Special Issue Article

NJECL

New Journal of European Criminal Law
2023, Vol. 14(2) 206–230

DOI: 10.1177/20322844231178927
journals.sagepub.com/home/nje
Sage

(Covert) Surveillance of Foreign Terrorism Fighters via the Schengen Information System (SIS): Towards Maximum Operationalisation of Alerts and an Enhanced Role for Europol

Niovi Vavoula
Queen Mary University of London, UK

Abstract
This article aims to critically evaluate how the legal framework of the Schengen Information System (SIS) and its practical implementation have evolved to address concerns regarding the phenomenon of foreign terrorist fighters (FTFs) and which operational and fundamental rights challenges this evolution poses. In that regard, emphasis is placed on two examples: first, the article examines the maximised operationalisation of alerts on discreet checks under Article 36 of the SIS Regulation on police and judicial cooperation in criminal matters. Then, focus is placed on the forthcoming iregistration of alerts on third-country nationals in the interest of the Union based on Regulation 2022/1190. These alerts will be registered in the SIS with the increased involvement of Europol following information received by third countries or international organisations.

Keywords
Schengen information system, foreign terrorist fighters, Europol, data protection, alerts

Corresponding author:
Niovi Vavoula, Department of Law, Queen Mary University of London, Mile End Road, London E1 4NS, UK.
Email: n.vavoula@qmul.ac.uk

Introduction

In the past decade, the phenomenon of foreign terrorist fighters (FTFs) has risen high in the EU security agenda, as FTFs returning from conflict areas may engage in violence, spreading terrorist propaganda and recruiting followers in Member States, and may attempt to orchestrate attacks in the EU. The EU Security Union Strategy places emphasis on addressing the phenomenon, stating that "[t]he threat posed by radicalised individuals remains high – potentially bolstered by returning foreign terrorist fighters and by extremists released from prison".[1] A key strand of action by the EU to tackle the issue of FTFs has been the strengthening of information exchange, and a wide array of legal instruments and policies, such as the EU Passenger Name Record (PNR) Directive,[2] have been adopted, many of which are discussed in this Special Issue. Known as the "heart" of the compensatory measures adopted for the abolition of internal border controls, the Schengen Information System (SIS) – the most widely used and largest information sharing system for security and border management in Europe – has been a first-class tool for enabling such information exchange by the recording of alerts that are accessible by different national authorities depending on their purpose.

This article has a twofold aim: first, to map how the SIS has maximised covert surveillance on suspected FTFs in the form of monitoring their movements and associations, and, second, to critically evaluate the challenges posed by surveillance via the SIS to the fundamental rights of the individuals whose personal data are recorded in the system. After a brief outline of the SIS rules in order to introduce readers to the intricacies of the system, the article explores the early changes in the SIS in response to terrorism concerns so as to inform the subsequent analysis and draw parallels. Emphasis is then placed on two instances whereby FTF-related concerns are particularly visible and have been translated into policy and/or legislative reform. First, the article examines the case of alerts on discreet and specific checks, which allow for covert surveillance of individuals suspected of serious criminality and have been increasingly used to monitor the movement of suspected FTFs. Second, the article looks into a second example which concerns the expansion of Europol's mandate, giving the agency the possibility to propose to Member States the entry of a new category of alerts into the SIS, which also have a surveillance effect, the so-called information alerts in the interest of the Union. Finally, the article summarises the findings of the research and proposes important revisions to improve transparency in the operationalisation of the SIS.

The SIS in a nutshell

Launched in 1995, the overarching purpose of the SIS is to ensure a high level of security in a borderless Schengen area by facilitating both border control and police investigations.[3] The SIS

1. Commission, 'EU Security Union Strategy' (Communication) COM(202) 605 final, 6.
2. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime [2016] OJ L119/132.
3. In its early days, the specific objective of the SIS was twofold; a) to maintain public order and security, including State security and b) to enable the Contracting parties to automatically search the information on persons and objects registered therein for the purposes of border control and police investigations, control and other searches. See the Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders [2000] OJ L239/19 (CISA), art 93.

legal framework has undergone multiple reforms[4] and it is currently comprised of the following instruments: Regulation (EU) 2018/1860 on the use of the SIS for the return of illegally staying third-country nationals;[5] Regulation (EU) 2018/1861 on the establishment, operation and use of the SIS in the field of border checks;[6] and Regulation (EU) 2018/1862 on the establishment, operation and use of the SIS in the field of police cooperation and judicial cooperation in criminal matters,[7] as amended by Regulation (EU) 2022/1190.[8]

To pursue its aims, the SIS stores so-called 'alerts', understood as a set of data entered into the system, allowing the competent authorities, which may be border, law enforcement, custom or prosecutorial authorities, to identify a person or an object with a view to taking specific action.[9] Alerts, which are around 90 million,[10] may be entered for the following categories of individuals and objects: (a) third-country nationals subject to return decisions issued by the Member States;[11] (b) third-country nationals to be refused entry or stay in the Schengen area;[12] (c) persons wanted for arrest to be surrendered or extradited;[13] (d) missing persons or vulnerable persons who need to be

4. Originally, the SIS rules were envisaged in the Convention Implementing the Schengen Agreement, which was replaced by Regulation (EC) 1987/2006 of the European Parliament and of the Council on the development, operation and use of the second generation Schengen Information System (SIS II) [2006] OJ L381/4 (SIS II Regulation); Regulation (EC) 1986/2006 of the European Parliament and of the Council of 20 December 2006 regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates [2006] OJ L381/1; Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) [2007] OJ L205/63 (SIS II Decision). For a detailed overview of those rules see Evelien Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System* (Martinus Nijhoff 2008); Stephen Kabera Karanja, *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation* (Martinus Nijhoff 2008).
5. Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals [2018] OJ L312/1 (SIS Regulation for returns).
6. Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006 [2018] OJ L312/14 (SIS Regulation for border checks). For an analysis see Niovi Vavoula, *Immigration and Privacy in the Law of the European Union: The Case of Information Systems* (Brill 2022); Simona Demkova, *EU Automated Decision-Making and Effective Remedies: The New Dynamics in the Protection of Fundamental Rights in the Area of Freedom, Security and Justice* (forthcoming Edward Elgar); Evelien Brouwer, 'Schengen's Undesirable Aliens' in Paul Minderhoud, Sandra Mantu and Karin Zwaan (eds), *Caught in between Borders - Citizens, Migrants, Humans: Liber Amicorum in honour of prof.dr. Elspeth Guild* (Wolf Legal Publishers 2019).
7. Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU [2018] OJ L312/56 (SIS Regulation for police and judicial cooperation in criminal matters).
8. Regulation (EU) 2022/1190 of the European Parliament and of the Council of 6 July 2022 amending Regulation (EU) 2018/1862 as regards the entry of information alerts into the Schengen Information System (SIS) on third-country nationals in the interest of the Union [2022] OJ L185/1.
9. SIS Regulation for police and judicial cooperation in criminal matters, art 3(1).
10. eu-LISA, 'SIS II Annual Statistics 2021' (March 2022).
11. SIS Regulation for returns, art 3.
12. SIS Regulation for border checks, art 24.
13. SIS Regulation for police and judicial cooperation in criminal matters, arts 26-31.

prevented from travelling;[14] (e) persons sought to assist with a judicial procedure;[15] (f) persons and objects (such as vehicles, aircrafts, containers) to be subjected to discreet checks, inquiry or specific checks;[16] (g) objects for seizure or use as evidence in criminal proceedings;[17] and (h) unknown wanted persons for the purposes of identification under national law.[18] The variety of possible alerts reflect the system's overall purpose, which is not unitary.[19] Two branches have thus emerged, immigration and law enforcement, but alerts involving different individuals or events that are inserted under different legal bases may be interlinked.[20]

Each alert contains information about a particular person (a series of biographical and biometric data, to the extent available) or object, but also envisages clear instructions for concrete action to be taken by national officers when the person or object is found.[21] Therefore, the alerts are not meant to provide exhaustive information about the wanted or missing person or object; instead, complementary information may be exchanged through the SIRENE (Supplementary information request at the national entries) Bureaux. The retention period varies depending on the type of alert; alerts on unwelcome third-country nationals, individuals wanted for surrender or extradition and missing persons are, as a rule, stored for five years, alerts on persons sought to assist with a judicial procedure and on unknown persons to be identified for three years, and alerts on vulnerable persons to be prevented from travelling and discreet checks, inquiry checks or specific checks for one year.[22]

Overall, the system has been designed to be flexible and adaptable to new challenges and the evolution of digital technologies, as evident by its multiple legislative reforms. This flexibility exemplifies how the EU approach to counter-terrorism has always involved the maximisation of the SIS functionalities. For example, the terrorist events of 9/11, coupled with the Madrid bombings of 2004, led to the informal expansion of SIS capacities to allow access by security and intelligence services,[23] and prescribe the registration of persons included in the UN terrorist list established by the Sanctions Committee on Afghanistan, based on UN Security Council Resolution 1390/2002.[24] Furthermore, Council Regulation (EC) No 871/2004[25] and Council Decision 2005/211/JHA[26] aimed to improve the SIS's capabilities in the fight against terrorism – for instance, by allowing Europol and Eurojust to access the SIS in respect of certain types of alerts of the criminal-law

