



RESEARCH ARTICLE

# Politics of creep: Latent development, technology monitoring, and the evolution of the Schengen Information System

Matthias Leese<sup>1</sup>  and Vanessa Ugolini<sup>2</sup> 

<sup>1</sup>Department of Humanities, Social and Political Sciences, ETH Zurich, Zurich, Switzerland and <sup>2</sup>Law, Science, Technology and Society Research Group, Faculty of Law and Criminology, Vrije Universiteit Brussel, Brussels, Belgium

**Corresponding author:** Matthias Leese; Email: [mleese@ethz.ch](mailto:mleese@ethz.ch)

(Received 30 June 2023; revised 6 December 2023; accepted 16 January 2024)

## Abstract

The Schengen Information System for law enforcement, border control, and judicial cooperation in the European Union has over the years seen a considerable expansion of the amount and types of data stored and its functionalities, as well as its user base. In light of this transformation from a simple information-sharing tool to a full-blown investigative database, there has, however, been surprisingly little public debate and pushback against the growing surveillance and control capacities that the system enables. This article proposes to understand the largely uncontested evolution of the SIS through the concept of ‘creep’, i.e. the incremental, unforeseen, and/or stealthy development of a technological system beyond what it was originally introduced for. More specifically, it retraces how creep has in the case of the SIS been enabled and facilitated through (1) latent development principles, i.e. the rationale of building dormant features into a system that can be activated at a later point in time once technology has sufficiently matured and/or legal foundations have been adopted; and (2) technology monitoring and steering mechanisms, i.e. the continuous assessment of the readiness of key technologies for anticipated updates to the system as well as interventions in publicly funded research programmes.

**Keywords:** data; European Union; Schengen; security; technology

The Schengen Information System (SIS) for the sharing and pooling of data for law enforcement, border control, and judicial cooperation is widely regarded as a key knowledge infrastructure for European Union (EU) internal security. As such, it plays a pivotal role in how political order in the EU is imagined and enacted through the everyday work of national and EU-level authorities. Notably, the system has undergone significant transformations since the original SIS I went live in 1995. After two updates to accommodate larger numbers of participating countries (SIS I + in 2001; SISone4all in 2007) and the roll-out of a completely overhauled second-generation SIS (SIS II) in 2013, the latest upgrade to the SIS has been the SIS Recast package, which became operational in March 2023.<sup>1</sup> SIS Recast consists of three new regulations that introduce new biometric data elements and alert categories, as well as enhanced access rights to the system for EU agencies.<sup>2</sup>

<sup>1</sup>European Commission, ‘Security Union: The renewed Schengen Information System enters into operation’, Brussels, 7 March 2023, available at: [https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip\\_23\\_1505/IP\\_23\\_1505\\_EN.pdf](https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_23_1505/IP_23_1505_EN.pdf).

<sup>2</sup>European Union, ‘Regulation (EU) 2018/1860 of the European Parliament and the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals’ (Brussels: Official Journal of the European Union, 2018); European Union, ‘Regulation (EU) 2018/1861 of the European Parliament and the Council

Overall, the SIS has over the years seen a considerable expansion of the amount and types of data stored and its functionalities, as well as its user base.

While from the authorities' point of view, this expansion has been widely praised as a success story,<sup>3</sup> it has also sparked some concerns about growing technologically mediated surveillance and control capacities.<sup>4</sup> Overall, there has, however, been surprisingly little public debate and pushback against the gradual transformation of the SIS from a simple information sharing tool to a full-blown investigation database with more than 86 million entries, more than 12 million search queries per year,<sup>5</sup> and a broad user base of national and supranational authorities.

This article proposes to understand the largely uncontested evolution of the SIS through the concept of 'creep', i.e. the incremental, unforeseen, and/or stealthy development of a technological system beyond what it was originally introduced for.<sup>6</sup> More specifically, it retraces how creep has in the case of the SIS been enabled and facilitated through two interlinked strategies: (1) latent development principles, i.e. the rationale of building dormant features into a system that can be activated at a later point in time once technology has sufficiently matured and/or legal foundations have been adopted; and (2) technology monitoring and steering mechanisms, i.e. the continuous assessment of the readiness of key technologies for anticipated updates to the system as well as interventions in publicly funded research programmes.

Taken together, so the argument we put forward here, these features constitute a politics of creep that aims at the expansion of digital knowledge infrastructures in gradual and almost imperceptible ways that decrease the likelihood of contestation and pushback. The concept of creep in this context allows us to understand how the expansion of the SIS in terms of data, functionalities, and user base was realised in a way that works in a seemingly banal and unspectacular fashion, thus managing to largely stay below the level of scandal and public problematisation. Our analysis thereby contributes to current debates at the intersections of International Relations, Science and Technology Studies, and Critical Security Studies that have highlighted the role of information infrastructures in contexts of governance and international security.<sup>7</sup> It does so by pointing to the dynamic nature of infrastructures that are otherwise usually considered as more or less fixed and stable, and to the politics involved in setting up such dynamics in ways that are geared towards suppressing public awareness and debate.

The paper proceeds as follows. It first engages literature that has analysed the role of the SIS and other security-related databases in changing modes of governance and regulation. It then discusses

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' (Brussels: Official Journal of the European Union, 2018); European Union, 'Regulation (EU) 2018/1862 of the European Parliament and 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' (Brussels: Official Journal of the European Union, 2018).

<sup>3</sup>European Commission, 'Schengen Information System', available at: [https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system\\_en](https://ec.europa.eu/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system_en).

<sup>4</sup>Ben Hayes, 'Statewatch analysis: From the Schengen Information System to SIS II and the Visa Information System (VIS): The proposals explained' (London: Statewatch, 2004); Ben Hayes, 'SIS II: *Fait accompli*? Construction of EU's Big Brother Database underway. Statewatch analysis' (London: Statewatch, 2005); Didier Bigo and Sergio Carrera, 'From New York to Madrid: Technology as the ultra-solution to the permanent state of fear and emergency in the EU. CEPS commentary' (Brussels: Centre for European Policy Studies, 2004).

<sup>5</sup>eu-LISA, 'SIS II 2021 annual statistics' (Strasbourg: European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, 2022).

<sup>6</sup>Bert-Jaap Koops, 'The concept of function creep', *Law, Innovation and Technology*, 13:1 (2021), pp. 29–56.

<sup>7</sup>See for instance Georgios Glouftsiou, *Engineering Digitised Borders: Designing and Managing the Visa Information System* (Basingstoke: Palgrave Macmillan, 2021); Matthias Leese, 'Fixing state vision: Interoperability, biometrics, and identity management in the EU', *Geopolitics*, 27:1 (2022), pp. 113–33; Rocco Bellanova and Georgios Glouftsiou, 'Formatting European security integration through database interoperability', *European Security*, 31:3 (2022), pp. 454–74; Paul Trauttmansdorff, 'Borders, migration, and technology in the age of security: Intervening with STS', *Tecnoscienza: Italian Journal of Science & Technology Studies*, 13:2 (2022), pp. 133–54.

the SIS and its evolution and introduces the notion of creep and its analytical benefits for understanding the gradual transformation of the SIS. Eventually, the empirical analysis shows how creep was in the case of the SIS enabled through latent development principles that set up the system for future flexibility and technology monitoring and steering mechanisms that have emerged as a concrete way to realise anticipated expansions in the future. The article concludes by spelling out the agenda-setting capacities of political actors in complex socio-technical systems and highlights the potential for public visibility and debate to contest a politics of creep.

### Methodological note

The argument presented here builds on an extensive document analysis that covers political, legislative, and technological aspects relating to the SIS between 1995 and 2023. Documents are a valuable analytical resource, as their contents have been recorded and consolidated independent of the intervention of a researcher and can be understood as socio-political facts that are produced, shared, and used in organised ways. Overall, more than 90 public-domain documents – including directives, regulations, feasibility studies, progress reports, activity reports, minutes, evaluations, and opinions – pertaining to the policy process, development, and design aspects, as well as management and operation of the SIS, were retrieved and analysed. The aim was to compile an exhaustive collection of available documentation that allows for an in-depth reconstruction of the interlinked political and technical development of the SIS. The resulting corpus of documents was analysed using qualitative content analysis methods, i.e. software assisted *in vivo* coding that allowed us to break down content into thematic parts and re-aggregate it in a cross-cutting fashion. For the analysis presented here, the code structure was used to analytically reconstruct political prioritisations and their socio-technical realisation and implementation, yielding insights into how the SIS was set up in a way to facilitate creep during its development and design phase and beyond.

