The shape of things to come:
Electronic surveillance and control

Statewatch—a voluntary organisation that encourages investigative journalism and critical research in the fields of justice, civil liberties, and accountability—has drawn attention to the growing encroachment by EU agencies on civil liberties, especially in the area of electronic and internet surveillance. This article is based on a recent report prepared for Statewatch by Tony Bunyan, "The shape of things to come" (www.statewatch.org/analyses/the-shape-of-things-to-come.pdf).

A paper on new technologies prepared by the Portuguese Presidency of the EU Council states: "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."

The Statewatch report points out that the capacity now exists, or will very soon exist, for European states to combine data from various sources on every individual, including financial transactions, train journeys, visits to a town hall, images from "searchable digital technologies," and internet use, together with various state records, electoral registers, social insurance details, schools and universities, criminal records, tax records, health records, driving licences and records of motoring offences, which could be used to monitor and control social, economic and political life.

A cause of particular concern is a paper entitled "Freedom, Security, Privacy: European Home Affairs in an Open World" (www.statewatch.org/news/2008/jul/eu-futures-jha-report.pdf), prepared in June 2008 by a shadowy group called the Informal High-Level Advisory Group on the Future of European Home Affairs Policy, or the Future Group, as it also likes to call itself.

The European Security Research Agenda is an important part of the background to the report of the Future Group. This involves thousands of local and global surveillance systems, the introduction of biometric identification, electronic tagging and satellite monitoring, "less lethal" weapons, paramilitary equipment for "public order" and crisis management, and the militarisation of border controls. According to Statewatch, "technological advances in law enforcement are often welcomed uncritically but rarely are these technologies neutral, in either application or effect. Military organisations dominate research and development in these areas under the banner of 'dual-use' technology, avoiding both the constraints and controversies of the arms trade. Tomorrow's technologies of control quickly become today's political imperative;

contentious policies appear increasingly irresistible."

Home affairs and security

In 1999 the EU Council adopted the "Tampere programme" (www.statewatch.org/news/2003/sep/tamp.htm), covering the whole area of justice and home affairs for the period 1999–2004. The final text, adopted on 16 October 1999, was not available until the morning of the meeting at Tampere in Finland and was adopted a few hours later. There was no involvement by national parliaments or the European Parliament in drafting the text, nor could any outside organisation discuss it or comment on it. It is still not known who drew up the draft that was presented to the meeting.

A new five-year strategy for justice and home affairs policy and "security" policy is being developed for 2009–14. EU policy-makers and governments are pursuing virtually unfettered powers to gather masses of personal data on the everyday life of everyone, on the grounds that in this way we can all be safe and secure from ill-defined "threats." It is expected that the new five-year plan will be adopted under the Swedish Presidency in the second half of 2009. The Future Group suggests that the European Parliament be "consulted" in this process, but as usual it is the Council of the European Union that will have the final say.

The Future Group's proposals

Statewatch draws attention to the fact that the Future Group's report introduces some new EU terminology, especially a change from "law enforcement agencies"—essentially the police—to "public security organisations," which includes law enforcement agencies but is not limited to them.

As well as a range of measures in the area of techniques of surveillance, the proposals include enhanced "security" co-operation with the United States. The EU-US axis developed significantly after 11 September 2001. "The Group considers close and continuous cooperation with the United States to be indispensable . . . this cooperation should lead to greater convergence, including the different legal frameworks of data protection. By 2014 the European Union should also make up its mind with regard to the political objective of achieving a Euro-Atlantic area of cooperation with the USA in the field of Freedom, Security and Justice."

Also relevant is the extension of the role of NATO beyond the bounds of Europe in 2002. Twenty-one of the twenty-seven EU member-states are in NATO; most of them are involved in the war in Afghanistan.

Communications

In 2006 a directive on the mandatory retention of all communications data throughout the European Union was adopted. Service providers are obliged to keep, and give agencies access to, records of all phone calls, mobile phone calls (and the whereabouts of the callers), faxes, e-mail, and internet use. Most states that had not already done so are

now implementing this directive. In short, records of the use of all forms of telecommunications by everyone within the European Union are held and can be examined by agencies in connection with “serious crime, as defined by each Member State in its national law” (which varies from state to state), or for suspicion of a serious crime.

Travel

From 2004 a regulation on EU passports has required the taking of fingerprints from all people applying for a passport. There has been a time lag in implementing this, but from 2009 millions of people in all EU member-states will have to attend special centres to be interviewed and then compulsorily fingerprinted in order to obtain a new (or replacement) passport. Fingerprinting everyone applying for a visa to visit an EU country from third countries is already done, and the fingerprinting of resident nationals of third countries has been agreed.

Discussions are under way on extending the taking of fingerprints for national identity cards, as these are used for travel within the Schengen area (a group of twenty-five countries that have abolished all border controls with each other).

The information system set up under the Schengen Agreement is to be upgraded to hold more categories of data (including fingerprints and DNA information), and access to all the data is to be extended to all agencies, including police, immigration, and customs. It has been agreed that the Schengen information system is to have a “common technical platform” with the visa information system used for the policing of visitors, thus becoming a specifically surveillance tool.

Discussions towards creating an EU “passenger name record” system are also under way. A number of European governments do not want to limit the use of data to terrorism and organised crime and want to extend its scope from travel into and out of the European Union to travel between EU states and even within each state. The same view also supports extending the scope from air travel to land and sea travel.