14. Ibid arts 32-33.
15. Ibid arts 34-35.
16. Ibid arts 36-37.
17. Ibid arts 38-39.
18. Ibid arts 40-41.
19. Commission, 'Overview of information management in the area of freedom, security and justice' (Communication) COM(2010) 385 final, 22.
20. SIS Regulation for police and judicial cooperation in criminal matters, art 63; SIS Regulation for border checks, art 48.
21. For the categories of personal data collected and stored see SIS Regulation for police and judicial cooperation in criminal matters, art 20; SIS Regulation for border checks, art 20; SIS Regulation for returns, art 4.
22. SIS Regulation for police and judicial cooperation, art 53; SIS Regulation for border checks, art 39. All alerts may be renewed following a comprehensive individual assessment on the necessary and proportionate for the purposes for which the alert was entered
23. Ben Hayes, 'From the Schengen Information System to the SIS II and the Visa Information System (VIS): The Proposals Explained' (Statewatch 2004) 9.
24. UN Security Council Resolution 1390/2002, S/RES/1390 (2002).
25. Council Regulation (EC) No 871/2004 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism [2002] OJ L162/29.
26. Council Decision 2005/211/JHA of 24 February 2005 concerning the introduction of some new functions for the Schengen Information System, including in the fight against terrorism [2005] OJ L68/44.

branch, so that the alerts could feed into the agencies' operations in cross-border crime.[27] Additionally, in the first overhaul of the SIS rules, among many other reforms, a new category of third-country nationals was to be included in the system: individuals subject to a restrictive measure intended to prevent entry into, or transit through, Member States, including measures implementing a travel ban issued by the Security Council of the United Nations.[28]

Overall, the SIS was conceived as a means of enhancing inter-state cooperation reflecting mutual trust among Member States and is now operational in 30 Schengen States.[29] EU agencies, particularly the European Border and Coast Guard (EBCG) Agency, Eurojust and Europol have progressively acquired access to some or all the alerts stored in the system, depending on their mandate.[30] Europol's role is a bit more advanced; considering that the agency constitutes the EU's criminal information hub, it is part of the SIRENE Network and is able to receive and process supplementary information exchanged by the SIRENE Bureaux.

The case of alerts on discreet checks

The nature of alerts on discreet checks

As early as 2013, when the FTF phenomenon started becoming a concern, emphasis was placed on the role of the SIS in registering alerts against suspected FTFs.[31] At the forefront of the attention was the registration of alerts on persons or objects for discreet or specific checks under Article 36 of Council Decision 2007/533/JHA (which regulated the law enforcement branch of the SIS at the time). In particular, Article 36(2) enabled national authorities to register alerts on discreet or specific checks pursuant to national law for the purposes of prosecuting criminal offences and preventing threats to public security where there is a clear indication that a person intends to commit or is committing a serious criminal offence or where an overall assessment of a person gives reason to believe that that person will also commit serious criminal offences in the future. Article 36(3) further prescribed that authorities responsible for national security, including intelligence services, could also request the issuance of an alert on discreet or specific check for the prevention of threats, including threats to internal or external national security. Thus, either police authorities or secret services are entitled to issue secret surveillance alerts. According to Article 37 of Council Decision 2007/533/JHA, the alert contains information on the fact that the person of interest has been located and the modalities of that detection: the place, time and grounds for the check, itinerary and destination, accompanying persons or passengers and items carried. The means of transport used (including vessels, aircraft and containers) and the circumstances under which the person or the vehicle, boat, aircraft or container was located may be also logged.

27. ibid art 1(9).
28. Regulation (EU) No 1987/2006, art 26. Interestingly, these alerts may be entered on the basis of incomplete data, such as merely using the person's alias, which may lead to increased false positive matches (meaning that a number of individuals may be wrongly identified based on partial information) or no matches, thus affecting the effectiveness of these alerts.
29. The Member States of the EU connected to the SIS are: Austria, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden. The United Kingdom was disconnected on 1 January 2021. The Associated Countries connected to SIS are: Iceland, Liechtenstein, Norway and Switzerland. Ireland operates the law enforcement branch of SIS.
30. SIS Regulation for border checks, arts 35-36. SIS Regulation for police and judicial cooperation, arts 48-51.
31. Council, Document 9946/1/13 (28 May 2013).

Alerts under Article 36 enable secret surveillance of individuals who are not subject to a European Arrest Warrant (EAW) and thus cannot be arrested. In the case of discreet checks, the individuals cannot be searched either. The interest rather lies in obtaining information on their movements or persons accompanying them; whenever the individuals in question are intercepted within the Schengen area, the interested authority is notified. While persons are unaware that they are under surveillance when intercepted, their items may be covertly searched. Discreet checks are, therefore, generally invisible, resulting in the mere monitoring of whereabouts and related circumstances of individuals, whereas specific checks may lead to searching the person or object pursuant to national laws. Individuals are not informed and may only realise that they are subject to a discreet check alert by inference. This invisibility of discreet checks has been an advantageous feature, which is not found in specific checks, and has made them particularly attractive for being used in the case of FTFs.

Enhancement of the SIS as a response to the phenomenon of FTFs: Feeding the SIS with alerts on discreet checks

In 2013, the EU Counter-Terrorism Coordinator called for the "increased and harmonised use of the SIS alert system".[32] The calls for intensifying Member States' efforts in populating the system with FTF alerts multiplied – at the time around 40,000 alerts were recorded, as shown in Figure 1, coupled with efforts to develop a list of criteria for inserting such alerts into the system. Such a list

	Number of alerts	Hits
2013[33]	41,097	14,169
2014[34]	46,528	23,942
2015[35]	69,475	34,313
2016[36]	96,073	60,867
2017[37]	129,983	79,923
2018[38]	156,534	89,763
2019[39]	168,032	98,383
2020[40]	161,634	65,877
2021[41]	155,816	65,388

Source: Author's own compilation based on eu-LISA's reports, as listed in the footnotes.

Figure 1. Article 36 alerts in the SIS.
Source: Author's own compilation based on eu-LISA's reports, as listed in the footnotes.[33–41]

32. Ibid
33. eu-LISA, 'SIS II – 2013 Statistics' (June 2014).
34. eu-LISA, 'SIS II – 2014 Statistics' (October 2015).
35. eu-LISA, 'SIS II – 2015 Statistics' (March 2016).
36. eu-LISA, 'SIS II – 2016 Statistics' (February 2017).
37. eu-LISA, 'SIS II – 2017 Statistics' (February 2018).
38. eu-LISA, 'SIS II – 2018 Statistics' (February 2019).
39. eu-LISA, 'SIS II – 2019 Statistics' (March 2020).
40. eu-LISA, 'SIS II – 2020 Statistics' (March 2021).
41. eu-LISA, 'SIS II - 2021 Statistics' (March 2022).

developed by the Ministers of the Interior coming from the EU countries "most concerned by the issue of foreign fighters" emerged in July 2014.[42] These criteria included knowledge that the person intends to leave or has left the territory of a Member State to reach a jihadi area of conflict, or knowledge that the person has the intention to leave or has left a jihadi area of conflict.[43] More contentiously, one of the criteria concerned cases where an individual facilitated such activities (e.g., driving a suspected FTF to the airport).

Following the Charlie Hebdo events, the Riga Joint Statement of February 2015 reaffirmed the need to reinforce information exchange and develop further cross-border cooperation on fighting trafficking of firearms by systematically ientering information into the SIS.[44] In the Council meeting following the Paris events in November 2015, Member States were called to ensure that national authorities systematically enter data on suspected FTFs into the SIS, in particular under Article 36(3) of the SIS II Decision regarding discreet checks.[45] This followed the replies to a questionnaire circulated among Member States a few weeks earlier.[46] These revealed that, in absolute terms, there had been a significant increase of alerts entered in 2015 compared with 2014,[47] as also shown in Figure 1, but that there was disparity between the actual threat posed to some EU Member States and the amount of alerts entered and that the number of SIS alerts entered under Art. 36(3) remained generally very low and several Member States had not used this legal basis for entering alerts on discreet checks.[48] Furthermore, the possibility for immediate reporting, introduced by the Implementing Decision, was underused.[49] Overall, despite the efforts to reinforce the use of the SIS to tackle the phenomenon of FTFs, the Council acknowledged that there was a lack of comprehensive and consistent action by the Member States. This could be attributed to the reluctance of the national security services to use the SIS due to the sensitive and confidential nature of the information. Thus, Member States themselves could be considered as putting a brake to the fight against FTFs. To further promote the use of the system, a Catalogue of Best Practices and Recommendations was issued in December 2015.[50]

42. Council, Document 12757/14 (4 September 2014).
43. Ibid Annex 1.
44. Council, Document 5855/15 (2 February 2015).
45. Council, Document 14406/15 (20 November 2015).
46. Council, Document 13059/15 (14 October 2015).
47. This increase must also be viewed in conjunction with the 30% increase of such alerts that was reported in 2014. See Commission, Report from the Commission to the European Parliament and the Council – Fifth bi-annual report on the functioning of the Schengen area 1 November 2013 – 30 April 2014, COM(2014) 292 final.
48. Council, Document 14438/15 (23 November 2015).
49. Ibid. Monroy has revealed that in May 2015, only 319 of the approximately 50,000 secret alerts recorded at that time were marked with this information, compared with 880 in November 2015. Alerts requiring immediate reporting were issued for 6,100 people in September 2016. Matthias Monroy, 'Sharp Increase of Secret alerts in the Schengen Information System' (*DigitSite36*, 1 March 2018) https://digit.site36.net/2018/03/01/sharp-increase-of-secret-alerts-in-the-schengen-information-system/ accessed 31 January 2023.
50. Member States should add photographs and fingerprints, when available, to the alerts. Where there is sufficient evidence, they can issue a European Arrest Warrant (EAW) together with an alert for arrest, which must be interlinked. If the person should be observed, especially entering the Schengen area, a discreet check alert is appropriate. Such an alert can also be issued on his or her vehicle. If there is an operational need, the person's belongings can be also searched if a specific check alert has been issued. If the suspect is still a minor, Member States should issue a missing person alert which will require officers on the ground to place the person under protection and question him or her. Commission Recommendation of 16 December 2015 establishing a catalogue of recommendations and best practices for the correct application of the second generation Schengen Information System (SIS II) and the exchange of supplementary information by the competent authorities of the Member States implementing and using SIS (C(2015) 9169).

