisory Board (ESRAB) and its report, published in September 2006, which:

"identifies around 120 security capabilities and 100 key technologies"

The Commission paper's only concern is to create a "mechanism" for disseminating security research to:

"only those who are entitled to access the information"

No explanation is given of the ESRAB's background or its part in the emerging EU security-industrial complex, on which see: Arming Big Brother by Ben Hayes (Statewatch and the Transnational Institute, TNI):

http://www.statewatch.org/news/2006/apr/bigbrother.pdf

c) "Needs and solutions": concerns the:

"real needs of the end-users"

with a:

"view to preserving the values and nature of our societies"

As current systems are often unable to communicate with each other:

"The integration of data from different detection technologies into a single data analysis system may make detection systems more effective. Any measure adopted in this respect has to comply with data protection rules"

The "integration" of data from different systems utterly undermines any concept of data protection under which data collected for one purpose may not be use for another purpose.

d) "Use of data – and text – mining tools":

We are told that:

"National and European security authorities are facing a constant increase in the volume of documentation and information they have to process. To address this challenge more efficiently, modern software tools for data and text mining exist. This technology can help to extract relevant information from huge numbers of documents. For example it is possible to intelligently filter text and documents to aid navigation (clustering of documents), for auto-categorisation (channelling and prioritising document flow within investigation teams)"

and that data-mining involving, for example, e-mails, are covered by the ECHR and therefore:

"The use of any techniques for data and text mining must be in accordance with the law, be necessary in a democratic society to protect an important public interest and be proportionate to the public interest pursued."

In the "war on terrorism" (post 11 September) climate it is only to easy to see that the "law" could decide that data-mining is "necessary in a democratic society", that it does "protect an important public interest" and is "proportionate".

Who is setting the agenda

The Annex tells us more about the view expressed at the conference in November 2005 attended by "major European business and industry associations" and the users/"stakeholders" members of the law enforcement, customs and "other security authorities". The conference provided for:

"interaction between solution-providers and those who need solutions in the public sector"

One of the three main topics was:

"personal detection technologies and biometrics"

"Detection technologies":

"can be almost anything used to detect something in a security or safety context, with the focus on law enforcement, customs or security authority"

And a "non-exhaustive list of categories" includes:

- *"Hand-held detectors*
- *Detection portals*
- *Surveillance solutions*
- *Detection of biometrics*
- *Data- and text-mining tools*
- *Other software-based detection tools, etc."*

The conference proposed that a series of studies should be carried out.

These include:

1. The "protection of mass events" with the possibility of "Community-owned" or "Community-shared equipment" which could be transferred from "event" to "event" – from a Summit meeting of Prime Ministers to a football match or a major demonstration.

2. “Cooperation and information-sharing among forensic and security research institutes” – presumably this might cover the question of whether forsensic laboratories in some EU member states are already sending DNA samples to other member states?

3. The law:

“Even if the technology as such is not in breach of legal standards, the manner of its use may raise concerns”

Moreover:

“the changing use of existing technologies may result in situations where a law regulating their use does not exist”

4. Having recognised that:

“Personal detection (including surveillance) and biometrics are issues which affect individuals directly, and therefore a sensitive political debate is ongoing on the use of these tools for the purposes of improving security in Europe”

Extraordinarily a study is proposed on:

“the levels of acceptance of surveillance and biometrics by the population in individual Member States and in the EU”

to help:

“EU and national governments to deploy adequate communication strategies on these issues”

It is not proposed to carry out studies to highlight the dangers to rights and liberties posed by the new technologies but rather to find out the levels of “*acceptance of surveillance and biometrics by the population”* so as to aid *“communications strategies”* to effectively sell their benefits.

The concept of “acceptance” is a passive one implying tacit agreement, disinterest in, or simple ignorance of, the detail of what is being planned. “Consent”, on the other hand, involves an active, informed and open debate of the problems, possible solutions and the consequences – “consent” and “legitimation” are the true “cornerstones” of a democratic society.

Conclusion

“Democracy” is increasingly taken to simply mean a parliamentary election every four or five years.

A meaningful “democratic life” on the other hand is about a democratic culture which defines the everyday interactions between the state (and

multinationals) and people. It sets out the limits on state power whether coercive or "soft" (surveillance and social control), sets out lines of accountability and scrutiny which are transparent and open, and lays down legal sanctions if power is misused or abused.

In this context the core of the debate is whether people should be subject to surveillance and monitoring because everyone is a potential "suspect", a potential criminal, or a potential terrorist or whether people have a right to go about their everyday lives without being routinely subject to surveillance and monitoring for no good reason.

The outcome of this debate – which so far is largely behind closed doors or limited to small numbers of informed and concerned individuals and groups - will determine the quality (or absence) of democracy in the EU.

Tony Bunyan, Statewatch editor, comments:

"This initiative is entirely directed at the "needs" of the agencies not the "needs" of the people. It presumes that multinationals and state agencies can be trusted to know what is best for us.

The quality of democratic life is too important to be decided by multinationals and the law enforcement and security agencies"

Sources

Commission Green paper:
http://www.statewatch.org/news/2006/sep/eu-com-detection-techn-com-474.pdf

Background

Arming Big Brother:
http://www.statewatch.org/news/2006/apr/bigbrother.pdf

EU: Biometrics - from visas to passports to ID cards:
http://www.statewatch.org/news/2005/jul/09eu-passports-id-cards.htm

- The EU does not have the powers to introduce biometrics for national ID cards
- The ICAO standard only requires a "facial image"
- USA not intending to introduce biometrics on its passports - only a digitised normal passport photo

Search on Statewatch database for Features on "biometrics":
http://database.statewatch.org/searchdisplay.asp?grpid=57

Tony Bunyan
September 2006