# Briefing

# EU-wide biometric databases, "soft targets", cybersecurity and data protection: Commission's fourth report on building the 'Security Union'

Chris Jones

February 2017

At the end of January the European Commission issued its fourth report on "building an effective and genuine Security Union", examining four topics: "information systems and interoperability, soft target protection, cyber threat and data protection in the context of criminal investigations." The report puts significant focus on the need for "interoperability" between EU and national-level information systems and databases, in order to enable EU-wide biometric surveillance, one of the current favourite topics of EU security officials.

See: European Commission, **Fourth progress report towards an effective and genuine Security Union** (COM(2017) 41 final, 25 January 2017, pdf)

### Information systems and interoperability

The term "information systems and interoperability" refers to national and EU law enforcement databases and networks and the long-standing ambition of some officials to interconnect them all: "the dream of total data collection," as a report in the *Statewatch* bulletin remarked in 2007. [1]

The Commission's report remarks that the Berlin Christmas market attack in December showed up various weaknesses in information systems:

> *"The fact that the different information systems are not interconnected – allowing attackers to use multiple identities to move undetected, including when crossing borders - and that that information is not routinely uploaded by Member States into the relevant EU databases are practical implementation weaknesses that need urgently to be remedied."*

[1] Heiner Busch, The dream of total data collection: status quo and future plans for EU information systems, *Statewatch Bulletin*, Vol 16(5/6), August-December 2006, p.18, http://www.statewatch.org/subscriber/protected/sw16n56.pdf

Thus, the Commission is keen to start work on a ‘Single Search Portal’, as recommended by the High-Level Group on Information Systems and Interoperability, [2] while Europol is continuing work on a tool (known as QUEST) that will give law enforcement officers access to their national databases at the same time as searching Europol’s systems.

Of course, simply linking up databases will not do much to track down those using multiple identities unless something can be used to link all those identities together – hence the demand for EU-wide biometric identification systems. The report says:

> *“There is a clear need for existing and future EU information systems to be searchable simultaneously using a biometric identifiers to close off this avenue for terrorists and criminals."*

The forthcoming Entry/Exit System may include the development of “shared biometric matching service”, which could:

> *“process both fingerprints and facial images [and] perform identifications and verifications for all the centralised systems (SIS, VIS, Eurodac, the future Entry/Exit System and the European Criminal Records Information System for third-country nationals, and possibly the Europol data). This would not necessarily require any changes to the legal instruments…”*

The EU Agency for Large-Scale IT Systems (eu-LISA) is to undertake a study on the issue, and the Commission notes the possibility – raised in the recent interim report of the High-Level Expert Group and to be examined more closely in its final April 2017 report – of setting up a “common identity repository” including biometric and alphanumeric data. Depending on the scale and scope of collection, it might be more accurate to refer to it as a proposal for an EU-wide population register. [3] In this regard, there is a somewhat unnerving connection between the plans for EU databases and ongoing discussions on “soft targets” (see below).

The Commission’s report continues by calling for swift adoption of the proposals to revise the Schengen Information System, which include requirements for mandatory issuing of alerts on "persons related to terrorist offences", and for which other proposals include permitting searches using biometrics: fingerprints, palm prints and DNA profiles, to be precise, although this is only currently included in the proposal on using the SIS for police and judicial cooperation. [4] Two other proposals deal with “illegally staying third-country nationals” and border checks. [5]

[2] High-level expert group on information systems and interoperability, Interim report by the chair of the high-level expert group, December 2016, http://www.statewatch.org/news/2016/dec/eu-com-hlg-interoperability-report.pdf

[3] Matthias Monroy, The road to a population register: EU Commission outlines roadmap for a “common repository of data”, 5 January 2017, https://digit.site36.net/2017/01/05/the-road-to-a-population-register-eu-commission-outlines-roadmap-for-a-common-repository-of-data/

[4] European Commission, Proposal for a Regulation on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, COM(2016) 883 final, 21 December 2016, http://www.statewatch.org/news/2016/dec/eu-com-883-com-sis.pdf

[5] Proposal for a Regulation on the use of the Schengen Information System for the return of illegally staying third country nationals, http://statewatch.org/news/2016/dec/eu-com-881-com-sis-returns.pdf; Proposal for Regulation on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, http://statewatch.org/news/2016/dec/eu-com-882-com-sis-border-checks.pdf

Member States have also discussed the possibility of adding a new type of alert to the SIS that would allow “preliminary and temporary holding or detention in the context of the fight against terrorism.” [6]

**Protecting "soft targets" against terrorist attacks**

Places where the public are present in large numbers are often referred to in the counter-terrorism and security lexicon as “soft targets”, and they have long been of concern to EU and national officials. A renewed focus has emerged following a November 2016 Europol report that said Islamic State “appears to have a preference for attacking soft targets as a means to instil maximum fear in the general public.” [7]

The Commission describes these locations as:

> *"typically... civilian sites where people gather in large numbers (e.g. public spaces, hospitals, schools, sporting arenas, cultural centers, cafés and restaurants, shopping centres and transportation hubs)."*

The Commission has produced for Member States "operational handbooks and guidance material" on how to better "prevent and respond to soft target attacks," and work is ongoing on "a comprehensive manual on security procedures and templates applicable to different soft targets," which is supposed to be ready in the next few months.