Regrettably, there is no requirement for eu-LISA to release statistical data on how the number of alerts issued in each category per Member State on the specific legal basis - Article 36(2) or Article 36(3) – is used or on the distinction between discreet and specific checks.[51] That said, in 2016, the German Ministry of the Interior released information highlighting the uneven use of the alerts.[52] It appeared that 44.34% of all alerts were issued by France, 14.6% by the United Kingdom (UK), 12% by Spain, 10% by Italy and 4.63% by Germany. The statistics did not clarify whether or not the number of alerts entered under Article 36(2) or (3) related to FTFs. Indeed, since February 2015 it has been possible, but not mandatory, for authorities to add a note on the type of crime that the alert involves and to indicate 'terrorism related activity'.[53] In the following years, the statistical data show a sharp increase in the number of alerts on discreet checks. Figure 1 demonstrates that between 2015 and 2018 the registration of these alerts increased by 30% every year, followed by a corresponding increase in the number of hits. Overall, it is deduced that between 2013 and 2021 there was a 300% increase in the number of alerts. Nevertheless, as eu-LISA does not have information on the follow-up procedures at the national level following a hit, it is unclear how effective these alerts have been in practice, i.e. leading to the prevention, detection, investigation and prosecution of terrorism-related offences.

The use of these alerts is problematic, particularly due to the vague wording regarding the criteria used by national authorities to insert them, as neither the SIS rules nor the SIRENE Manual contain binding rules for the registration of such alerts. First, the list of these offences is non-exhaustive: Article 36(2)(a)-(b) refers to serious criminal offences, "such as the offences referred to in Article 2(2) of the Framework Decision 2002/584/JHA". Second, it is unclear how the overall assessment of a person, in particular on the basis of past criminal offences, takes place so as to provide reasons to believe that that person will also commit serious criminal offences in the future. Third, there is unclear variation in the terms used: what is the difference between a "clear indication" under Article 36(2) and a "concrete indication" under Article 36(3)? Fourth, from a historical perspective, Article 36 of Council Decision 2007/533/JHA represents a lower threshold compared to Article 99 CISA, its predecessor, which referred to the commission of "numerous and extremely serious criminal offences". Fifth, the criteria employed for the inclusion of these alerts are highly flexible, since they are entered on the basis of Member States' differing legal frameworks. It is not unknown for alerts to be issued on political activists,[54] which constitutes an abuse of the system. Sixth, there are discrepancies in the issuance and execution of the alerts: some Member States – and this was the case with the UK before Brexit – may not authorise specific checks, in which case they can only register a discreet check alert. Conversely, where the executing Member State does not allow the conduct of specific checks, national authorities must conduct a discreet check, even though the alert may mandate a specific check.

51. A parliamentary question in that respect has been posed to the Commission. See 'Decline in alerts for discreet checks under Article 36 of the Council Decision on SIS II' (26 February 2021) https://www.europarl.europa.eu/doceo/document/E-9-2021-001157_EN.html accessed 31 January 2023. Limited information for the years 2013-2015 on the alerts under Article 36(2) and 36(3) is provided in the 2016 SIS evaluation. Commission, Commission Staff Working Document - Accompanying the document Report from the Commission to the European Parliament and the Council on the evaluation of the second generation Schengen Information System (SIS II) in accordance with articles 24 (5), 43 (3) and 50 (5) of Regulation (EC) No 1987/2006 and articles 59 (3) and 66 (5) of Decision 2007/533/JHA' SWD(2016) 450 final, 40. The alerts by secret services in 2016 amounted to 8,000 out of the 70,000 stored.
52. As retrieved by Monroy (n 49).
53. Commission, Commission Staff Working Document (n 51) 41.
54. Statewatch, 'EU: Council's internal security committee discusses use of "discreet checks" in the Schengen Information System' (28 February 2018) https://www.statewatch.org/news/2018/february/eu-council-s-internal-security-committee-discusses-use-of-discreet-checks-in-the-schengen-information-system/ accessed 31 January 2023.

The vagueness of the criteria to enter alerts on discreet checks raises concerns as to whether the system can be misused through the *en masse* registration of alerts by specific countries. This is more than rhetoric. As early as 2016, it was reported that France was responsible for more than 40% of the alerts and, in early 2018, it was found that France had been responsible for around 60% of the alerts by registering more than 78,000 out of the 134,000 alerts.[55] This misuse has not been picked up by the Schengen Evaluation and Monitoring Mechanism, at least not in official documentation: in December 2021, when the evaluation of France on the application of the Schengen *acquis* in the field of the SIS was released, there was no comment on the large amounts of alerts issued; the only comment in respect of discreet check alerts concerned the need to ensure that it is possible to add the type of the 'terrorism related activity' offence to all the alerts.[56] Overall, France has issued 104,760 such alerts, amounting to 66% of all individuals registered by the Member States, approximately 13,000 of which concern individuals connected to Sunni terrorism – and around 500 alerts per year are recorded based on information received from non-EU States, which is discussed later on.[57] The SIS has received 26,562 'discovery forms', meaning 'hits' from checking States, which suggests that the yearly 'discovery rate' of French alerts amounts to a maximum of 25%.[58]

The *en masse* registration abuses the capabilities of the system and jeopardises its effectiveness by potentially wasting resources on less significant cases and by undermining mutual trust among Member States. This mutual trust operates at different levels; the issuing Member State must trust that other States will effectively cooperate in locating the FTFs and thus contribute to the prevention of internal security threats. At the same time, Member States must trust each other in regard to the quality of the personal data stored – in order words, that the data fed into the system have been entered in a proportionate and lawful manner pursuant to the prescriptions of the SIS rules. This latter dimension of mutual trust is safeguarded through the inclusion of a requirement that only proportionate, adequate, and relevant data must be stored in the system, as enshrined in Article 21 of Council Decision 2007/533/JHA, now Article 21 of the SIS Regulation for police and judicial cooperation in criminal matters.

Most importantly, the differentiated practices at the national level result in a differentiated impact on individuals, who may find themselves affected, depending on whether the issuing Member State follows overzealous practices in registering alerts. Furthermore, *en masse* registration runs counter to the explicit requirement for a proportionality assessment prior to recording an alert. In the absence of common criteria and with the concept of FTFs gradually expanding, individuals run the risk of being unlawfully registered in breach of the principle of proportionality. This may lead to the secret surveillance of the movements of thousands of individuals and, potentially, of their families or contacts. Thus, individuals may be indirectly implicated in terrorism-related activities on the basis of the vague criteria laid down in the SIS legislation. The fact that the numbers remain high may be interpreted in two ways: either the alerts, which are reviewed after one year, are constantly renewed, or new alerts are inserted. Regrettably, there is no information as to whether the alerts are new or old. In addition, in cases where the alerts concern terrorist offences, as in the case of FTFs, Europol must be informed, unless doing so would jeopardise current investigations or the safety of an individual, or would be contrary to essential interests

55. Lori Hinnant, 'France Puts 78,000 Security Threats on Vast Police Database' (*Associated Press*, 4 April 2018) https://apnews.com/a1690ac25cea4d5b8d2b622d3fd4e646 accessed 31 January 2023. The disparity with the eu-LISA number is because the latter corresponds to the number of alerts at the end of 2018.
56. Council, Document 15120/21 (21 December 2021).
57. Council, Document 5009/22 (5 January 2022) 4.
58. Ibid.

of the security of the issuing Member State.[59] This is particularly important, because although the agency may not be able to amend or delete the alert, Europol being informed means that the individual's data may feed into the Europol databases and be integrated within the agency's own analysis, e.g., in the content of analysing trends on terrorism for the production of TESAT reports or in the context of the European Counter Terrorism Centre (ECTC). Thus, the personal data of the alert may continue to be processed in accordance with the Europol rules.