EU regulations on driving licences have been harmonised, so that licences will have to be renewed every ten years, with the option of having them renewed every five years. A microchip on the licence will hold data on the owner, which can be updated as well as adapted for other purposes.

An upgraded border control system would require registering in advance, with iris scans and fingerprints to allow speedy clearance, an electronic system for travel authorisation (ESTA), following exactly the American model, and an exit-entry system for third-country nationals. Permission to travel would have to be given before a ticket could be bought. Common visa application centres in third countries should be stepped up, and “uniform European Schengen visas should be issued.”

Though these proposals are presumed to refer to travel into the European Union, it should be borne in mind that the planned system could be used to record the travel of everyone in and out of, or within, EU member-states, by air, land, or sea.

All this is to be accompanied by an “awareness” (i.e. publicity) campaign promoting “the advantages of increased use of information and communication technologies.”

Police

The Prum Treaty, agreed by seventeen member-states, has led to agreement on the automated exchange of DNA, fingerprint and vehicle data being incorporated in EU law, thus applying in all twenty-seven member-states.

The Lisbon Treaty includes extensive increases in police co-operation at the EU level and the creation of a new Committee on Internal Security.

Immigration

The European Union has also agreed in principle on the Returns Directive, under which those found to be illegally resident are to be rounded up and held in detention centres for up to eighteen months before being deported to their assumed country of origin. Some people defined as illegal will have been in an EU country for days or weeks, others may have been there for years, with their children having been born there. The directive makes no distinction: they are all “illegal.”

At the same time “legal migration” is to be encouraged. Because of Europe's ageing population, it needs skilled labour from the Third World to maintain its standard of living—and its continued exploitation of the Third World's own resources.

An attempt will be made to enlist the co-operation of the countries that are seen as the source of Europe’s immigration “problems,” the object being for “illegal immigration to be curbed at its roots.” The idea is to be much more interventionist, not merely at EU borders but within the offending countries themselves. This will include offers of easier visas for the middle classes of the Third World and subsidies to bring in EU-style border controls. The Future Group recommends that sea patrols, for example in the Mediterranean, should be extended to “include the territorial waters” and “search and rescue areas” of third countries and that agreements be negotiated for joint patrols. In parallel with this, “joint return measures should be facilitated.”

E-government

The Future Group is also keen on so-called “e-government” cards, and much research is being conducted in this area. These would give people access to state services on condition that they prove who they are, for example to get medical or hospital treatment, local government services, such as libraries, and social welfare benefits. The day may not be far off when all these state-run systems will be put on a single card: passport, identity card, driving licence, health record, and “e-government” card.

The power of new technologies is a constant theme of the Future Group report, whether in law enforcement and security, in “border management,” where the “integrated control of EU borders” is recommended, or in “civil protection,” where improved information management is called for, with “better interoperability of

operational techniques."

Reading this report, as with so many others, requires decoding the jargon manufactured by EU bureaucrats, whether for their own self-importance or to disguise their intentions. It is argued that in the "digital tsunami environment" (an extraordinary term, to say the least) citizens' expectations of protection become "ever more acute," especially as traditional measures for protecting privacy "will become less and less effective," making "privacy-enhancing technologies" essential for guaranteeing civil and political rights in the "age of cyberspace." How this might be done in reality is not explained.

Instead the report's emphasis is almost exclusively on the opportunities the "digital tsunami" gives to "public security organisations" to "have access to almost limitless amounts of potentially useful information." Mastering this "data tsunami" will require "automated data analysis" and getting this through to a "multitude of stakeholders" in agencies throughout the European Union. "Interoperability" (access to data-bases in all member-states) is taken for granted: what is needed is for "outputs from different parts of the system" to be shared and a move to "converged networks (or where necessary solutions that ensure [that] all their networks can 'talk' to each other) and [that] all data streams are digital and capable of being meshed together."

Necessary preparatory elements for this strategy are the automated transfer of data and intelligence and defining "what types of information are useful, needed or required . . . So far a total of 49 types of relevant information have been identified, of which six have been the subject of an assessment as to how the principle of availability could be applied to them." These are, as set out in the Prum Decision: "DNA, fingerprints, ballistics, vehicle registration, telephone numbers and minimum data for [the] identification of persons contained in civil registers."

Conclusion

The Future Group report was drawn up by high-level officials and agreed by EU ministers. Frighteningly, they really seem to believe that they are "balancing" the demands of security and civil liberties; they embrace new technology on the grounds that if it is technologically possible it should be used; they assume that the "digital tsunami" should be harvested by "public security organisations," simply because it is there; and they assume that everyone will accept that the "threats" they proclaim require a gargantuan, and privately agreed, leap. There is no recognition that people not only want to live and travel in safety but also want protection from the activities of an all-powerful state.

The creation of a surveillance state—for that is what is being proposed—will take the European Union further down the road to authoritarianism, a path that seems less and less likely to be reversible.

In the aftermath of 11 September 2001 the rationale for new powers, new agencies and new data-bases was presented as if they were exceptional initiatives needed to meet the terrorist threat. We know now that what was termed exceptional has become the

norm, that what were unthinkable (and politically unacceptable) uses of technology only seven years ago are almost upon us.