In February the Commission will host Member States at its first workshop on "Soft Target Protection," and at the same time:

> *"The Commission is also funding a pilot project by Belgium, the Netherlands and Luxembourg under the Internal Security Fund to establish a regional Centre of Excellence for law enforcement special interventions, which will offer training to police officers who are often the First Responders in case of an attack."*

The Commission has funded dozens of projects concerning the “protection of soft targets” through the ‘Secure societies’ programme of the Horizon 2020 research and development budget, many of them focusing on forms of pervasive surveillance, tracking and detection. In the latest report on the Security Union, some other sources of financing not usually mentioned in relation to security measures are suggested:

> *"Together with Member States, the Commission will also explore what EU support could be mobilised to help build resilience and strengthen security around potential soft targets. Member States could also apply for financing from the European Investment Bank (EIB) (including the European Fund for Strategic Investments) in line with EU and EIB Group policies.”*

There is also a reference to the conclusions of a workshop held in November 2016 on public transport:

> *"The conclusions underline the significance of building a security culture that encompasses not only staff but also passengers, the importance of local risk assessments as a base for defining appropriate countermeasures and the need to enhance communication between all parties involved."*

[6] Counter-terrorism: alerts for temporary detention to be added to the SIS?, *Statewatch News Online*¸19 December 2016, http://www.statewatch.org/news/2016/dec/eu-sis-detention.htm
[7] Europol, Changes in modus operandi of Islamic State (IS) revisited, November 2016, p.3, http://www.statewatch.org/news/2016/dec/eu-europol-is-mod-op-report.pdf

The conclusions have not yet been made public, but other information on related ongoing work is available from the Commission's page on its Expert Group on Land Transport Security. [8]

A recent study on rail travel security produced for the Commission by the transport sector consultants Steer Davies Gleave  recommends mandatory CCTV "with recording and facial recognition" on all high-speed trains and platforms. The preliminary findings of the report were presented at the Expert Group's meeting in October 2016, where the Commission "made a disclaimer that the study has not yet been agreed by the Commission and no operational conclusion has been drawn." Meeting participants were nevertheless invited to express their views. If any were forthcoming, they have not been included in the minutes. [9]

Here lies the link with the proposals on interconnecting databases: in a scenario in which Europe's security systems (for example facial recognition on trains) and databases were all seamlessly interconnected, the Berlin Christmas market attack culprit would – in theory – have been apprehended far sooner, if he had managed to carry out the attack at all. But, assuming it were actually possible, would it really desirable to submit society to constant biometric surveillance, tracking and checking in the name of preventing attacks that, while horrifying, remain relatively uncommon occurrences?

**Facing the challenges of cyber threats**

The Commission's report warns that:

> *"As we increasingly rely on on-line technologies, our critical infrastructures (ranging from hospitals to nuclear power plants) will become ever-more vulnerable."*

The EU is thus pushing for the implementation of existing measures – for example the Network and Information Security (NIS) Directive [10] – and is working on a progress report alongside the Council and the EU's foreign and security policy chief, Federica Mogherini, which will evaluate progress on the 22 operational actions outlined in EU's 'Joint Framework on Countering Hybrid Threats'.

Reference is also made to the EU's €1.8 billion "private partnership on cyber security with industry". This was agreed in July 2016 and will see an industry-led consortium draw up a "strategic research agenda" on cybersecurity. Officially called a "public-private partnership", one wonders if the typo in the Commission's report could say more about the direction of the "partnership" than intended.