The 2018 SIS reform: The introduction of inquiry alerts

Notwithstanding these major challenges, the quest of how to use discreet checks for counter-terrorism purposes remains ongoing. In the aftermath of the Brussels attacks in March 2016, the Commission called for the creation of a 'Security Union' and, *inter alia*, required Member States to systematically introduce all terrorism information into the SIS, going beyond FTF-related information.[60] In its 2016 Communication on smarter and stronger borders, the Commission stressed – among other shortcomings – the need for storing hit information on discreet and specific check alerts in the SIS.[61] Subsequently, in June 2016, the Council agreed on a Roadmap to enhance information exchange and information management, including interoperability solutions in the Justice and Home Affairs area, which elaborated on the goals regarding the optimisation of the discreet checks alerts in three respects: by agreeing on indicative (thus non limitative or legally binding) criteria for inserting terrorism-related alerts, which have not been developed; by ensuring that Member States insert alerts only when criteria are met, unless there are operational reasons not to; and, by distinguishing those alerts involving terrorism-related activity with a marker – which, as mentioned above, has been done to a certain extent.[62] However, in the absence of binding criteria in legislation, national authorities retain full operational discretion to decide in which cases alerts will be issued and under which category of alerts.[63] Therefore, though the EU legislature is clearly willing to impose limits on, or, put differently, to take away Member States' powers, there appears to be resistance in favour of procedural autonomy.

The evaluation of the SIS released in December 2016 stressed that over 72,000 travelling serious criminals and other people posing threats to security were located on the basis of Article 36 alerts, and highlighted additional needs.[64] However, these needs did not concern the aspects identified in the Roadmap and included: (a) the creation of alerts on identity documents – passports, in particular – linked to individuals subject to the checks; (b) the possibility to temporarily detain a person, to gain more information about their movements and activities — essentially, enabling a check which is not as limited as a discreet check, but which does not involve a full physical search of the person; and (c) the creation of alerts on persons lawfully banned from leaving the Schengen area or their own Member State, on the basis of mutual recognition of national exit bans. As indicated, this latter proposal was partly prompted by considerations relating to the FTF phenomenon, without further explanation on the rationale, simply noting that the SIS does not mandate

59. SIS Regulation for police and judicial cooperation in criminal matters, art 48.
60. Commission, 'Delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union' (Communication) COM(2016) 230 final, 6.
61. Commission, Communication from the Commission to the European Parliament and the Council – Stronger and smarter information systems for borders and security, COM(2016) 205 final.
62. Council, Document 9368/1/16 (6 June 2016) 31–33.
63. Council, Document 12286/16 (19 September 2016).
64. Commission, Commission Staff Working Document (n 51) 41-42.

the issuance of an EU-wide exit ban on a person, which can only be imposed pursuant to national law.[65]

The release of the evaluation was accompanied by a package of proposals reforming the SIS rules, including reforms in the field of police and judicial cooperation in criminal matters.[66] While the SIS package was negotiated, Member States continued considering additional reforms beyond those proposed on how to improve the exchange of information on FTFs and returnees based on the SIS post-hit procedures and to discern how to better use metadata information from SIS hits in order to map patterns of movements of FTF/returnees or individuals involved in terrorism or terrorism-related activities.[67] These tasks are linked to Europol's mandate in mapping and analysing terrorist trends and the work of its ECTC. The revised SIS rules were adopted in November 2018 and entered into force in March 2023, expanding the use of biometrics and introducing the possibility of processing dactylographic data (fingerprints and palm prints) and DNA profiles, expanding access for law enforcement authorities and Europol to all alerts (and the relevant supplementary information exchanged by the SIRENE Bureaux) and introducing new types of alerts, in particular, on unknown wanted persons,[68] on inquiry checks,[69] and on vulnerable persons to be prevented from traveling.[70] As mentioned in the evaluation, an exit ban on FTFs was not included in the revised SIS rules, only exit bans in respect of minors. An inquiry check is an alert lying inbetween discreet and specific checks, allowing authorities to stop and question the person concerned. As a result, it is more in-depth than the existing discreet check but does not involve a search or arrest. It may, however, provide sufficient information to decide on further actions to be taken. The aim of this new type of alert is to assist authorities in gathering essential information for combating terrorism by mandating the conduct of an interview of the person, including on the basis of information or specific questions added to the alert by the issuing Member State. The 'inquiry check' will therefore constitute an intermediate stage in terms of disturbance to the individual. The interview must be carried out in accordance with the law of the executing Member State. The person concerned may, for example, consult a lawyer.

Immediate reporting following a hit requires police cooperation and the adoption of decisions on the fate of the individual concerned on the spot. However, the instructions for action in this context are vague, with limited information on the aftermath following a hit, thus raising risks as to the procedural safeguards applicable to the person questioned. The aforementioned consequences of an alert, however, should not rise to the level of an arrest and to a change of a 'discreet or specific

65. Ibid 43.
66. Commission, Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1986/2006, Council Decision 2007/533/JHA and Commission Decision 2010/261/EU, COM(2017) 883 final. For the other proposals, see European Commission, Proposal for a Regulation of the European Parliament and of the Council on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, amending Regulation (EU) No 515/2014 and repealing Regulation (EC) No 1987/2006, COM(2016) 882 final; Proposal for a Regulation of the European Parliament and of the Council on the use of the Schengen Information System for the return of illegally staying third-country nationals, COM(2017) 881 final.
67. Council, Document 5635/1/18 (13 February 2018) https://www.statewatch.org/news/2018/february/eu-council-s-internal-security-committee-discusses-use-of-discreet-checks-in-the-schengen-information-system/ accessed 31 January 2023.
68. Regulation 2018/1862, arts 40-41.
69. Ibid arts 36-37
70. Ibid arts 32-33.

check' alert to an alert for the purposes of returning the person to the country of origin.[71] This would amount to transforming individuals who may not have committed any terrorist offence at that point or individuals merely suspected of terrorism into convicted criminals facing the penalty of deportation, but without the involvement of a judge to issue a return decision. Coupled with the potential misuse, which must be expected, considering the past experience outlined earlier, individuals may have their free movement rights limited in a disproportionate manner.

Regarding the implementation of the revised rules, the Regulations have followed a step-by-step approach; for example, on 8 January 2020, eu-LISA gave Europol full access to all alerts in SIS, but various delays have ensued due to the complexity and volume of the tests to be executed by all Member States and EU agencies.[72]

The future of alerts on discreet, inquiry and specific checks

The efforts to maximise the use of these alerts continues. The French Presidency of the Council during the first half of 2022 had a particular interest in the use of SIS for counter-terrorism purposes, which is understandable, considering that it has the lion's share in entering such alerts and the terrorist events that have taken place in the past years. The issue for discussion concerns the functionalities of the SIS after a hit, in particular, the fact that only the issuing State (which registered a specific individual into the SIS) and the executing State (where said individual was detected) have access to information on the related SIS hit. Other Member States have no access to the hit, although the same individual might eventually travel to their territories. Additionally, terrorist fighters travelling to or from Europe often use "fragmented routes": for instance, they travel through several countries before returning to their country of origin or reaching their final destination.[73] The French Presidency proposed that Member States should be able to volunteer to be automatically notified of hits on certain terrorist profiles, described as the "most dangerous", namely Islamist terrorists released from prison and linked to Syrian-Iraqi networks; Europeans who have left for the Syrian-Iraq zone; and FTFs "reported by third partners". Individuals representing a home-grown threat, who have no specific European or international contacts with terrorist organisations, would not be affected by this reform.[74] The volunteering States would receive information on hits and could issue restrictive or surveillance measures, where appropriate, based on their own analysis of the threat posed by these individuals.[75]

The expansion of the list of recipients of these alerts would require more than just a revision of the SIRENE Manual, as it has significant fundamental rights implications which go beyond the delegated powers of the Commission. First, it may lead to magnifying and expanding the preventive surveillance powers of the volunteering Member States that will receive notifications of hits, and it will provide justification for extensive data collection,e.g., mass retention of telecommunication metadata and their automated analysis under the banner of national security.[76] In *La Quadrature du Net and Others,* the Court of Justice of the EU has found generalised and indiscriminate surveillance of telecommunications metadata to be permissible under EU law only in relation to national security purposes, which may

71. Council, Document 5635/18 (29 January 2018).
72. Council, Document 11863/21 (6 October 2021).
73. Council, Document 5009/22 (5 January 2022).
74. Council, Document 6246/22 (21 February 2022).
75. Ibid.
76. Statewatch, 'EU: Fine-tuning Surveillance: Proposal to Enhance Monitoring of "Most Dangerous" Terrorists' (22 March 2022) https://www.statewatch.org/news/2022/march/eu-fine-tuning-surveillance-proposal-to-enhance-monitoring-of-most-dangerous-terrorists/,accessed 31 January 2023.

include terrorism, and not in respect of fighting serious crimes.[77] This is particularly worrying, considering the misuse of these alerts, as discussed earlier, which may effectively mean that individuals may be subject to surveillance on the basis of disproportionately inserted alerts. Second, it will lead to a *de facto* expansion of the recipients of supplementary information on the hits, under a broad interpretation of the 'need to know' principle. Third, it may become a gateway, leading to other categories of individuals subject to these alerts also becoming subject to the mechanism.