### Databases and the governance of mobility and security

There is a broad and multidisciplinary body of literature that has empirically and conceptually investigated the role of centralised databases as knowledge infrastructures for the governance of mobility and security in Europe and elsewhere. While it is not possible to engage with this literature in its entirety here, in the following we discuss those analyses that are most pertinent in the context of the SIS.

Maybe most importantly, scholars have highlighted how the SIS and other databases (such as for example the Visa Information System or Eurodac) have reshaped how mobility and security are rendered knowable and governable in the EU.<sup>8</sup> Scheel et al. have, for example, shown how data are mobilised to produce knowledge on migration and enable novel biopolitical modes of governing.<sup>9</sup> Similarly, Pelizza has analysed how registration and enrolment practices in EU databases constitute identities and politics.<sup>10</sup> And Amelung et al. have highlighted how the exchange of forensic DNA data has come to establish a new type of hidden, differentiated borders within the Schengen area.<sup>11</sup>

<sup>8</sup>E.g. Rocco Bellanova and Denis Duez, 'A different view on the "making" of European security: The EU passenger name record system as a socio-technical assemblage', *European Foreign Affairs Review*, 17:2/1 (2012), pp. 109–124; Huub Dijkstra and Dennis Broeders, 'Border surveillance, mobility management and the shaping of non-publics in Europe', *European Journal of Social Theory* 18:1 (2015), pp. 21–38; Julien Jeandesboz, 'Smartening border security in the European Union: An associational inquiry', *Security Dialogue*, 47:4 (2016), pp. 292–309.

<sup>9</sup>Stephan Scheel, Evelyn Ruppert, and Funda Ustek-Spilda, 'Enacting migration through data practices', *Environment and Planning D: Society and Space*, 37:4 (2019), pp. 579–88.

<sup>10</sup>Annalisa Pelizza, 'Processing alterity, enacting Europe: Migrant registration and identification as co-construction of individuals and politics', *Science, Technology, & Human Values*, 45:2 (2020), pp. 262–88.

<sup>11</sup>Nina Amelung, Rafaela Granja, and Helena Machado, *Modes of Bio-bordering: The Hidden (Dis)integration of Europe* (Basingstoke: Palgrave Macmillan, 2021).

Other studies have shown how the unprecedented amount of data stored and circulated in the SIS and other digital infrastructures potentially gives way to new forms of data-driven profiling and social sorting.<sup>12</sup> This work starts from the assumption that digital and networked databases can be used as control apparatuses that monitor, evaluate, and sort mobile populations. In doing so, it particularly focuses on issues concerning surveillance and privacy along with other ethical and legal issues that the generation and use of data engender. Moreover, scholars have pointed out how the addition of biometric data and algorithmic biometric-matching capacities to the SIS and other databases has furthered surveillance and control capacities through novel modes of identifying individuals,<sup>13</sup> especially since in light of recent efforts to render databases interoperable, these tendencies are likely to be aggravated.<sup>14</sup> Finally, scholars have explored how new ways of governing the Schengen area have at the same time generated a push for the collection of more and new types of data.<sup>15</sup>

At the policy level, analyses of the SIS and other databases reflect the larger trajectory towards anticipatory forms of regulation that seek to preempt the occurrence of unwanted events by means of risk analysis and preventive interventions,<sup>16</sup> especially under the moniker of Big Data analytics.<sup>17</sup> Specifically in regard to the SIS, scholars have analysed the actor constellations and power dynamics that have coined the policy processes that have established the legal bases for SIS I and II – and how such policy processes have additionally become tangled up in multiple reforms of the EU and its institutions.<sup>18</sup>

Whereas this literature puts emphasis on the historical political conditions under which the construction of the SIS became possible (and massively delayed) in the first place, it has somewhat neglected the question of how political priorities became translated into technical development and design choices. In other words, while the SIS is often used as an example in governance- and policy-focused analyses, there is, however, surprisingly little research that engages the system directly. Specific attention to the SIS has predominantly come from legal scholars who have analysed the

<sup>12</sup>E.g. Louise Amoore, 'Data derivatives: On the emergence of a security risk calculus for our times,' *Theory, Culture & Society*, 28:6 (2011), pp. 24–43; Dennis Broeders and James Hampshire, 'Dreaming of seamless borders: ICTs and the pre-emptive governance of mobility in Europe,' *Journal of Ethnic and Migration Studies*, 39:8 (2013), pp. 1201–18; Matthias Leese, 'The new profiling: Algorithms, black boxes, and the failure of anti-discriminatory safeguards in the European Union,' *Security Dialogue*, 45:5 (2014), pp. 494–511.

<sup>13</sup>E.g. Irma van der Ploeg and Isolde Sprenkels, 'Migration and the machine-readable body: Identification and biometrics,' in Huub Dijkstra and Albert Meijer (eds), *Migration and the New Technological Borders of Europe* (Basingstoke: Palgrave Macmillan, 2011), pp. 68–104; Btihaj Ajana, 'Asylum, identity management and biometric control,' *Journal of Refugee Studies*, 26:4 (2013), pp. 576–95; Charlotte Epstein, 'Embodying risk: Using biometrics to protect the borders,' in Louise Amoore and Marieke de Goede (eds), *Risk and the War on Terror* (London: Routledge, 2008), pp. 178–93.

<sup>14</sup>E.g. Bellanova and Glouftis, 'Formatting European security integration'; Leese, 'Fixing state vision'; Didier Bigo, 'Interoperability: A political technology for the datafication of the field of EU internal security?', in Didier Bigo, Thomas Diez, Evangelos Evangelos, Ben Rosamond, and Yannis A. Stivachtis (eds), *The Routledge Handbook of Critical European Studies* (London: Routledge, 2021), pp. 400–417.

<sup>15</sup>E.g. Huub Dijkstra, Rogier van Reekum, and Willem Schinkel, 'Surveillance at sea: The transactional politics of border control in the Aegean,' *Security Dialogue*, 48:3 (2017), pp. 224–40; Georgios Glouftis, 'Governing circulation through technology within EU border security practice-networks,' *Mobilities*, 13:2 (2018), pp. 185–99.

<sup>16</sup>E.g. Louise Amoore and Marieke de Goede, 'Governance, risk and dataveillance in the war on terror,' *Crime, Law and Social Change*, 43:2 (2005), pp. 149–73; Claudia Aradau and Rens van Munster, 'Governing terrorism through risk: Taking precautions, (Un)knowing the future,' *European Journal of International Relations*, 13:1 (2007), pp. 89–115; Leese, 'The new profiling.'

<sup>17</sup>E.g. José van Dijk, 'Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology,' *Surveillance & Society*, 12:2 (2014), pp. 197–208; Claudia Aradau and Tobias Blanke, 'Politics of prediction: Security and the time/space of governmentality in the age of Big Data,' *European Journal of Social Theory*, 20:3 (2017), pp. 373–91; Dennis Broeders, Erik Schrijvers, Bart van der Sloot, Rosamunde van Brakel, Josta de Hoog, and Ernst Hirsch Ballin, 'Big Data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data,' *Computer Law & Security Review*, 33:3 (2017), pp. 309–23.

