European Journal of International Security (2026), **11**, 247–261
doi:10.1017/eis.2025.14

EJIS

RESEARCH ARTICLE

Imaginaries and infrastructures of platform security

Marieke de Goede

Department of Political Science and Faculty of Humanities, University of Amsterdam, Amsterdam, The Netherlands
Email: M.deGoede@uva.nl

(Received 17 January 2024; revised 16 December 2024; accepted 21 February 2025)

Abstract
This paper develops the notion of 'Platform Security' to analyse the type of security power that seeks to work through facilitation and decentralised connection. The paper draws an analogy between the metaphor and model of the platform economy and contemporary security practices. It analyses the *imaginaries* and *infrastructures* of the platform economy and shows how these are present in the work of transnational security authorities. Like online platforms, contemporary security practitioners seek to connect local players in a manner that is data-driven and decentred. Like digital platforms, security organisations like FATF and Europol seem to understand themselves as utilities or services, whose primary aim is to 'transmit communication and information data' that they have not themselves produced or commissioned (Van Dijck 2013: 6). Analysing platform security through this lens, allows the development critical purchase on this mode of security power and raise critical questions about the organisation of responsibility and protections.

Keywords: counterterrorism; European security; media studies; platform; security practices

'We are a service provider' [European Police Agency official, public workshop remarks]

Introduction: Security service provider

In 2019, the European Court of Justice (ECJ) asked whether property rental platform AirBnB should be classified as a 'lodging corporation' or whether it is a 'sharing economy platform'.[1] In this case, brought by the French Tourist Agency, the ECJ found in favour of AirBnB and confirmed that the platform is not a property company but an *information company*. This verdict had consequences for AirBnB's regulation, and its liability for licensing and taxation. In brief, the court found that AirBnB is a 'mere connector', which means that it carries 'no responsibility' for sector-wide standards like consumer protection and safety.[2] Around the same time, European Police Agency Europol outlined its *2020+ Vision*, and set out its ambition to become 'the EU criminal information hub making full use of data from an extensive network of partners', and to become 'a *platform* for European policing solutions'.[3] This vision is accompanied by new types of technology infrastructures, like Ma3tch, that allow European national police databases to connect and

[1]Tarik Dogru, Makarand Mody, Courtney Suess, Nathan Line, Mark Bonn, 'Airbnb 2.0: Is it a sharing economy platform or a lodging corporation?,' *Tourism Management,* 78 (2020), pp. 1–5.

[2]José van Dijck, Thomas Poell and Martijn de Waal, *The Platform Society: Public Values in a Connective World* (Oxford: Oxford University Press, 2018), p. 74.

[3]Europol, *Europol 2020+ Vision*, Vienna, December 13, 2020, p. 2

© The Author(s), 2025. Published by Cambridge University Press on behalf of The British International Studies Association. This is an Open Access article, distributed under the terms of the Creative Commons Attribution-NonCommercial licence (http://creativecommons.org/licenses/by-nc/4.0), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original article is properly cited. The written permission of Cambridge University Press must be obtained prior to any commercial use.

https://doi.org/10.1017/eis.2025.14 Published online by Cambridge University Press

communicate *without* central integration. This also has consequences for regulation, as the lack of centrally integrated databases means that EU privacy law does not centrally apply. As one European law enforcement official put it in a public meeting: 'We are a service provider'.[4]

This article proposes that the imaginary and infrastructure of the platform economy – as exemplified in the AirBnB case – is also emerging in the security practices of a range of Western security institutions in recent years – as exemplified in the Europol 2020+ approach. There is a deep analogy at work between the AirBnB case and the Europol vision. Like digital platform companies, security authorities sometimes seek to position themselves as neutral intermediaries and technical facilitators, rather than influential powers. Instead of claiming supranational authority and competence, some (European) security institutions are presenting themselves as 'mere' information services, connectors, and information hubs. As such, these security institutions emulate the discourses and practices of digital platforms that connect and commercialise the contributions of end-to-end users in the online environment. Like the 'information society service' of AirBnB, these security practices work through the facilitation and connection of decentred participants. They involve a discursive minimisation of power and enable regulation avoidance.