Finally, the 2022 Council Conclusions on the implementation of the EU information systems and their interoperability at the national level considered that Member States should be able to carry out inquiry and specific checks even when the person concerned is not the subject of a national procedure in the executing Member State *where such checks are authorised by national law.*[78] This is noteworthy because this wording is somewhat watered down compared to a previous version of the conclusions, which did not refer to the existing national laws, thus arguably calling on Member States to (re-)consider their legal framework to ensure operationalisation of these alerts.[79]

What about information from third countries on suspected FTFs?

The 2020 informal protocol

The estimations that, among the 50,000 persons who have travelled to Syria and/or Iraq since 2012 to join Da'esh, European FTF suspects represent just 10% of the estimated total, stirred interest in acquiring information on the identities of all FTFs, both European and non-European, should they try to cross EU borders.[80] This rationale placed the personal data of *non-European FTFs*, which are held by *third countries*, on the EU radar. This constitutes another example of how the flexibility of the SIS as a security tool has resulted in an expansion of the collection of personal data, with the fight against terrorism legitimising the intrusiveness of the measures; the fact that the targeted individuals are third-country nationals made it even easier to justify his course of action.

Discussions on whether it would be possible to establish a procedure for entering information from third countries on suspected non-EU terrorists in the SIS, taking into account legal and operational constraints, particularly with regard to the list of suspected FTFs received by Europol either directly from a third country or from a Member State, emerged in autumn 2019.[81] Europol, as the EU's criminal information hub, may receive information primarily from Member States, as well as private parties or third countries on the basis of operational agreements.[82] However, that information may have only been shared with the agency and not with the Member States, so the

77. Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others* ECLI:EU:C:2020:791.
78. Council, Document 10056/22 (9 June 2022).
79. Statewatch, EU: Council to Push for "on the Spot" Biometric ID Checks, Inserting "All Available Data" in Schengen Information System' (19 May 2022) https://www.statewatch.org/news/2022/may/eu-council-to-push-for-on-the-spot-biometric-id-checks-inserting-all-available-data-in-schengen-information-system/ accessed 31 January 2023.
80. Council, Document 11564/20 (5 October 2020).
81. See Council, Documents 7741/20 (19 May 2020); 7699/20 (30 April 2020); 6322/20 (26 February 2020).
82. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA [2016] 135/53, as amended by Regulation (EU) 2022/991 of the European Parliament and of the Council of 8 June 2022 amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role in research and innovation [2022] OJ L169/1 (Europol Regulation), art 17.

potential exploitability of that pool of information at the domestic level was at stake. At the same time, however, in its more than twenty-year history, Europol has often struggled with the reluctance of national authorities that were – and remain – sometimes not very keen to share their data with the agency. These dynamics create a tension between the distrust of Member States or their unwillingness to give away parts of their sovereign powers regarding the SIS and their eagerness to get their hands on Europol's data. In November 2020, an informal Protocol was agreed that laid down a process for evaluating information from Europol on suspected FTFs from third countries and possibly entering relevant data in the SIS, if legal prerequisites on national and EU levels are met.[83]

The Protocol outlined a voluntary coordinated approach with the involvement of Europol as a middleman, where the agency conducts a first quality check on lists of FTFs, including to verify whether individuals on the list are already included in the SIS and prepares an updated list, enriched with relevant additional information. However, it is not clear what this exactly entails and why Member States must be informed before the first quality check by Europol – presumably to enable Member States to first have the raw data, so that, should Europol discard any information, the Member States could intervene. Following Europol's check, the Member States have the opportunity to conduct a quality check of the list and edit it, if necessary, whereupon a voluntary group of Member States who are willing to further process the list is formed, allowing for its possible entry into the SIS. Member States participating in the voluntary group analyse parts of the list, and alerts may be registered in the SIS by following the usual SIS principles regarding individual assessment and conditions for entering alerts. In such cases, Europol is available to support the Member States. Europol must ensure that information on hits related to FTFs inserted in the SIS is shared in accordance with the SIS Regulation on police and judicial cooperation in criminal matters to the agency's counterparts, thus being subject to the consent of the issuing Member State. This is an oxymoron, considering that the information comes from Europol and a third country, but it is understandable because the data may (or may not) be enriched by the Member States. If a Member State allows the use of such information, its handling by Europol must be governed by the applicable rules on transfer of personal data to third entities, as set out in the Europol Regulation.[84]

The procedure has provided a new, prominent role for Europol, which becomes involved in the processing of the list as a middleman, but ultimately the competent national authorities conduct the heavy assessment of the reliability of the information contained in the list and are entirely responsible for issuing and updating the respective SIS alert. Notwithstanding that, the whole procedure is wholly non-transparent and raises rule-of-law challenges due to its informal character. Sources of concern include the involvement of the agency beyond the prescriptions of the SIS rules, the agency's sources of information, their reliability, the possibility for Europol to insert data through the backdoor, and the extent to which volunteering Member States could effectively verify the information on individuals who may have no connection to the Member State. Furthermore, information on FTFs can be inserted in the system as an alert, but without an obligation to enter it under a particular category of alert; as long as the necessary requirements under the SIS rules and national legislation are met, the information can be scattered throughout the system. Moreover, from an operational perspective, when a volunteering Member State enters the SIS alert, the information

83. See Council Document 13037/20 (16 November 2020). Prior to the agreement, personal data on those individuals were entered on an ad-hoc basis by volunteering Member States that verified the information; issuing Member States were responsible for the accuracy and lawfulness of the personal data entered in the system. See Council Document 11564/3/2020 (16 November 2020).

84. Europol Regulation, art 25.

on a hit is sent back to that Member State which might not have sufficient interest or capacity to follow up a case which potentially has no link to its territory.[85]

The contentious case of information alerts

The 2020 informal Protocol was provisional, as a revision of Europol's mandate was underway, and served as a first-class opportunity to address the matter. On 9 December 2020, the Commission released a proposal amending the Europol Regulation;[86] among the many reforms proposed, Europol would be enabled to enter alerts into the SIS.[87]

A separate proposal amending the SIS Regulation for police and judicial cooperation in criminal matters envisaged a detailed process for the issuance of so-called "information alerts".[88] That proposal prescribed the establishment of a new alert category to be used for the registration of alerts by Europol in order for the agency to provide information directly and in real time to front-line officers, namely police officers and border guards. Such alerts would be issued based on Europol's analysis of information, on the basis of information received from third countries or international organisations in relation to crimes which fall within the agency's mandate and only concerning third-country nationals, excluding those who are beneficiaries of free movement rights.[89] These third-country nationals must either be suspected of having committed or taken part in a criminal offence in respect of which Europol is competent, or convicted of such an offence, or there must be factual indications or reasonable grounds to believe that they will commit criminal offences in respect of which Europol is competent.[90] While the Explanatory Memorandum and the Impact Assessment heavily emphasised a counter-terrorism rationale to justify the need to enable Europol to enter alerts into the SIS, the reform encompassed all criminal offences on which Europol may have third-party sourced information and which fall within Europol's mandate.[91]

The proposal for information alerts foresaw a step-by step approach prior to the entry of an alert in the system. Europol would analyse the information received and carry out a detailed individual assessment, example.g., by cross-checking it against other available information it already holds in its databases, to verify the reliability of the source and the accuracy of the information. If necessary,

85. Council, Internal Document WK 3974/2021 (19 March 2021).
86. Commission, 'Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/794, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation' COM(2020) 796 final.
87. Ibid art 1(2)(a)(iv), aimed to revise Regulation (EU) 2016/694, art 4.
88. Commission, 'Proposal for a Regulation of the European Parliament and of the Counci amending Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters as regards the entry of alerts by Europol' COM(2020) 791 final, 3 (Proposal for information alerts).
89. Ibid art 1(2) (proposed art 3).
90. Ibid art 1(4) (proposed art 37a(1)).
91. Ibid 1; Commission, 'Staff Working Document – Impact Assessment Report accompanying the document Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/79, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation Part 1/2' SWD(2020) 543 final (Europol Impact Assessment Part 1); Commission, 'Staff Working Document – Impact Assessment Report accompanying the document Regulation of the European Parliament and of the Council amending Regulation (EU) 2016/79, as regards Europol's cooperation with private parties, the processing of personal data by Europol in support of criminal investigations, and Europol's role on research and innovation Part 2/2' SWD(2020) 543 final (Europol Impact Assessment Part 2)'.

Europol would exchange further information with the third country or international organisation involved to assess whether entering the alert is necessary for achieving its objectives.[92] Europol would check whether an alert already exists in the SIS on the same person[93] and carry out a prior consultation, in order to confirm that no Member State intends to enter the alert itself based on the information collected by Europol, and that Member States do not object to the alert being entered by Europol.[94] To ensure data protection monitoring by the European Data Protection Supervisor (EDPS), the EU body entrusted with the tasks of supervising data processing activities by EU institutions and agencies, Europol would keep detailed records relating to the entry of the alert and the grounds for such entry that permit verification of compliance with the substantive and procedural requirements.[95] In case of a 'hit', the proposed action to be taken is similar to the action taken in cases of alerts on discreet checks, pursuant to Article 37(1) of the SIS Regulation on police and judicial cooperation in criminal matters. The front-line officer would immediately report the 'hit' to the National SIRENE Bureau, indicating the place, time and reason for the check carried out.[96] The National SIRENE Bureau would then communicate this information to Europol.[97] No further obligation for the Member State was foreseen, but the reporting Member State would have the discretion to determine, on a case-by-case basis, whether further measures would need to be taken with regard to the person *under national law* and at the full discretion of that Member State.[98]

Both proposals entailed considerable implications regarding the nature of the SIS as an instrument exemplifying and fostering mutual trust among Member States and raised concerns both in relation to fundamental rights and operational effectiveness.