<sup>18</sup>E.g. Bigo and Carrera, 'From New York to Madrid'; Hayes, 'Statewatch analysis'; Hayes, 'SIS II: *Fait accompli*?'; Joanna Parkin, 'The difficult road to the Schengen Information System II: The legacy of "laboratories" and the cost for fundamental rights and the rule of Law. CEPS Papers in LIBERTY and SECURITY in Europe' (2011).

impact of information sharing on data protection<sup>19</sup> and civil liberties.<sup>20</sup> The most pertinent work is thereby arguably Brouwer's study on the effects of the SIS on the rights of third-country citizens, and more specifically the possible remedies for individuals registered in the system.<sup>21</sup> By placing the SIS within the intersecting legal frameworks of the EU itself, data protection, human rights, and migration, she concludes that the capacities of the SIS 'entail a risk to the protection of human rights such as the right to privacy and the right to data protection, but also the freedom of movement of persons and the principle of non-discrimination.'<sup>22</sup>

In summary, despite the academic attention that databases for the regulation of mobility and security have garnered, the SIS itself surprisingly remains somewhat understudied. This diagnosis does fall in line with the argument that we put forward here: that the SIS has over the years expanded in a creeping fashion that has largely remained below the level of exception and scandal – and has therefore garnered comparatively little attention. This stands in stark contrast to the capacities of the system and its key role in regulating the Schengen area. The next section introduces the SIS and its evolution in more depth to illustrate its significance.

### The Schengen Information System and its evolution

The SIS has historically played a pivotal role in the establishment of the Schengen area as a political space that is characterised by a communalised approach to the regulation of mobility and security. When five European states (Belgium, France, Germany, Luxembourg, and the Netherlands) decided to abolish internal border controls by signing the Schengen agreement in 1985, this was only considered possible on the condition that there would be compensation for the elimination of security work carried out at state borders. Such compensation was created in the form of harmonised control practices at the new common external border, a common visa policy, and notably the SIS.<sup>23</sup> The latter was seen as the key element for practical cooperation between the authorities of the involved states through information exchange.

The rationale of the SIS is a simple yet compelling one: rather than having multiple national authorities carry out the same knowledge-production and control tasks for the regulation of mobility and security, information on border crossers, criminal activities, missing persons, stolen goods, etc. is pooled in a centralised database and made available for authorities from each member state.<sup>24</sup> From an architectural point of view, the SIS consists of a central database (C-SIS) and national databases in each of the Schengen countries (N-SIS). National systems are connected to the central database and are used to directly enter, update, delete, and query data stored in the central

<sup>19</sup>E.g. Izabella Majcher, 'The Schengen-wide entry ban: How are non-citizens' personal data protected?', *Journal of Ethnic and Migration Studies*, 48:8 (2022), pp. 1944–60; Stephen Kabera Karanja, *Transparency and Proportionality in the Schengen Information System and Border Control Co-operation* (Leiden: Martinus Nijhoff Publishers, 2008); Elisa Orrù, 'The Schengen Information System and data retention: On surveillance, security and legitimacy in the European Union', in Elisa Orrù, Maria Grazia Porcedda, and Sebastian Weydner-Volkman (eds), *Rethinking Surveillance and Control: Beyond the 'Security versus Privacy' Debate* (Baden-Baden: Nomos, 2017), pp. 115–136.

<sup>20</sup>E.g. Katina Michael and M. G. Michael, 'Schengen Information System II: The balance between civil liberties, security and justice', in Katina Michael and M. G. Michael (eds), *Australia and the New Technologies: Evidence Based Policy in Public Administration* (Wollongong: University of Wollongong, 2008), pp. 247–258; Michiel Besters and Frans Brom, '“Greedy” information technology: The digitalization of the European migration policy', *European Journal of Migration and Law*, 12:4 (2010), pp. 455–70; Sergio Carrera, 'What does free movement mean in theory and practice in an enlarged EU?', *European Law Journal*, 11:6 (2005), pp. 699–721.

<sup>21</sup>Evelien Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System* (Leiden: Martinus Nijhoff Publishers, 2008).

<sup>22</sup>Brouwer, *Digital Borders and Real Rights*, p. 534.

<sup>23</sup>Official Journal of the European Communities, '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. 22 September' (Brussels, 1990).

<sup>24</sup>Official Journal of the European Communities, 'Convention implementing the Schengen Agreement of 14 June 1985', title IV.



database through national interfaces. In that way, authorities from one country are able to access and act upon information produced by authorities from another country and vice versa.

To do this, the SIS features a broad range of information categories that are considered relevant for law enforcement, border control, and judicial matters. These so-called alerts are: (1) information on the stay of third-country nationals; (2) information on refusal of entry for third-country nationals; (3) information on return decisions for third-country nationals illegally residing within the Schengen area; (4) arrest warrants; (5) alerts on missing persons; (6) alerts on unknown persons based on fingerprints that were found at crime scenes; (7) alerts on persons who are supposed to facilitate in judicial procedures (for instance to appear in court as witnesses); (8) alerts on persons and objects for checks (either discreet or specific); (9) alerts on persons and objects that are to be checked for further inquiry; (10) information on false documents; (11) alerts on objects for seizure or for use as evidence; and (12) alerts on children who might be at risk of abduction or potential victims of terrorism, trafficking in human beings, gender-based violence, or armed conflict/hostilities.<sup>25</sup>

The data that are stored in the SIS to support these alerts are (1) data for the identification of persons and objects that are the subject of an alert, including photographs and fingerprints when available; (2) facial images, fingerprints, palm prints, fingermarks, and palm marks for biometric identification; (3) DNA profiles of missing persons; as well as (4) links between alerts and (5) information on what course of action should be taken once a person or an object under alert has been encountered.<sup>26</sup> Search queries can be run either based on alphanumeric data (e.g. names, passport numbers, licence plates) or on biometric data. When a query produces a match in the system, national authorities can access the information stored on that specific alert and receive instructions on the action to be undertaken (e.g. take a person into custody, notify a person that they are wanted for judicial assistance, or seize an object or travel document).

While the present iteration of the SIS is considered the most pertinent and powerful European database for the regulation of mobility and security,<sup>27</sup> the system has come a long and at times heavily contested way from its original version.<sup>28</sup> Its evolution can be characterised by expansion in regard to three main dimensions: (1) the amount and types of data stored; (2) upgraded system functionalities; and (3) access rights for new user groups. An important caesura has in this sense been constituted by the jump from the original SIS I, which went live in 1995, to its successor, the completely redesigned SIS II, which only went live in 2013 with considerable delay after it had been politically agreed upon already in 2001.<sup>29</sup>

When it eventually became operational, the SIS II realised a series of novel features that set it apart from the SIS I and which have since been further developed and complemented. The most prominent novelties pertained to the inclusion of new alert categories and new types of data, most notably biometric data (fingerprints and photographs) and with that the possibility of running search queries based on biometrics; the possibility of creating links between different alerts in the system (e.g. to link an alert on a person to an alert on a stolen identity document or a vehicle);

<sup>25</sup>European Commission, 'The Schengen Information System factsheet' (2018), available at: [https://ec.europa.eu/home-affairs/document/download/6cce6045-79d5-4ace-ad09-230e3290f765\\_en](https://ec.europa.eu/home-affairs/document/download/6cce6045-79d5-4ace-ad09-230e3290f765_en); European Commission, 'The renewed Schengen Information System enters into operation: SIS Factsheet (7 March 2023)', available at: <https://ec.europa.eu/commission/presscorner/api/files/attachment/874647/SIS%20factsheet.pdf.pdf>.

<sup>26</sup>European Commission, 'Schengen Information System factsheet'; European Commission, 'Renewed Schengen Information System'.

<sup>27</sup>Rocco Bellanova and Georgios Glouftsiou, 'Controlling the Schengen Information System (SIS II): The infrastructural politics of fragility and maintenance', *Geopolitics*, 27:1 (2020), pp. 160–84.

<sup>28</sup>Parkin, 'The difficult road to the Schengen Information System II'.

<sup>29</sup>European Commission, 'COM(2001) 720 final: Development of the Schengen Information System II. 18 December' (Brussels, 2001); Parkin, 'The difficult road to the Schengen Information System II'; for a detailed overview of the political process and the reasons/nature of the delay, see European Court of Auditors, 'Lessons from the European Commission's development of the second generation Schengen Information System (SIS II)' (Luxembourg: Publications Office of the European Union, 2014).

and a considerably expanded user base of both European and national-level authorities that have access to the system (e.g. Europol, Eurojust, national prosecutors, vehicle licensing authorities).