If security authorities are thought to exist by virtue of claiming power and speaking security,[5] this minimisation of the own role and the emphasis on 'mere' facilitation seems surprising and something that requires more explanation. Notions of mundane and material security practices,[6] for example as expressed in the idea of 'little security nothings', go some way towards analysing everyday and seemingly modest self-representations of security authorities.[7] The modest positioning of Europol is also understandable in the context of its limited role in a European context, whereby police matters remain primarily national affairs. Yet this does not fully explain the way in which the platform metaphor and model has become so crucial to the discourses and technical infrastructures of transnational security institutions like Europol and others. Nor do these elements explain the ways in which transnational security institutions adopt technical practices that emulate key technologies and infrastructures of digital platform companies.

This article asks: why and how do transnational security institutions depict and deliver their services in terms drawn from discourses and practices of internet platforms? The paper draws out the analogy between discourses and practices of the *platform economy* and what I call *platform security*. I do not claim that platform security and platform economy are exactly the same – yet I argue that we see more than a superficial parallel here. There is a deep analogy at work between the way that security institutions represent themselves and organise their technical practices, and the ways in which digital platform companies represent themselves and organise their technical practices. I use the term 'analogy' here to compare digital company practices and security practices for 'the purpose of explanation or clarification',[8] and to explore how critical questions concerning digital platforms may be applied to security practices. Digital platform companies reorganise collective responsibility for sectors including news, transport, and urban housing. Their imaginaries and infrastructures raise questions concerning regulation, responsibility, accessibility, and privacy protection, among other issues.[9] The analogy between platform economy and platform security

[4]European police agency official, public remarks, workshop, University of Amsterdam, March 8, 2019.

[5]Lene Hansen, *Security as Practice: Discourse Analysis and the Bosnian War* (Abingdon: Routledge, 2006); Jef Huysmans, *The Politics of Insecurity: Fear, Migration and Asylum in the EU* (London: Routledge, 2006).

[6]For example, Rocco Bellanova and Gloria Gonzalez-Fuster, 'Composting and computing: On digital security compositions,' *European Journal of International Security*, 4:3 (2019), pp. 345–65; Michael Bourne and Debbie Lisle, 'The many lives of border automation: Turbulence, coordination and care', *Social Studies of Science,* 49:5 (2019), pp. 682–706; Stefan Elbe and Gemma Buckland-Merrett, 'Entangled security: Science, co-production, and intra-active insecurity', *European Journal of International Security*, 4:2 (2019), pp. 123–41; Nathaniel O'Grady, 'Automating security infrastructures: Practices, imaginaries, politics', *Security Dialogue*, 52:3 (2021), pp. 231–48.

[7]Jef Huysmans, 'What's in an act: On security speech acts and little security nothings', *Security Dialogue*, 42:4–5 (2011), pp. 371–383.

[8]Oxford Languages, via Google.

[9]van Dijck, Poell, de Waal, *The Platform Society.*

https://doi.org/10.1017/eis.2025.14 Published online by Cambridge University Press

enables us to ask similar questions about transnational security practices: how they reorganise collective responsibility and regulation and challenge traditional modes of governance.

This paper argues that the analogy between platform security and platform economy comprises both discursive representation and technological practices. I use the term *imaginaries* to explore analogies in discursive representation, and the term *infrastructures* to unpack the material analogies between digital platforms and security practices.[10] Imaginaries are understood as 'collectively imagined forms of social life and social order' that help shape and enable discourses and policy outcomes.[11] They entail 'distinctive … visions of desirable futures driven by science and technology'.[12] In addition, the concept of infrastructures is useful to analyse the material-technical aspects of platform imaginaries.[13] The focus on infrastructure draws attention to the material organisation and technical properties of platforms. It helps analyse the affordances or 'dispositions' encoded into technologies, understood as their propensity to enable or constrain possibilities.[14]

In order to develop the argument, the paper first fosters a discussion between critical security studies on the one hand, and the literature in media studies that analyses digital platforms as a metaphor and model of power, on the other. Then, I zoom in on the *imaginaries* and the *infrastructure* of the platform economy, as they have been identified in the literature. This is followed by a short note on method. Empirically, the paper draws on examples from fieldwork in the realm of European counterterrorism, with a specific focus on institutions and practices that aim to counter-terrorism financing (CTF). The final section of the paper raises the question how platform security impacts public values and raises critical questions about security practices in Europe.