New proposals on cybersecurity are on the way:

> *"in the coming months, the Commission and the EU High Representative will identify the actions needed to provide an effective EU-wide response to these threats, building on the 2013 EU Cybersecurity Strategy."*

[8] Expert Group for Land Transport Security, http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2821

[9] European Commission, Summary report of the 13th meeting of the Expert Group for Land Transport Security, 18 October 2016, http://www.statewatch.org/news/2017/feb/eu-com-land-transport-security-expert-group-minutes-10-16.pdf

[10] Cybersecurity: report on national implementation of the Network and Information Security Directive, *Statewatch News Online*, 9 January 2017, http://www.statewatch.org/news/2017/jan/eu-nis-implementation.htm

**Protecting personal data while supporting efficient criminal investigations**

The Commission notes the importance of the Data Protection Directive in the police and criminal justice sectors, which it refers to as “a building block in the fight against terrorism and serious crime.” Adopted around the same time as the General Data Protection Regulation, the Directive has received far less attention, although an academic workshop held shortly after its approval raised a number of concerns and potential shortcomings. [11]

The Commission is also keen to highlight its proposal issued earlier this month for an ePrivacy Regulation (updating the 2002 ePrivacy Directive). [12] EDRi has noted that “strong forces seem to have watered down the [Commission’s] text considerably, compared to the earlier version that was leaked in December 2016,” [13] and called for the European Parliament to ensure that the text ensures a high level of privacy.

The Commission’s report on the Security Union notes two of the provisions of the proposal relating to law enforcement:

- The obligation for electronic communications service providers based outside the EU to appoint a representative in a Member State, giving “Member States the possibility to facilitate law enforcement and judicial authorities’ cooperation with service providers to access electronic evidence”; and
- The fact that the possibility for introducing national data retention schemes, as permitted by Article 11 of the current ePrivacy Directive, remains unchanged, and the Commission is developing guidance on how national data retention laws can be made compatible with the recent Court of Justice ruling in Watson and Tele2. [14]

The issue of electronic evidence-gathering, particularly from non-EU jurisdictions, has been on the agenda of EU law enforcement and judicial agencies for some time. In June the Council adopted conclusions on the issue [15] and EU agencies and Member States have been cooperating on the topic for some time. [16]

[11] Fanny Coudert, The Directive for data protection in the police and justice sectors: towards better data protection?, *KU Leuven*¸26 April 2016, https://www.law.kuleuven.be/citip/blog/the-directive-for-data-protection-in-the-police-and-justice-sectors-towards-better-data-protection/

[12] Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), http://www.statewatch.org/news/2017/jan/eu-com-privacy-and-coms-reg-com-10-17.pdf

[13] e-Privacy Regulation: Good intentions but a lot of work to do, *EDRi*, https://edri.org/eprivacy-regulation-good-intentions-lot-of-work-to-do/; and the leaked draft of the proposed regulation, http://www.statewatch.org/news/2016/dec/eu-com-eprivacy-directive-draft-politico-leak.pdf

[14] Judgment of the Court (Grand Chamber), Joined cases C-203/15 and C-698-15, 21 December 2016, http://www.statewatch.org/news/2016/dec/cjeu-watson-judgment-surveillance-blanket-retention.pdf

[15] Available here: EU: Justice and Home Affairs Council, 9-10 June 2016: adopted conclusions and action plans, *Statewatch News Online*, June 2016 http://database.statewatch.org/article.asp?aid=36639

[16]  Cybercrime, encryption, obtaining evidence from the "cloud": report on Eurojust seminar "Keys to Cyberspace", *Statewatch News Online*¸14 November 2016, http://statewatch.org/news/2016/nov/eu-eurojust-cyberspace.htm; German and French interior ministers demand EU discussion on undermining encryption, *Statewatch News Online*, 11 November 2016, http://statewatch.org/news/2016/nov/de-fr-comms-letter.htm

### Next report

The Commission’s report says that the next update on the Security Union will be published on 1 March.

### Previous Commission reports

Third progress report towards an effective and genuine Security Union (COM(2016) 831 final, December 2016, pdf)

Second progress report towards an effective and genuine Security Union (COM(2016) 732 final, November 2016, pdf)

First progress report towards an effective and genuine Security Union (COM(2016) 670 final, October 2016, pdf)

---

*Statewatch does not have a corporate view, nor does it seek to create one, the views expressed are those of the author. Statewatch is not responsible for the content of external websites and inclusion of a link does not constitute an endorsement.*

Statewatch is a non-profit-making voluntary group founded in 1991. It is comprised of lawyers, academics, journalists, researchers and community activists. Its European network of contributors is drawn from 18 countries. Statewatch encourages the publication of investigative journalism and critical research in Europe the fields of the state, justice and home affairs, civil liberties, accountability and openness.

One of Statewatch's primary purposes is to provide a service for civil society to encourage informed discussion and debate - through the provision of news, features and analyses backed up by full-text documentation so that people can access for themselves primary sources and come to their own conclusions.

Statewatch is the research and education arm of a UK registered charity and is funded by grant-making trusts and donations from individuals.

**Web: www.statewatch.org | Email: office@statewatch.org | Phone: +44 (0) 207 697 4266**

**Post: c/o Resource for London, London, N7 6PA**

Charity number: 1154784 | Company number: 08480724
Registered office: 2-6 Cannon Street, London, EC4M 6YH