The latest update of the SIS in the form of the SIS Recast package<sup>30</sup> has added further alert categories (alerts on non-EU nationals subject to a return decision; unknown wanted persons to identify suspects of serious crimes and terrorism; preventive alerts on children and vulnerable adults at risk of abduction; and people and objects for inquiry checks) and extended access and/or modification rights for existing and new users (full access rights for immigration authorities, boat and aircraft registration authorities, services responsible for registering firearms, and the European Border and Coast Guard Agency when conducting operations in support of member states, as well as Europol and Eurojust rights to issue alerts directly in the system).

Taken together, these changes raise the question how to understand and theorise the dynamic nature of a key knowledge infrastructure for the regulation of mobility and security in Europe. How, in other words, has such substantial expansion of size and scope of the SIS been possible without significant pushback against the increasing surveillance and control capacities for state authorities that come with it?

### Databases as ‘creepy’ systems

To understand how the SIS has evolved from its beginnings as a simple tool for information exchange between national-level authorities to the full-fledged supranational identification and investigation tool that it is today, we propose to turn to the notion of ‘creep’. Literally meaning to move closely to the ground, to move quietly or stealthily, or to advance by imperceptible degrees,<sup>31</sup> in the literature the term has been used to describe the expansion of (mostly) technological systems beyond their original intent. Generally speaking, the idea of creep expresses concern or warnings against the expansion of the functionality of technical systems,<sup>32</sup> surveillance capacities,<sup>33</sup> control capabilities,<sup>34</sup> or policy goals.<sup>35</sup>

Authors have paired the notion of creep with a multiplicity of different concepts, resulting in terminological variety that includes the likes of function creep, scope creep, feature creep, mission creep, competence creep, authority creep, regulation creep, interest creep, surveillance creep, or control creep.<sup>36</sup> Wisman has, for example, used the terms function creep and purpose creep in relation to the tendency to repurpose data in ways that differ from the initial intent underpinning their collection.<sup>37</sup> And Reidenberg has put forward the term data creep to describe how personal data are processed in varying contexts based on their portability.<sup>38</sup> A common denominator in most

<sup>30</sup>European Union, ‘Regulation (EU) 2018/1860 of the European Parliament and the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals’; European Union, ‘Regulation (EU) 2018/1861 of the European Parliament and 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’; European Union, ‘Regulation (EU) 2018/1862 of the European Parliament and 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’.

<sup>31</sup>Koops, ‘The concept of function creep’, p. 32.

<sup>32</sup>Bruce Schneier, ‘Security and function creep’, *IEEE Security & Privacy*, 8:1 (2010), p. 88.

<sup>33</sup>Dorothy Nelkin and Lori Andrews, ‘DNA identification and surveillance creep’, *Sociology of Health & Illness*, 21:5 (1999), pp. 689–706.

<sup>34</sup>Martin Innes, ‘Control creep’, *Sociological Research Online*, 6:3 (2001), pp. 13–18.

<sup>35</sup>Tim Dekkers, ‘Technology driven crimmigration? Function creep and mission creep in Dutch migration control’, *Journal of Ethnic and Migration Studies*, 46:9 (2020), pp. 1849–64.

<sup>36</sup>Koops, ‘The concept of function creep’, pp. 39–41.

<sup>37</sup>Tijmen Wisman, ‘Purpose creep by design: Transforming the face of surveillance through the internet of things’, *European Journal of Law and Technology*, 4:2 (2013), pp. 1–15.

<sup>38</sup>Joel R. Reidenberg, ‘Resolving conflicting international data privacy rules in cyberspace’, *Stanford Law Review*, 52:5 (2000), pp. 1315–71.

of the literature on creep is the assumption that creep should be considered a wilful political move by a system's originator, i.e. a strategy to stagger expansion and thus render change more slow, gradual, and thereby less contestable.<sup>39</sup> For Koops, creep in this sense fundamentally undercuts public debate and potential resistance against change by concealing the 'tipping point' between the acceptability and non-acceptability of a technology and/or its use cases.<sup>40</sup> As he argues:

the new function is, in some sense, unacceptable (to the one speaking of function creep), but the acceptability of the change can (or could) not be discussed properly because the change is (or will be or was) not generally perceived to be controversial at the material time. Why a function expansion or shift is unacceptable (for opponents), can vary widely, from making the system ineffective or unmanageable (e.g. because of featuritis, over-complexity, or contradictory rules) to negative externalities, such as loss of human control (e.g. through self-augmentation or reverse adaptation), a legitimacy deficit (e.g. through mission creep, abuse of power, or incompatible secondary use), or lack of appropriate checks and balances (e.g. because a system expands to other domains with different norms).<sup>41</sup>

In regard to databases, the concept of creep has been primarily mobilised by scholars studying the collection and use of DNA data.<sup>42</sup> Authors have in this context pointed out how DNA samples, once produced and assembled for a particular purpose (for example a criminal investigation), are unlikely to be limited to that purpose in the future.<sup>43</sup> Rather, DNA databases are likely to be expanded to larger population groups and aggregated to support large-scale identification and surveillance schemes. Dahl and Sætнан have in this regard pointed out that resistance against the expansion of technologically mediated capacities decreases if such change occurs in a 'creepy' fashion: 'When additional functions are added to a technology slowly, people will often be less skeptical of the development than they might have been had those functions been proposed early on.'<sup>44</sup> In light of such considerations, they discuss what remedies and safeguards can be implemented to enable fair governance of DNA databases by presenting some of the expansions that have taken place in the Norwegian forensic DNA database.<sup>45</sup>

Overall, the notion of creep has been widely used by scholars to describe forms of politically prioritised and/or coincidental expansions of technologically mediated capacities, often against the backdrop of the expansion of surveillance and control capacities that come with it. Importantly, scholars have discussed how, despite their implications for power and social ordering, creepy forms of capacity expansion tend to stay below the level of exception and scandal, thus being less likely to spark public debate and potential resistance. These analyses are timely and important, yet they tend to ignore the interlinked political and technical approaches that enable creep in the first place. We thus suggest focusing on what exactly constitutes a politics of creep and how it comes into being, thereby turning attention to the socio-technical means that have facilitated the gradual evolution of the SIS over time. The remainder of this paper empirically reconstructs how, in the case of the SIS, creep has been set up through latent development principles during the design of the SIS II and how it is continually maintained through the technology monitoring and steering activities of involved actors.

<sup>39</sup>Tania Simoncelli and Barry Steinhardt, 'California's Proposition 69: A dangerous precedent for criminal DNA databases', *Journal of Law, Medicine & Ethics*, 34:2 (2006), pp. 199–213; Robin Williams and Paul Johnson, *Genetic Policing: The Use of DNA in Criminal Investigations* (Collumpton: Willan Publishing, 2008).

<sup>40</sup>Koops, 'The concept of function creep', pp. 52–3.

<sup>41</sup>Koops, 'The concept of function creep', p. 53.

<sup>42</sup>E.g. Simoncelli and Steinhardt, 'California's Proposition 69'; Williams and Johnson, *Genetic Policing*; Nelkin and Andrews, 'DNA identification and surveillance creep'.

<sup>43</sup>Nina Amelung and Matthias Wienroth, "'Crisis', control and circulation: Biometric surveillance in the policing of the "cimmigrant other", *International Journal of Police Science & Management*, 25:3 (2023), pp. 297–312.

<sup>44</sup>Johanne Yttri Dahl and Ann Rudinow Sætнан, "'It all happened so slowly": On controlling function creep in forensic DNA databases', *International Journal of Law, Crime and Justice*, 37:3 (2009), pp. 83–103 (p. 100).

<sup>45</sup>Dahl and Sætнан, "'It all happened so slowly"'.



## The politics of creep

The following analysis is divided into two time periods. The first period, marked by latent development principles, covers the time between the roll-out of the original SIS I in 1995 and the roll-out of its successor, the SIS II, in 2013. Due to the rapid expansion of the Schengen area, it had already in 1995 become apparent that the original SIS I would not be capable of supporting the expected number of member states and volumes of data. This is why, essentially at the time of the launch of the SIS I, a political process was set in motion to replace the system with a completely new SIS II, to be designed from scratch.<sup>46</sup> The period between 1995 and the roll-out of this new system in 2013 thus constitutes the space where key development and design decision for the SIS in its present form were made and implemented.