Critical security studies meets platform studies

Critical security studies offers good starting points for thinking through a platform model of security; from both a rhetorical and a material-technical perspective. Within the literature on European security, Mai'a Davis Cross was one of the first authors to analyse EU security as a hub-and-spoke model whereby knowledge networks play a crucial role.[15] This literature has shown how EU security is dependent on the creation and connection of digital databases.[16] Authors have critically analysed the new EU approach of digital 'interoperability', and shown how it dislodges existing accountability structures.[17]

Furthermore, literatures in critical security studies have analysed how ubiquitous digitisation and Artificial Intelligence (AI) have impacted security politics and practices of warfare and

[10]Nikhil Anand, Akhil Gupta, and Hannah Appel, *The Promise of Infrastructure* (Durham: Duke University Press, 2018); Keller Easterling, *Extrastatecraft. The Power of Infrastructure Space* (London and New York: Verso, 2016).

[11]Sheila Jasanoff and Sang-Hyun Kim, 'Containing the atom: Sociotechnical imaginaries and nuclear power in the United States and South Korea', *Minerva* 47:2 (2009), pp. 119–146 (p. 120); Andreas Baur, 'European dreams of the cloud: Imagining innovation and political control', *Geopolitics*, 29:3 (2023), pp. 796–820; Lucy Suchman, 'Algorithmic warfare and the reinvention of accuracy', *Critical Studies on Security*, 8:2 (2020), pp. 175–187.

[12]Jasanoff and Kim, 'Containing the atom', p. 121.

[13]Star, Susan Leigh Star, 'The ethnography of infrastructure', *American Behavioral Scientist*, 43:3 (1999), pp. 377–391; Anand et al., *The Promise of Infrastructure*.

[14]Easterling, *Extrastatecraft*.

[15]Mai'a Davis Cross, *Security Integration in Europe: How Knowledge-based Networks are Transforming the European Union* (Ann Arbor: University of Michigan Press, 2011); Huub Dijstelbloem, *Borders as Infrastructure: The Technopolitics of Border Control* (Harvard: MIT Press, 2021).

[16]Rocco Bellanova, Helena Carrapico and Denis Duez, 'Digital/sovereignty and European security integration: an introduction', *European Security*, 31:3 (2022), pp. 337–355; Julien Jeandesboz, 'Smartening border security in the European Union: An associational inquiry', *Security Dialogue,* 47:4 (2016), pp. 292–309; Lena Ulbricht, 'When Big Data Meet Securitization', *European Journal for Security Research* 3:2 (2018), pp. 139–161.

[17]Rocco Bellanova and Georgios Glouftsios, 'Controlling the Schengen Information System (SIS II): The infrastructural politics of fragility and maintenance', *Geopolitics*, 27:1 (2022), pp. 160–184; Deirdre Curtin and Mariavittoria Catanzariti (eds), *Data at the Boundaries of European Law* (Oxford: Oxford University Press, 2023); Matthias Leese, 'Fixing state vision: Interoperability, biometrics, and identity management in the EU', *Geopolitics*, 27:1 (2022), pp. 113–33.

https://doi.org/10.1017/eis.2025.14 Published online by Cambridge University Press

sovereignty.[18] Information dominance is considered crucial to modern warfare, meaning that the digitisation and acceleration of information are core to the military revolution. A modern tank, for example, is not simply a military vehicle but also a platform for battlefield information and situational awareness.[19] This literature has extensively discussed the importance of data analytics to modern security practices.[20] With the role of Big Tech companies like Google in data-driven battlefield targeting and experimentation, Marijn Hoijtink signals 'a new regime of warfare'.[21] Yet, with some exceptions, this literature has not really engaged with the question of the relation between the modern platform economy (of Google, Uber, AirBnB) and contemporary security practice.[22] That is surprising, because the modern 'Big tech' companies affect all aspects of contemporary life, including the ways in which security is imagined, practiced, and experienced.

In a different field, there is a burgeoning literature about online digital platforms and the ways in which they transform social, economic, and cultural practices.[23] This literature shows that the platform economy impacts every aspect of everyday life, from the way we interact with friends to the way we consume foods; from the way in which sexual encounters take place, to the way in which we travel.