First, significant questions were raised as to whether this shift in its Europol's role, which essentially places Europol, whose work is characterised by some secrecy and non-transparency,[99] on a more equal footing with Member States, and whether it is in line with its mandate as an agency aimed to *support* Member States in investigations. The agency would no longer be serving Member States, but Member States would be requested to consider acting upon information fed by the agency. It would bring the agency one step closer to becoming a decision-making body and remove segments of the control that Member States have over the SIS. Such an extension also raised fundamental questions as to whether the principle of mutual trust is, to some degree, extended to Europol and its partners from outside the EU with different legal systems, protection of human rights, procedural safeguards and adherence to the rule of law and whether Europol can and should

92. Commission, 'Proposal for information alerts' (n 88) recital 8 and art 1(4) (proposed art 37a(3)(a)).
93. Ibid recital 9 and art 1(4) (proposed art 37a(3)(c)).
94. Ibid art 1(4) (proposed art 37a(3)(d). For example, for reasons of national security reasons or due to a risk for official or legal inquiries, investigations or procedures.
95. Ibid recital 10 and art 1(4). Elsewhere in the proposal the EDPS should conduct an audit at least every four years. See art 1(5)(d) (proposed art 48(7a)).
96. Ibid art 1(4) (proposed art 37b(1)).
97. Ibid (proposed art 37b(2)).
98. Ibid (proposed art 37b(1)(b)).
99. For example, see European Ombudsman, 'The European Union Agency for Law Enforcement Cooperation's (Europol) public register of documents' https://www.ombudsman.europa.eu/en/opening-summary/en/125610 accessed 31 January 2023; 'Europol: small steps on transparency, but many documents still under lock and key' (*Statewatch*, 15 June 2022) https://www.statewatch.org/news/2022/june/europol-small-steps-on-transparency-but-many-documents-still-under-lock-and-key/ accessed 31 Januaey 2023.

be allowed to operate as a Member State. In that regard, the wide scope of information alerts beyond terrorism-related activities – though counter-terrorism was the predominant underlying reason behind the reform – was also problematic.[100]

Second, from a fundamental rights perspective, the proposal for information alerts aimed to bypass national constraints as regards the entry of SIS alerts, as well as the lack of information from national authorities, which may not receive information from third countries and establish alerts on threats against collectively the EU internal security, without the need for a national interest. The potential misuse of such alerts, whereby the threat that individuals may pose would first be determined according to the standards of third countries and transplanted into the EU, is highly problematic, as the threat may be remote or even non-existent. Important data protection concerns were also raised as to whether and how Europol could analyse information received from third countries or organisations to undertake a meaningful quality check and thus comply with the principle of data accuracy.[101] Europol has signed a series of operational agreements with third countries, including the US, on the basis of which the agency receives information from those partners, some of which agreements are quite old.[102] For example, the agreement with the USA has been criticised for not meeting legal safeguards including on data protection.[103] In particular, the 2002 Supplemental Agreement with the USA makes no mention of an adequate level protection of personal data and is laconic about data protection safeguards, while its provisions on liability are unclear and it does not include elaborated provisions on dispute settlement. However, the existence of these agreements does not automatically signify that those countries are trustworthy sources of information. The proposal for information alerts did not contain criteria to qualify specific third countries as trustworthy and to verify the reliability and accuracy of information. Furthermore, it was doubtful whether Europol could provide such assessment, given the potentially large quantity of data involved, which must be dealt with on a case-by-case basis. The verification could potentially be more problematic in cases where more than two countries are involved, e.g., when one third country has information about an individual who does not hold the nationality of that country and resides in a different third country (e.g. information from the USA on an Algerian FTF in Syria).[104]

100. A proposal to delimit the scope to terrorism-related activities and from trusted countries, namely third countries with which Europol has an operational agreement or which are subject to the Commission adequacy decision was made. See Council Document 7732/21 (13 April 2021).
101. Europol Regulation, art 75, referring to the applicability of Chapter IX of Regulation (EU) 2018/1975. See Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2019] OJ L295/39, art 71(1)(d).
102. For Europol's operational agreements see https://www.europol.europa.eu/partners-agreements/operational-agreements?page=1.
103. Dick Heimans, 'The External Relations of Europol – Political, Legal and Operational Considerations' in Berndt Martenczuk and Servaas van Thiel (eds), *Justice, Liberty and Security: New Challenges for EU External Relations* (VUBPRESS 2008) 385-387; Florin Coman-Kund, 'Europol's International Cooperation between 'Past Present' and 'Present Future': Reshaping the External Dimension of EU Police Cooperation' (2018) 2(1) Europe and the World 1.
104. In 2019, Europol accepted almost 12,000 operational contributions from third countries, and there were over 700,000 objects recorded in the Europol Information System that stem from Europol's analysis of data it received from third countries. Commission, 'Europol Impact Assessment Part 2' (n 91) 89. However, more information was needed on whether Europol rejected information from third countries or whether following its own analysis Europol incorporates *en masse* information from third countries and organisations.

Third, from an operational perspective, the alerts would have limited operational value. National police officers and border guards would be merely required to inform Europol and decide in accordance with their national law whether to take further action. The potential further action to be taken by Member States was vague, as was the responsibility of Member States, which would have to decide on whether and what action should be taken to adequately respond, without much clarity about the purpose to be achieved. This could lead to wide divergences at the national level and, consequently, fragmented and uneven implementation. The type of action undertaken by Member States is also unclear, e.g., whether alerts should lead to proactively open investigations or as an open suggestion to assist a third country in their investigation, even if the Member States themselves might have no clear interest.[105] Further legality issues could occur in cases where a front-line officer takes concrete action on the basis of an information alert which has been entered without appropriate control.

Surveillance of third-country nationals suspected FTFs: A remote danger?

The aforementioned concerns signified that the proposed rules on governing information alerts were heavily revised. On 6 July 2022, the co-legislators adopted Regulation (EU) 2022/1190 establishing the category of information alerts to be entered into the SIS. The scope of these alerts has remained the same as in the proposal, e.g., third-country nationals suspected to be involved in offences falling within Europol's mandate, and their aim is to monitor their movement and to make all information on the suspect available directly and in real time to front-line officers in Member States.[106]

However, the process is fundamentally different: Regulation (EU) 2022/190 enables Member States to register information alerts in the SIS on third-country nationals in the interest of the Union following a proposal by Europol to enter an information alert on the basis of information received from the authorities of third countries or international organisations.[107] Europol must notify its Data Protection Officer where it makes such a proposal,[108] which is not a ground-breaking safeguard, considering that its role is merely to be informed. Europol will propose to Member States to enter information alerts into the SIS in the following situations: (a) where there is a factual indication that a person intends to commit or is committing any of the mentioned offences; or (b) where an overall assessment of a person, in particular on the basis of past criminal offences, gives reason to believe that that person may commit such offence.[109]

Prior to proposing the registration of an information alert, Europol must establish that the information alert is necessary and justified, e.g., Europol must be certain that the information received is from a reliable source and accurate, and that no other alert on the person concerned already exists in the SIS.[110] To that end, Europol is allowed, where necessary, to carry out further exchanges of information with the third country or the international organisation.[111] As such, this possibility opens the door for expanding the exchange of information with third countries beyond the prescriptions of the Europol Regulation. In order for the Member State to which Europol

105. Ibid.
106. Ibid recital 6.
107. Ibid art 37a(1).
108. Ibid.
109. Ibid art 37a(3).
110. Ibid art 37a(4).
111. Ibid.

proposed the entry of an information alert to assess a case, Europol must share all the information it holds on the case and the assessment of the person concerned, which also constitutes an expansion of the information exchanges compared to the previous regime.[112] Furthermore, the agency must inform Member States without delay if Europol has relevant additional or modified data in relation to its proposal to enter an information alert into SIS or evidence suggesting that data included in its proposal are factually incorrect or have been unlawfully stored.[113] Where an alert is issued, Europol must transmit information to the issuing Member State as soon as possible if it has evidence suggesting that data entered into SIS as information alert are factually incorrect or have been unlawfully stored (e.g., if third countries provide the information for politically motivated reasons).[114] Records relating to its proposals must also be kept and reports must be provided to Member States every six months on the information alerts entered into SIS and on the cases where Member States did not enter the information alerts.[115]