The second period is marked by the roll-out of the SIS II and goes on up to the present day. With the SIS II in place, further changes were from 2013 onwards no longer be possible in a way as radical as the break between SIS I and II. Rather, as the analysis will show, the further expansion of the SIS has since then been approached through forms of technology monitoring and steering that are geared towards catching up on earlier political visions from a technological point of view. Both periods should thereby be understood as closely interlinked, with technology monitoring and steering providing a functional extension of latent development principles into the future.

### *1995–2013: Latent development*

The period between the decision to set up a second-generation SIS II from scratch and its eventual roll-out is characterised by an overall techno-scientific strategy that can be described as ‘latent development’.<sup>47</sup> Latency in this context refers to the inclusion of dormant functionalities in a system, either in the form of interfaces for later upgrades or in the form of deactivated features that can be activated at a later point in time. As a design approach, latent development pertains to a future-oriented, pre-emptive way of setting up a technological system in a flexible fashion, such that the end product, even after implementation, can still be modified in easy and cost-effective ways. In practice, latent development thus usually means to plan beyond what is actually mandated in terms of the definition of scope, use cases, and technological components – and to ensure already the possibility for future expansion.

Politically, latent development principles were prioritised by the Council and the Commission as a way to integrate technologically mediated capacities into the SIS II that had not yet been agreed upon or even discussed. As the Council documented in its meeting conclusions from June 2003, ‘it [had] been clear from the earliest conception of SIS II that this system should be a flexible tool, that will be able to adapt to changed circumstances and fulfil, within a reasonable time and without major additional costs and efforts, user requests made during its lifecycle’.<sup>48</sup> The Commission, officially tasked with the design, development, and implementation of the system along the preferences set by the Council, added that the SIS II should:

offer a simple and manageable solution and keep down maintenance costs and changes in comparison with the current system; once set up, the IT solution should be easily adaptable to incorporate new fields or categories of data. It should also be possible to continue developing the technical solution while progressively adding new functions.<sup>49</sup>

In this vein, the Commission’s staff working paper later on clarified that ‘the system should have the flexibility to incorporate new functionalities as well as new information and rules without major

<sup>46</sup> European Union, ‘Council Regulation (EC) No 2424/2001 of 6 December 2001 on the Development of the Second Generation Schengen Information System (SIS II)’ (Brussels: Official Journal of the European Union, 2001).

<sup>47</sup> Hayes, ‘Statewatch analysis’.

<sup>48</sup> Council of the European Union, ‘C/03/150: 2514th Council Meeting, Justice and Home Affairs. Luxembourg, 5–6 June’ (2003), p. 13.

<sup>49</sup> Commission of the European Communities, ‘COM(2001) 720 final: Development of the Schengen Information System II, 18 December’ (Brussels, 2001), p. 11.

technical changes<sup>50</sup> and that ‘most of the Member States favour a solution taking into account the latest technological developments and are willing to plan modifications at national level for allowing the building up of a flexible information system which is easy to change.’<sup>51</sup>

Based on these political priorities, the SIS II feasibility study, contracted to private consultancy Deloitte, defined ‘flexibility’, ‘scalability’, and ‘extensibility’ as key requirements to make the SIS II’s design effective and future-proof.<sup>52</sup> This is important, because although the timeframe for large IT projects such as the SIS II development usually comprises multiple years, the capacity for future change was in practice taken as a mandate to specify system functionalities that would go beyond the techno-scientific and political state of play. Pertinent examples for such an approach concern preparations for future inclusion of more data, more storage-intensive types of data (images, fingerprints), the exchange of larger quantities of data in an accelerated fashion, search functionalities based on biometric templates, and access for extended user groups.<sup>53</sup>

The latent development strategy was arguably facilitated by a number of factors. First of all, the Council and the Commission were resolved not to repeat the perceived mistakes made with the SIS I, i.e. to design a system that would already be technologically outdated at the point of its roll-out. Rendering the SIS II future-proof was therefore made a political priority that could rather easily be justified in light of the experiences with the SIS I. Second, multiple delays in the establishment of the legal foundations for the SIS II provided an additional, unexpected opportunity to render the system much more powerful than originally anticipated. A complete reset of the design process was caused by the integration of the Schengen acquis into the EU legal framework in 1999, changing the legal basis and legislative procedures for law enforcement, border control, and judicial cooperation in Europe.<sup>54</sup> As a result, the legal foundations for the SIS II were only fully established in 2006/7, and this reset resulted in the availability of enhanced network capacities and technological features that had not been an option at an earlier point in time.

Finally, the latent development approach to the SIS II design was aided by the overall growth of the landscape of EU border and migration databases. The Schengen Joint Supervisory Authority (JSA) had already in 1999 foreseen that ‘information systems in Europe [would] undergo major changes’ in the following years and had argued that it would be central to ‘enable all these systems to function in harmony’.<sup>55</sup> In particular, the relationship between the SIS II and the newly mandated Visa Information System (VIS) was in this context considered crucial. Looking for possible synergy effects, the Commission actively explored the possible co-development of both systems in terms of infrastructure, software, and data.<sup>56</sup> The main argument for this approach was that functionalities in one European database should, in the best-case scenario, also be mirrored in other systems to facilitate data exchange and the effectiveness of the systems. Such interoperability was, most notably, mobilised as an argument for making the SIS II ready for the future inclusion of biometric data. Biometric data had already been agreed upon for the inclusion in the VIS, and their future integration into the SIS II was thus treated as a strong likelihood.<sup>57</sup>

<sup>50</sup> Commission of the European Communities, ‘SEC(2003) 206 final: Commission staff working paper on the development of the second generation Schengen Information System (SIS II): 2002 Progress report. 18 February’ (2003), p. 4.

<sup>51</sup> Commission of the European Communities, ‘SEC(2003) 206 final: Commission staff working paper on the development of the second generation Schengen Information System (SIS II): 2002 Progress report. 18 February’, p. 7.

<sup>52</sup> Deloitte, ‘SIS II feasibility study. Additional study: NIs at the central location’ (25 May 2003), p. 9. It should be noted at this point that, while at times seeming rather odd, it is a common practice for public sector agencies to delegate the planning and realisation of technical projects to private companies because in many cases they lack the relevant expertise and resources to do it themselves. The Commission in particular has a history of contracting out such activities to the private sector.

<sup>53</sup> Deloitte, ‘Feasibility study SIS II: Technical report’ (7 April 2003).

<sup>54</sup> Commission of the European Communities, ‘COM(2001) 720 final: Development of the Schengen Information System II, 18 December’.

<sup>55</sup> Schengen Joint Supervisory Authority, ‘Third annual activity report (March 1998–February 1999)’, p. 13.

<sup>56</sup> European Commission, ‘COM(2003) 771 final: Development of the Schengen Information System II and possible synergies with a future Visa Information System (VIS)’, 11 December (Brussels, 2003).

<sup>57</sup> Deloitte, ‘SIS II feasibility study. Additional Study: SIS–VIS synergies’, 23 May 2003, p. 10.