Member States are explicitly given discretion as to whether to enter an information alert or not, but must also perform several obligations: they must verify and analyse Europol's proposal to assess whether a particular case is adequate, relevant and important enough to warrant the entry of that information alert into SIS, and in order to confirm the reliability of the source of information and the accuracy of the information on the person concerned, but the legislation does not specify how this can take place.[116] If an information alert is entered in the SIS, other Member States and Europol must be informed. To this end, Member States must put in place a periodic reporting mechanism.[117] In any case, Member States must also inform other Member States and Europol on the outcome of the verification and analysis of the data within 12 months after Europol's proposal.[118] Where Member States decide not to record the information alert and where the respective conditions are met under national legislation, they may decide to enter another type of alert on the same person.[119] Alerts on objects related to the persons subject to information alerts may also be entered and interlinked with the information alerts with a view to locating the person.[120]

In terms of action following a hit on an information alert, Article 37b prescribes that the reporting Member State must collect and communicate to the issuing Member State via SIRENE certain information, similar to the information collected in respect of discreet, inquiry and specific checks.[121] Such information must be collected even when the person is located by the issuing

112. Ibid art 37a(5). According to recital 8 'Europol should share all of the information that it holds on the case, except for information which has clearly been obtained in obvious violation of human rights. Europol should share, in particular, the outcome of cross-checking the data against its databases, information relating to the accuracy and reliability of the data and its analysis of whether there are sufficient grounds for considering that the person concerned has committed, taken part in, or intends to commit a criminal offence in respect of which Europol is competent'.
113. Ibid.
114. Ibid recital 8 and art 37a(10).
115. Ibid art 37a(14).
116. Ibid art 37a(6).
117. Ibid art 37a(7).
118. Ibid art 37a(9).
119. Ibid art 37a(8).
120. Ibid art 37a(12).
121. Ibid art 37b(1). These are: (a) the fact that the person who is the subject of an information alert has been located; (b) the place, time and reason for the check; (c) the route of the journey and destination; (d) the persons accompanying the subject of the information alert who can reasonably be expected to be associated with the subject of the information alert; (e) objects carried, including travel documents; (f) the circumstances in which the person was located.

Member State so that Europol is informed.[122] As much of this information as possible must be collected discreetly during routine activities carried out by its national competent authorities without making the person in question aware of the existence of the alert.[123] Finally, the issuing Member State must review the need to maintain the information alert after retention for one year. Following a thorough individual assessment, the information alert can be kept longer than the review period.

In essence, the Regulation establishes a mechanism whereby Europol supports the Member States in the processing of third-country information they should enter into the SIS, with subsequent reporting to Europol regarding any action taken.[124] Member States remain in the driving seat, thus curbing at least some concerns regarding the tipping of the balance between the Member States' and the agency's powers, as well as the nature of the SIS as a reporting system supporting national authorities. The information alerts are closely connected to alerts on discreet/inquiry and specific checks in terms of the process followed – with the exception, of course, being that the registration process takes place in accordance with EU rules, not national law.

However, a number of data protection challenges remain, arguably questioning the proportionality of these alerts. Some challenges relate to the path dependency with the alerts inserted under Article 36; as the latter is criticised for its vague wording regarding the conditions for entering these alerts, the same challenges apply to this case as well. Furthermore, the extent to which the collection of the information in the third country would be effectively checked by Europol is doubtful. As mentioned in Recital 8 of Regulation (EU) 2022/1190, Europol must transmit all available information on the case "except for information which has clearly been obtained in obvious violation of human rights". Thus, the first quality check to be conducted by Europol does not seem to very substantial, as the threshold is rather low. Another related issue is which criteria Europol will employ to determine to which Member State to submit the proposal for entering the information alert. The Regulation is silent on this matter, which may lead to essentially asking the Member States with a track record of *en masse* registration on the basis of a flexible interpretation of the conditions for entering alerts, or ask several Member States, which is possible, until finding one willing to do so. In any case, even if Member States have restrictions under national law, such as the need to establish a link to national jurisdiction, information alerts bypass that restriction by elevating the case to a European one – hence their nature as alerts in the interest of the Union. The 'need to know' principle is thus transplanted from its traditional law enforcement context and its European contours to the international area, and the SIS morphs from a Schengen-wide reporting system to a globalised reporting system.

Member States will have the difficult task to analyse the information provided and decide with full discretion whether to record an information alert – all this notwithstanding the fact that, as acknowledged in the explanatory memorandum attached to the proposal for information alerts, Member States may not have the means to sufficiently analyse and verify the received information and they may simply have to trust Europol, or limit themselves to a basic evaluation.[125] This is perhaps why a 12-month period for analysing the information is provided; the long processing period may arguably be interpreted as further evidence that Europol's quality check will not offer much, and that, in any event, those cases, despite concerning public and national security, are not that urgent. The rigorousness of the quality check conducted by Member States may also be

122. Ibid art 37b(2) and art 48(8)(b).
123. Ibid art 37b(4).
124. Council Document 7732/21 (n 100).
125. Commission, Proposal for information alerts (n 88) 2.

insufficient: the case of uneven operationalisation of alerts on discreet checks is testament to the difficulties in ensuring a meaningful proportionality assessment of each individual case. It may even depend on the bilateral relations of the Member State with the third country. Similarly, the extent to which the alerts will be deleted after a year is also questionable. Regrettably, another existing information gap concerns the review and deletion of alerts, therefore it is difficult to predict for how long these alerts will be stored. If there is any indication from the steadily increasing number of Article 36 alerts, it is highly likely that the alert – and therefore the surveillance activities they entail in the form of monitoring of individuals' movement and connections – will arguably be longlasting, with significant implications on individuals whose mobility may be restricted or who may be implicated in other surveillance practices or become subject to criminal investigations.

At the heart of the data protection concerns relating to the incorporation of international lists on FTFs and other suspected perpetrators of terrorism and serious crimes lies the reliability of the data and the accuracy of the information, in line with the data accuracy principle of data protection law. Adding to the concerns mentioned in the previous section, internalising information from third countries which do not have an adequate data protection framework compared to that of the EU could signify that these alerts may contain unlawfully acquired information or be unreliable, for example, as mentioned earlier, where individuals are put on these lists for political purposes. This is particularly the case with information obtained from Interpol, which has been heavily criticised about the abuse of its notices by states with oppressive regimes.[126] Even though Interpol does not publish information about how many red notices it rejects, there is no doubt that certain states abuse Interpol's Notice System to persecute national human rights defenders, civil society activists and critical journalists in violation of international standards of human rights.[127] In other words, information alerts risk integrating, validating and legitimising an approach of 'garbage (unreliable data) in – garbage (unlawful surveillance) out' or a process of data laundering and legitimisation through their insertion in the SIS, the reliability of which may be undermined.

On a positive note, if Europol acquires additional information, it would be possible to amend or delete the relevant alerts, even though this is arguably difficult to operationalise due to lack of resources to follow up and keep track of all these alerts.[128] Ultimately, considering that the alerts concern secret surveillance and thus it will be very difficult to realise they are under surveillance, the heavy burden is placed on the supervision of the operationalisation of these alerts. This involves both supervision by national supervisory authorities, under which the supervision of the SIS falls, and the European Data Protection Supervisor (EDPS), responsible for Europol's supervision. This supervision must take place on many different instances: the initial check by Europol, including the potential exchanges with the third party, the verification and analysis process by the Member States, the review of the alert on a yearly basis, and the fate of the data within Europol after the insertion or non-insertion of the alert. Considering the limited resources of national data protection authorities, this seems a Herculean task.[129]

126. For further information see Rasmus H Wandall and others 'Misuse of Interpol's Red Notices and impact on human rights – recent developments' (Study requested by the European Parliament Research Service 2019); Hearing before the Commission on Security and Cooperation in Europe (12 September 2019) https://www.govinfo.gov/content/pkg/CHRG-116hhrg37829/html/CHRG-116hhrg37829.htm accessed 31 January 2023.
127. Ibid.
128. This was added at the behest of the European Parliament.
129. For further information on multi-level supervision in the case of information alerts see Sarah Tas, 'The Case of 'Information Alerts' in the Schengen Information System (SIS): A Dangerous and 'Unsupervised' Extension of Europol's Powers' European Papers (European Papers, forthcoming 2023).

From the perspective of operational value, information alerts will internalise information coming from third countries on third-country nationals who may have no relevance to the EU on the presumption that the person concerned may at some point in the future cross the EU's external borders. As such, the remoteness of the link with the EU may mean that the alert may never have a hit.

Importantly, a bird's eye view into the procedure raises further concerns regarding the actual necessity of creating this new category of alert. The purpose of entering these alerts is that all suspected terrorists – both European and non-European – are detected if they *try to cross EU borders*, and that action is taken upon receipt of the identities of suspected terrorists. Thus, the aim of these alerts is to make verified information provided by a third party available to front-line officers in Member States, in particular *border guards*. This brings to the forefront questions about the ability to use other EU large-scale information systems processing personal data of different groups of third-country nationals to perform the same task, thus making the registration of these alerts redundant; of particular relevance are the European Travel Information and Authorisation System (ETIAS)[130] and the Visa Information System (VIS).[131] The first concerns the pre-checking of visa-free nationals who wish to travel to the Schengen area, whereas the second one concerns visa-requiring third-country nationals. While the ETIAS is currently under development, aiming to become operational in 2023, the VIS is already operational but is currently undergoing technical amendments. In both cases, applicants' data must be automatically cross-checked against other EU databases, *including Europol data and a dedicated ETIAS watchlist*[132] developed by the agency which will contain data related to persons who are suspected of having committed or taken part in a terrorist offence or other serious criminal offence, or persons regarding whom there are factual indications or reasonable grounds, based on an overall assessment of the person, to believe that they will commit a terrorist offence or other serious criminal offence. The almost identical wording raises concerns as to how the different tools will operate in practice, when presumably the same information acquired by the agency will also feed into the Europol databases and the forthcoming ETIAS watchlist.