Unsurprisingly, the high-level treatment of the SIS II as a ‘test laboratory’<sup>58</sup> for new technologies sparked some critique. In this context, it was primarily the principle of technological flexibility and the possible future co-construction of new functionalities and new executive powers that caused concern. The Parliament called for ‘a public debate about the political objectives to be achieved with the SIS II and the nature of the SIS’ and requested a ‘clear definition of these objectives.’<sup>59</sup> Without such clarification, so the rationale, no reasonable democratic debate could be had about the appropriateness of the techno-scientific capacities of the system and their effects on the balance between executive powers and human rights/civil liberties. In the same vein, the JSA warned that without knowledge about the technical specifications of the SIS II, it would be almost impossible to evaluate the repercussions of a system ‘that would allow authorities to share information on millions of individuals for a variety of purposes – possibly using the latest technologies to process sensitive biometric data.’<sup>60</sup> Civil society organisation Statewatch even accused the Council and the Commission of outright conspiracy under the guise of technological progress, arguing that ‘by the time there is any public or “democratic” debate on the scope and function of the SIS II, the technical requirements will be in place, it will doubtless be a “waste” not to use them, and the new system will effectively be a *fait accompli*.’<sup>61</sup>

While such general critique towards latent development did not result in any major design changes, a certain amount of leverage was, however, provided by data protection legislation. Specifically, the principle of purpose limitation turned out to be a somewhat effective legal instrument to put possible future features of the SIS under oversight. Statewatch had already noted that some of the latent features, such as widened access rights and the incorporation of new types of authorities into SIS operations, would, if realised, present ‘a flagrant breach of one of the fundamental principles of data protection – that data may only be used for the purpose for which it was collected.’<sup>62</sup> The European Data Protection Supervisor (EDPS) eventually came to similar conclusions, arguing that the problem with a latent development approach would be ‘to maintain a strict purpose limitation principle for the processing of SIS II data’ in case more data and different types of data would eventually be shared among a wider user base.<sup>63</sup> Data protection arguments had also been put forward with regard to the plans to integrate biometric data into the SIS II at a later point in time.<sup>64</sup> Ultimately, the mobilisation of the data protection framework forced the Commission to explicitly acknowledge ‘the competence of the European Data Protection Supervisor to monitor the SIS II data processing carried out by the Commission and the application of the Community *acquis* relevant to this field.’<sup>65</sup>

Overall, the latent development strategy pursued by the Council and the Commission, did, however, turn out to be successful in setting up a ‘future-proof’ SIS II architecture, i.e. a system ready for upgrades, expansions, and the implementation of new functionalities at a later point in time. While latent development strategies potentially could have provided for future creep by themselves, they were arguably additionally facilitated by the extended delays during the development and design phase of the SIS II that were caused by political transitions in the late 1990s and early 2000s as well as the outlined political frictions over the scope of the system. As a result, development and design

<sup>58</sup>Schengen Joint Supervisory Authority, ‘First annual activity report (March 1995–March 1997)’, p. 3.

<sup>59</sup>European Parliament, ‘European Parliament recommendation to the Council on the second-generation Schengen Information System (SIS II)’ (Brussels: Official Journal of the European Union, 2003), C 87 E/469.

<sup>60</sup>Schengen Joint Supervisory Authority, ‘Sixth annual activity report (January 2002–December 2003)’ (2003), p. 15.

<sup>61</sup>Hayes, ‘Statewatch analysis’, p. 22.

<sup>62</sup>Hayes, ‘SIS II: *Fait accompli*’, p. 6.

<sup>63</sup>European Data Protection Supervisor, ‘Opinion of the European Data Protection Supervisor on the proposal for a Council decision on the establishment, operation and use of the second generation Schengen Information System (COM(2005) 230 final)’ (Brussels: Official Journal of the European Union, 2006), C 91/43.

<sup>64</sup>Schengen Joint Supervisory Authority, ‘Sixth annual activity report (January 2002–December 2003)’.

<sup>65</sup>European Commission, ‘COM(2005) 236 final: Proposal for a regulation of the European Parliament and of the Council on the establishment, operation and use of the Second Generation Schengen Information System (SIS II). 31 May’ (Brussels, 2005), p. 3.

could already start from a much more advanced techno-scientific basis than originally anticipated, which opened a window of opportunity that has worked in favour of implementing the SIS II in ways that would allow for easier modifications along the lines of future innovation. Specifically with regard to key anticipated future functionalities such as biometric search functions, the system was at the point of its roll-out considered to be on stand-by for the integration of new technologies as soon as they became available.

### *Since 2013: Technology monitoring and steering*

After the roll-out of the SIS II in 2013, the political approach to creep changed. With the implementation of the system architecture at both national and European level, it was clear that fundamental design changes would no longer be possible in the foreseeable future. Therefore, attention was now primarily given to the question how to best make use of the available latency going forward. To do so, involved actors turned to technology monitoring and steering mechanisms. Rather than a break from latent development principles, monitoring and steering capacities should be understood as an extension that enables the continuous integration of newly available technological upgrades even after the conclusion of the development and design phase. Technology monitoring in this context means to keep track of techno-scientific advancements, to evaluate whether and how they could contribute to the actualisation of policy goals through the continuous modification of the SIS, and to assess whether certain technologies would be 'mature' enough to be integrated into the existing system architecture. Technological steering, on the other hand, pertains to interventions into public research funding programmes, prioritising research on certain basic and applied technologies considered important for the further development of the SIS.

This strategic shift coincided with the emergence of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) as a novel actor directly involved in shaping the further evolution of the SIS. After its establishment in 2011, eu-LISA had taken over the responsibilities for the operational management of the SIS and other EU internal security databases and started to build an agenda around innovation as a key enabler of efficient security cooperation in the EU. To do so, eu-LISA 'embraces an experimental approach'<sup>66</sup> that includes the mapping and assessment of technologies that could become beneficial to the effectiveness and efficiency of large-scale information systems. As eu-LISA itself frames its mission statement in the area of innovation:

It is only by remaining fully aware of new developments and analysing their potential relevance in the context of large-scale IT systems and their usage that the Agency and its expert staff can ensure adherence to the principle that the best available technologies are always utilised.<sup>67</sup>

In the context of the SIS, technology monitoring became particularly pertinent with regard to biometrics, as the technology had come to be considered the key to unlocking an entirely new level of capacities in large-scale databases based on biometric matching and the identification of unknown persons in cross-border movements and criminal investigations.<sup>68</sup> The legal foundations of the SIS II regulation from 2006/7 had included the possibility of using the system not only for hit/no hit queries (i.e. using alphanumeric or biometric data to find out whether there is information available in the system with regard to an already known identity) but also for identification queries

<sup>66</sup>Paul Trauttmansdorff and Ulrike Felt, 'Between infrastructural experimentation and collective imagination: The digital transformation of the EU border regime', *Science, Technology, & Human Values*, 48:3 (2023), pp. 635–662 (p. 4).

<sup>67</sup>eu-LISA, 'Research and development', available at: <https://www.eulisa.europa.eu/Activities/Research-And-Development>.

<sup>68</sup>Council of the European Union, 'Council conclusions on better use of SIS and SIRENE for the exchange of information on third-country nationals refused entry. 3135th Justice and Home Affairs Council meeting, 13–14 December 2011' (Brussels: Council of the European Union, 2011).

(i.e. using biometric data, most notably fingerprints, of an unknown person to find out whether there is a match in the database, thus both establishing the identity of a person and knowledge about that person).<sup>69</sup> Such a functionality would, however, require the integration of an Automated Fingerprint Identification System (AFIS) into the SIS. While this possibility had already been anticipated in 2006 (and debated much earlier), it was only after the eventual roll-out of the SIS II in 2013 that the implementation of AFIS technology was considered a concrete option from a technological point of view. Moreover, the SIS II regulation required a scientific statement on the availability and readiness of AFIS technology to be presented to the Parliament before any action could be undertaken.<sup>70</sup>

The possibility of implementing AFIS functionalities in the SIS was, however, considered to be heavily reliant on the improvement of the biometric technology itself, notably in the form of enhanced data quality and improved success/failure rates in biometric matching processes. In 2015, eu-LISA published a report that evaluated the current state of play in biometric identification and possible use cases and implementation across different EU security and migration databases. The report made it clear that eu-LISA considered biometrics as a keystone in the further development of the SIS and intended to push the technology:

Biometric systems are powerful tools that should be leveraged to the fullest of their capabilities in large-scale IT systems where the accurate and efficient identification of persons is important going forward. eu-LISA must continue to monitor the biometrics literature and undertake research of its own on the topic. In this regard, it is particularly important that the Agency engages the biometric industry and increases interactions with operational actors worldwide so that it remains aware of the state-of-the-art and can advance current systems and implement new systems that utilise all applicable technologies to deliver quality service to all end users.<sup>71</sup>

The theme of biometrics thus effectively turned into a waiting game for the right level of technological readiness to actualise a fundamental shift in SIS capacities, i.e. the transformation from an information-sharing instrument into a full-blown investigation tool that could, for instance, be queried on the basis of fingerprints lifted from crime scenes or facial images from surveillance footage.