To illustrate the issue: for example, a third-country national suspected of terrorism-related activity aiming to cross the EU's external borders would have to apply for either a visa or a travel authorisation, therefore their data would be cross-checked against both the Europol database and the ETIAS watchlist, and a hit would draw the attention of the national authorities examining their application, which will have to manually process their application in consultation with Europol. This means that, irrespective of the existence of the SIS alert, the individual's data would in any case have a 'hit' with Europol's information. Even if an alert is not issued, it is possible that Europol will include the person's information in its ETIAS watchlist. The result would be that the individual concerned would most probably be denied a visa or a travel authorisation, thus preventing them from reaching the external borders or denying them entry if they still travel. This is unless national authorities would ask

130. Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226 [2018] OJ L236/1 (ETIAS Regulation).
131. Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) [2008] OJ L218/60, as amended by Regulation (EU) 2021/1134 of the European Parliament and of the Council of 7 July 2021 amending Regulations (EC) No 767/2008, (EC) No 810/2009, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1860, (EU) 2018/1861, (EU) 2019/817 and (EU) 2019/1896 of the European Parliament and of the Council and repealing Council Decisions 2004/512/EC and 2008/633/JHA, for the purpose of reforming the Visa Information System [2021] OJ L248/11 (VIS Regulation).
132. ETIAS Regulation, art 20 and art 34; VIS Regulation, art 9a.

for an interview and thereupon execute the information alert (if any) by questioning the person. If the person is granted authorisation, this could either mean that, after manual processing,the information proved insufficient to deny the visa or the travel authorisation, or that there is interest in nonetheless allowing the person to travel (for example to be questioned). Of course, allowing the entry of a person suspected of terrorism would create internal security concerns. The only possible way that information alerts could be useful is in cases where a third-country national enters irregularly (it is unlikely that the person would still appear at the border crossing point without an authorisation or a visa) and interact with a national authority on its territory, in which case it is unclear as to whether law enforcement authorities or intelligence services might have already entered an alert in the SIS on the basis of their own intelligence prior to the person's entry.

The above analysis aims to demonstrate that even without the creation of this new type of alert, there are other mechanisms in place, which will soon become operational, whereby Europol data will directly block the entry of individuals based on its information. Those mechanisms may provide some information, which is not the same as the information mandated for collection under Article 37b, but if these mechanisms work properly this means that the person may never reach the external borders in order for the information alert to be executed. If the individual would still be found on national territory, then these alerts would primarily serve Europol – in which case, the detection of a suspected person would be delegated to national law enforcement authorities – and the Member States. However, considering the cumbersome process, it is likely that these alerts will remain underutilised in the future. If there is one lesson learnt from the first case on discreet alerts, it is that underutilised functions result in efforts to make more use of them and in safeguards being watered down. So, ultimately, the aim of these alerts may be to function as a 'Trojan horse', and create a backdoor for Europol to take on a more influential role in the operation of the SIS, whereupon, in the near future, the lack of effectiveness of alerts and, potentially, a new wave of security concerns would dictate revisions to expanding the scope of alerts to EU FTFs or allowing the agency's role to propose the issuance of other types of alerts. Perhaps Eurojust may desire to be able to propose alerts on EAWs. As Europol progressively acquired access to all categories of alerts by following a 'salami approach', the history may repeat itself.

What happens until the revised SIS rules come into force?

The implementation of the new SIS rules on alerts in the interest of the Union requires the establishment of legal, technical and procedural prerequisites, namely to adopt amendments to the SIRENE Manual, to make technical changes to the system, and to have new procedures put in place, which should be defined by Europol. While waiting for the new SIS rules to enter into force, the coordinated approach on entering lists of suspected non-EU FTFs transmitted to Europol into the system, adopted in November 2020, applied until its revision in February 2023. The revision is meant to enable alignment of the process with the new legislation and on the basis of past experience by: adding deadlines for the different steps; ensuring sufficient reporting of the outcome of the verification of the data; including the Schengen associated countries; replacing the phrase 'third countries' with the broader wording 'third parties' to allow for information received, for instance, from international organisations, in particular Interpol; and enlarging the scope from FTFs to third-country nationals with suspected links to terrorism – but not to suspects of serious crimes as per Regulation (EU) 2022/1190).[133]

133. Council, Document 5153/2/23 (7 February 2023).

Concluding remarks

The aim of this article was to map and critically evaluate the reforms, whether embedded in legislation or informal, to the SIS legal framework in order to address the phenomenon of FTFs. The article demonstrated the political impetus for increased use of the existing capabilities of the SIS, capitalising on the system's ability to facilitate secret surveillance on individuals and its flexible nature. This has resulted in a stark increase in the number of alerts on discreet and specific checks due to the vague wording of the relevant SIS provisions and the overzealous approach of certain Member States. This uneven implementation has raised concerns about misuse of the system, which have not been addressed, as evidenced by the Schengen Evaluation and Monitoring Mechanism and the continuing increased number of the alerts. The effectiveness of these alerts in addressing the phenomenon of FTFs is also not particularly clear.

The article further examined the aspirations to make the SIS a global reporting system by internalising and legitimising information from third countries and international organisations on third-country nationals suspected of terrorism and other serious crimes. Despite its wider scope, the reform of the SIS to allow the insertion of alerts in the interest of the Union was clearly sparked by concerns regarding the FTF phenomenon, coupled with an interest in exploiting information received by Europol from outside the EU. The latter is the EU's powerful information hub receiving information from different types of partners worldwide, including third countries with dubious data protection regimes and international organisations. Thus, the potential internalisation of lists of potential FTFs raises concerns about potential abuse of the SIS, this time through Europol. In the fight against terrorism and particularly in order to address concerns regarding FTFs, the SIS risks laundering international data translated into actionable alerts, thus marking a new era for Europol, which exerts increasing influence on Member States and is placed on more equal footing as regards the operation of the system. Whether it is appropriate to treat lists on FTFs from third countries or international organisations the same way as lists of individuals suspected of terrorist-related activity is highly doubtful. Overall, the article has highlighted a series of concerns regarding the proportionality of these alerts from a data protection perspective and potential operational value, despite the Member States remaining in the driver's seat.

The story of the SIS ultimately demonstrates that it will continue to remain in the spotlight as a cure-all to address counter-terrorism concerns, and that the objective of fighting terrorism motivates the EU legislature to propose far-reaching and highly intrusive rules. These rules give rise to risks concerning the reliability of the alerts and the system as a whole, which may suffer from poor data quality. The insertion of alerts results in suspected FTFs being subject to covert surveillance, which is increasingly difficult to detect and consequently to contest. This impact on individuals affected may be particularly long-lasting, considering that the alerts are renewable; given the stakes of counter-terrorism, it is expected that national authorities may have limited incentive to delete them following review. Furthermore, it will not be surprising if Europol (or other agencies, such as Eurojust or the EBCG Agency) is allowed to enter alerts – ultimately, the name of these alerts 'in the interest of the Union' seems to suggest that this is just the beginning. It is also expected that these alerts will be expanded to EU nationals; after all, it is well known that, at the EU level, a number of controversial technologies or practices are first tested on third-country nationals before their more widespread application.[134] The forthcoming interoperability of large-scale IT systems for third-country nationals, whereby these alerts will become interconnected with millions of records from other information systems, may have additional implications, potentially blocking individuals' mobility based on poor

134. Vavoula, *Immigration and Privacy in the Law of the European Union* (n 6) 5.

data quality and registration in the system on the basis of vague criteria. It is high time that more statistical information on the insertion, retention and deletion of SIS alerts becomes publicly available, that supervisory authorities draw their attention to these matters and conduct effective supervision in coordination with the EDPS, and that the EU legislature considers establishing clear criteria for the insertion of alerts, without, however, resorting to a 'race to the bottom' approach.

Author's note

Senior Lecturer (Associate Professor) in Migration and Security, Queen Mary University of London. Section 4.2 is partly based on Niovi Vavoula, 'The EU Response to the Phenomenon of Foreign Fighters: Challenges for Fundamental Rights and the Rule of Law' in Ulrich Sieber et al. (eds), *Alternative, Informal, and Transitional Types of Criminal Justice and the Legitimacy of New Sanction Models in the Global Risk Society* (Duncker & Humblot 2018). Sections 5.1 and 5.2 are partly based on Niovi Vavoula and Valsamis Mitsilegas, 'Strengthening Europol' (Study commissioned by the LIBE Committee of the European Parliament, 2021). The author is grateful to Sarah Tas, Teresa Quintel and the special issue editors for their comments in the drafting process. Any errors remain, of course, my own.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Niovi Vavoula https://orcid.org/0000-0001-5460-7252