To do so, the Commission had already instructed the Joint Research Centre (JRC; the Commission's science and knowledge service) to engage in the monitoring of advancements in research on biometrics. A technical study on behalf of the Commission's Directorate-General for Migration and Home Affairs (DG HOME) in 2015 provided an assessment of the readiness of AFIS technology for the SIS II and detailed the use cases and technical preconditions that would need to be met to implement an AFIS in the central SIS database. Notably, the study came to the conclusion that 'AFIS technology [had] reached sufficient levels of readiness and availability for its integration into SIS-II'.<sup>72</sup> Based on these results, the Commission produced the required report to inform the Council and the Parliament on the 'availability and readiness of technology to identify a person

<sup>69</sup> European Union, 'Regulation (EC) No 1987/2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)', (Brussels: Official Journal of the European Union, 2006), art. 22(c); European Union, 'Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (SIS II)' (Brussels: Official Journal of the European Union, 2007), art. 22(c).

<sup>70</sup> European Union, 'Regulation (EC) No 1987/2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II)', art. 22(c); European Union, 'Council Decision 2007/533/JHA on the establishment, operation and use of the second generation Schengen Information System (SIS II)', art. 22(c).

<sup>71</sup> eu-LISA, 'Biometrics in large-scale IT: Recent trends, current performance capabilities, recommendations for the future' (Strasbourg: European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice, 2015), p. 8.

<sup>72</sup> Joint Research Centre, 'JRC science for policy report: Fingerprint identification technology for its implementation in the Schengen Information System II (SIS-II)' (Brussels: European Commission, 2015), p. 4.



on the basis of fingerprints held in the second generation Schengen Information System (SIS II).<sup>73</sup> In the report, the Commission made a strong case for the quick development and implementation of an AFIS into the SIS, arguing that ‘it is becoming increasingly difficult to establish the identity of a person due to changing names and the use of aliases or fraudulent documents. The use of document fraud is an increasing modus operandi to illegally enter and move around within the Schengen area.’<sup>74</sup> The SIS AFIS was eventually rolled out for implementation at the member-state level in 2018.<sup>75</sup>

The technology monitoring activities carried out by both eu-LISA and the Commission/JRC study are illustrative of the strategic turn towards tracking innovation in order to be able to make use of novel techno-scientific tools in the context of the SIS as early as possible. As the JRC report made clear, the question was in fact never whether or not to integrate biometric matching capacities into the system in the first place, but merely to determine the point in time when ‘fingerprint identification technology [would be] mature enough for inclusion in SIS-II’.<sup>76</sup> The decisive issue from a practical point of view had thus become how to best keep track of current techno-scientific developments and to find suitable methodologies to evaluate the level of fit between availability and system requirements.<sup>77</sup> All the same, the larger strategic goal in regard to the evolution of the SIS remained unchanged, as it was considered ‘vital that decision makers within the European Institutions remain cognisant of developments so that such systems are based on the most up-to-date technologies and are made sufficiently flexible to adapt to the new developments and technologies that will inevitably transpire in the near future’.<sup>78</sup> The turn to technology monitoring can in this sense be seen as a logical expansion to the latent development approach pursued during the design phase. As the SIS II had been set up in a flexibilised and scalable fashion, technological capacities for the further enhancement of SIS capacities were now considered to emerge almost by default at some point in time – and as long as one kept a keen enough eye on technological progress, the system could be upgraded as needed.

This strategy has been continued and reinforced in recent years. In 2019, the JRC published a series of technical studies that have explored the availability and readiness of DNA profiling,<sup>79</sup> facial recognition,<sup>80</sup> and fingermark and palm-mark identification<sup>81</sup> into the SIS. The recently adopted SIS Recast package has by now paved the way for these features to become part of the SIS, arguably constituting another leap in terms of the system’s identification and investigation capacities. Notably, the JRC studies did not even concern themselves with the question of whether such capacities would be desirable or appropriate in the first place but took the eventual implementation of cutting-edge technology into the SIS as a given.

More recently, technology monitoring has additionally been accompanied by a turn to technology steering. Rather than limiting itself to a passive mode of observing research and industry

<sup>73</sup>European Commission, ‘COM(2016) 93 final: The availability and readiness of technology to identify a person on the basis of fingerprints held in the second generation Schengen Information System (SIS II). 29 February’ (Brussels, 2016).

<sup>74</sup>European Commission, ‘COM(2016) 93 final: The availability and readiness of technology to identify a person on the basis of fingerprints held in the second generation Schengen Information System (SIS II). 29 February’, p. 3.

<sup>75</sup>eu-LISA, ‘Press release: eu-LISA successfully launches SIS II AFIS Phase One’ (6 March 2018), available at {<https://www.eulisa.europa.eu/Newsroom/PressRelease/Pages/eu-LISA-successfully-launches-SIS-II-AFIS-Phase-One.aspx>}.

<sup>76</sup>Joint Research Centre, ‘JRC science for policy report: Fingerprint identification technology for its implementation in the Schengen Information System II (SIS-II)’, p. 17.

<sup>77</sup>Joint Research Centre, ‘JRC science for policy report: Fingerprint identification technology for its implementation in the Schengen Information System II (SIS-II)’, p. 11.

<sup>78</sup>eu-LISA, ‘Biometrics in large-scale IT: Recent trends, current performance capabilities, recommendations for the future’, p. 39.

<sup>79</sup>Joint Research Centre, ‘JRC science for policy report: Study on DNA profiling technology for its implementation in the central Schengen Information System’ (Brussels: European Commission, 2019).

<sup>80</sup>Joint Research Centre, ‘JRC science for policy report: Study on face identification technology for its implementation in the Schengen Information System’ (Brussels: European Commission, 2019).

<sup>81</sup>Joint Research Centre, ‘JRC science for policy report: Study on fingermark and palmmark identification technologies for their implementation in the Schengen Information System’ (Brussels: European Commission, 2019).

activities that largely remain out of direct governmental control, eu-LISA has made an effort to play an active role within EU research funding. In 2021, DG HOME and eu-LISA agreed to Terms of Reference that established eu-LISA's capacity to shape EU research programmes along the lines of identified requirements for European internal security databases.<sup>82</sup> Notably, the agreement includes the competence for 'the timely identification, development and deployment of new technologies and non-technological solutions'<sup>83</sup> in basic and applied research funded by the EU under its Horizon 2020 research-funding framework. eu-LISA will thus in the future be able to define alleged techno-scientific 'gaps' in the SIS and other databases, set requirements for solutions to be researched with EU funding, and prioritise research activities that are considered capable of addressing these gaps.<sup>84</sup>

Such interventions in state-sponsored research activities have – for instance, when it comes to border control<sup>85</sup> or defence<sup>86</sup> – been identified as a prime means of fostering particular visions of social order. While it remains to be seen whether and how active interventions into European research funding will prove to be an effective complementary element within the larger strategy of gradually expanding technologically mediated surveillance and control capacities, the setting up of eu-LISA as a steering actor within EU research funding<sup>87</sup> arguably marks another step towards leveraging the flexible and scalable architecture of the SIS.

Overall, the analysis shows how the idea of a continually growing system in terms of data, user base, and functionalities has always been an integral part of the SIS II – both during its creation and after its roll-out and implementation. From a conceptual point of view, the notion of creep enables us to understand how such growth can happen in slow, gradual, and cumulative ways that result in a relatively stealthy expansion of capacities that obscures tipping points for acceptability and stifles public debate and pushback. At the same time, it directs attention to the deliberate set-up of creep from a political or economic perspective. What the literature on creep has, however, often ignored are the ways in which creep is enabled through specific development and design practices

<sup>82</sup>European Commission and eu-LISA, 'Ares(2021)1886757: Terms of reference between the Directorate-General for Migration and Home Affairs of the European Commission and the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) regarding the role of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice in the parts of the framework programme for research and innovation that include research themes related to innovative solutions for the operational management of large-scale IT systems in the area of freedom, security and justice' (Brussels, 2021).

<sup>83</sup>European Commission and eu-LISA, 'Ares(2021)1886757: Terms of reference between the Directorate-General for Migration and Home Affairs of the European Commission and the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) regarding the role of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice in the parts of the framework programme for research and innovation that include research themes related to innovative solutions for the operational management of large-scale IT systems in the area of freedom, security and justice', p. 2.

<sup>84</sup>Terms of reference between the Directorate-General for Migration and Home Affairs of the European Commission and the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) regarding the role of the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice in the parts of the framework programme for research and innovation that include research themes related to innovative solutions for the operational management of large-scale IT systems in the area of freedom, security and justice', p. 3.

<sup>85</sup>Clemens Binder, 'Developing future borders: The politics of security research and emerging technologies in border security', in Antonio Calcara, Raluca Csernaton, and Chantal Lavallée (eds), *Emerging Security Technologies and EU Governance: Actors, Practices and Processes* (London: Routledge, 2020), pp. 148–163; Trauttmansdorff and Felt, 'Between infrastructural experimentation and collective imagination'; Bruno Oliveira Martins and Maria Gabrielsen Jumbert, 'EU border technologies and the co-production of security "problems" and "solutions"', *Journal of Ethnic and Migration Studies*, 48:6 (2020), pp. 1430–47.

<sup>86</sup>Bruno Oliveira Martins and Jocelyn Mawdsley, 'Sociotechnical imaginaries of EU defence: The past and the future in the European Defence Fund', *Journal of Common Market Studies*, 59:6 (2021), pp. 1458–74.

<sup>87</sup>As well as a similar role for the European Border and Coast Guard Agency: European Commission and FRONTEX, 'Terms of reference between the Directorate-General for Migration and Home Affairs of the European Commission and the European Border and Coast Guard Agency regarding the role of the European Border and Coast Guard Agency in the parts of the framework programme for research and innovation which relate to border security' (Brussels, 2020).

and other measures. The analysis presented here explicitly engages this question and shows how in the case of the SIS, both latent development principles and technology monitoring and steering mechanisms have been used/set up in a way that facilitates the gradual expansion of system capacities and functionalities over time.

## Conclusions

This article has empirically analysed how the SIS has over the past decades evolved from a simple information-sharing network to a full-blown, large-scale investigatory database for the regulation of mobility and security that sits at the core of the Schengen area. Rather than asking what novel modes of governance and/or implications the expanded capacities mediated by the SIS bring about, we have started from the surprising lack of public debate and pushback against the expansion of the system over time. To understand this lack of critical engagement, we have suggested turning to the notion of creep, which has been used to conceptualise how the use of technological tools beyond their originally intended purpose can come about in gradual, slow, and sometimes even imperceptible forms, thus enabling transformations to remain below the threshold of exception and scandal. Notably, the literature on creep suggests that this might in many cases be on purpose, hinting at political rationales to deliberately introduce technologies in an originally narrow and limited use-case context, only to later on broaden the scope to additional use cases once the tool has been implemented and sufficiently normalised.

Taking this literature as a starting point, our analysis shows how the SIS – and more specifically the SIS II, which had been politically discussed and eventually designed from scratch right after the roll-out of the original SIS I – was set up in ways that enable and facilitate the evolving capacities (in the form of the amount and types of data stored, upgraded system functionalities, and access rights for new user groups) of the system. The design and development phase of the SIS II between 1995 and 2013 was marked by a latent development approach that foresaw the implementation of dormant functions in the system that could at a later point be activated once the necessary legal basis and/or technological readiness became available, and which was after 2013 accompanied by complementary mechanisms of technology monitoring and steering that extend notions of flexibility and scalability even beyond the development and design phase and are set to ensure that newly available technology can be integrated into the SIS in the form of updates and upgrades as soon as possible.

There are, so we put forward here, two main implications of our analysis. First of all, the findings highlight the intricate entanglement of political visions and their realisations via technological tools.<sup>88</sup> In this context, the analysis foregrounds how policy and development and design choices have become interlinked to shape a complex multilevel database for information sharing in a particular way. In concrete terms, it highlights how latent development principles have resulted in a deliberately flexible and scalable technological system that would be easily upgradable and expandable in the future. Moreover, the mechanisms for technology monitoring and steering that were introduced after the end of the development and design phase have enabled involved actors to actively keep track of and intervene in the availability and readiness of technological components necessary for such upgrades. This falls in line with more recent arguments about the role of political and bureaucratic actors as technological agenda-setters in national and international security contexts.<sup>89</sup>

Second, these insights do, however, also open up the possibility of a discursive space about the evolution of the SIS and its implications for political power and state actor capacities. If the

<sup>88</sup>Sheila Jasanoff and Sang-Hyun Kim (eds), *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power* (Chicago: University of Chicago Press, 2015).

<sup>89</sup>Bruno Oliveira Martins and Christian Küsters, 'Hidden security: EU public research funds and the development of European drones', *Journal of Common Market Studies*, 57:2 (2019), pp. 278–97; Martins and Jumbert, 'EU border technologies'; Trauttmansdorff and Felt, 'Between infrastructural experimentation and collective imagination'.

expansion of data, analytical functionalities, and user base of the SIS has managed to stay below the threshold of contestation by way of its incremental, slow, and imperceptible nature, rendering the politics of creep visible and public can serve as a means of fostering democratic debate and reclaiming a stronger level of control over the seeming inevitability of techno-bureaucratic projects such as the SIS. It seems safe to assume that the SIS will never be considered a finished product, this much becomes clear in the positions expressed by the Council, the Commission, and eu-LISA over the years. More public awareness of the implications of initiatives such as SIS Recast could, however, so we claim, lead to a broader and better-informed debate about the acceptability of technological expansions and potential tipping points.

The possibility of a discursive space with regard to databases for EU internal security appears all the more important given the current transformations of digital knowledge infrastructures. Existing databases are set to be complemented with new ones, notably the Entry-Exit-System (EES), the European Travel Information Authorisation System (ETIAS), and the European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN). Moreover, all these systems are supposed to be made interoperable through several technical layers of biometric matching and a global portal for search queries.<sup>90</sup> The question then becomes to what extent a politics of creep would also be possible in regard to future developments and in what forms. On the one hand, one might argue that today, there is more transparency about legislative processes at the EU level and subsequently more monitoring and discussions about the implications of enhanced technologically mediated capacities for state authorities. On the other hand, though, the construction and expansion of databases remain a highly complex niche topic that is difficult to edit for meaningful public debate. Critical scholarly engagements will thus remain an important contribution to understanding the origins, forms, and implications of creep – and in the best-case scenario to contribute to more democratic forms of deliberation and control of the techno-politics of EU internal security.

**Acknowledgements.** This article has benefitted immensely from critical yet generous engagement on multiple occasions. We are particularly grateful to Stefania Leuca and Apolline Roland for research assistance, as well as to the editors at *EJIS* for their support and two anonymous referees for productive critique. Matthias Leese's contribution was funded by the Swiss State Secretariat for Education, Research and Innovation SERI under grant agreement no. MB22.00035 (CURATE). Vanessa Ugolini's contribution was funded by the European Research Council (ERC-2021-STG) under grant agreement no. 101043213 (DATAUNION). Authors are listed in alphabetical order and all authors have contributed equally to the manuscript.

**Matthias Leese** is Assistant Professor of Technology and Governance at the Department of Humanities, Social and Political Sciences, ETH Zurich. His research is interested in the effects of digital technologies on social order. In doing so, it pays specific attention to security organisations and their digitally mediated rationales and practices.

**Vanessa Ugolini** is a post-doctoral researcher in the ERC Starting Grant project DATAUNION and a member of the Law, Science, Technology and Society research group at Vrije Universiteit Brussel. Her research investigates European security governance through technology-mediated data practices and looks specifically at the set-up and functioning of information-sharing networks in the domain of internal security.

<sup>90</sup>For an overview, see for instance Bellanova and Glouftsis, 'Formatting European security integration'; Leese, 'Fixing state vision'; Julien Jeandesboz, 'European Union information systems for border and migration enforcement: Trajectories, programmatics, and uses', in Graham Hudson and Idil Atak (eds), *Migration, Security, and Resistance: Global and Local Perspectives* (London: Routledge, 2021), pp. 47–65.