As this literature has extensively shown, platform power profoundly challenges public values. Platforms like Facebook and Uber 'claim to be mere connectors, carrying no responsibility for the sector as such'.[24] Yet their imaginaries and infrastructures change whole sectors and challenge the checks and balances that have been historically built to safeguard the quality of, for example, public transport, including 'consumer protection, passenger safety, and inclusiveness'.[25] This is powerfully illustrated in the AiRBnB case with which we started this paper which deliberately challenges regulation of the urban rental market, including licensing, taxation, and consumer protection, through its infrastructural form of a global 'information intermediary'.

Literatures on platforms, with some exceptions, have not paid much attention to the *security* roles of Big Tech platforms, and the ways in which practices of platform companies contribute to militarism and warfare.[26] This is surprising, because platform companies and technologies are crucial to modern warfare and security practices. Planqué-van Hardeveld enumerates three clusters of security roles that are played by Google, ranging from Google's involvement in AI technologies for

[18] Antoine Bousquet, Jairus Grove and Nisha Shah, 'Becoming war: Towards a martial empiricism', *Security Dialogue*, 51:2–3 (2020), pp. 99–118; Marcus Michaelsen and Johannes Thumfart, 'Drawing a line: Digital transnational repression against political exiles ad host state sovereignty', *European Journal of International Security*, 8:2 (2023), pp. 151–71; Nisha Shah, 'Gunning for War: infantry rifles and the calibration of lethal force', *Critical Studies on Security,* 5:1 (2017), pp. 81–104; Elke Schwartz, 'Autonomous weapon systems, Artificial intelligence and the problem of meaningful human control', *Philosophical Journal of Conflict and Violence,* V:1 (2021).

[19] James Der Derian, *Virtuous War*. Boulder (Co: Westview Press, 2001); Mikkel V. Rasmussen, *The Risk Society at War* (Cambridge: Cambridge University Press, 2006).

[20] Louise Amoore and Rita Raley, 'Securing with algorithms: Knowledge, decision, sovereignty', *Security Dialogue*, 48:1 (2017), pp. 3–10; Marijn Hoijtink, "Prototype warfare': Innovation, optimisation, and the experimental way of warfare', *European Journal of International Security*, 7:3 (2022), pp. 322–36.

[21] Hoijtink, 'Prototype Warfare', p. 324.

[22] But see Marijn Hoijtink and Anneroos Planqué-van Hardeveld, 'Machine learning and the platformization of the military: A study of Google's machine learning platform TensorFlow', *International Political Sociology*, 16:2 (2022), pp. 1–19.

[23] Tarleton Gillespie, *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media* (New Haven: Yale University Press, 2018); Robert Gorwa, 'What is platform governance?', *Information, Communication & Society*, 22:6 (2019), pp. 854–57; José van Dijck, *The Culture of Connectivity: A Critical History of Social Media* (Oxford: Oxford University Press, 2013); Karen Yeung, 'Algorithmic regulation: A critical interrogation', *Regulation & Governance*, 12:4 (2018), pp. 505–23.

[24] van Dijck, Poell, de Waal, *The Platform Society,* p. 74.

[25] van Dijck, Poell, de Waal, *The Platform Society,* p. 74.

[26] But see Amoore and Raley, 'Securing with algorithms'; Louise Amoore, *The Politics of Possibility: Risk and Security Beyond Probability* (Durham: Duke University Press, 2013); Rune Saugmann, 'Military techno-vision: Technologies between visual ambiguity and the desire for security facts', *European Journal of International Security*, 4:3 (2019), pp. 300–21.

https://doi.org/10.1017/eis.2025.14 Published online by Cambridge University Press

national defence to the online policing of digital content with possible terrorist intent.[27] Hoijtink uses the term 'platform warfare' to theorise the ways in which digital platforms and modern warfare are increasingly interrelated.[28] The most important way in which literatures on digital platforms have engaged with questions of security, is through the study of content moderation.[29] Social media platforms like Twitter, Instagram, Facebook, but also gaming sites and smaller platforms, are required (by law or regulation) to police their servers for material that may be criminal or terrorist in content, and take actions to remove or render such material invisible. This authorises big tech platforms to make important security decisions (about taking content offline, closing accounts) that makes them effective 'co-producers' of security.[30] In this manner, content moderation has become a crucial anchor of governance of platform power.

The next sections further discuss the literature on platform studies in order to tease out some core elements of *platform imaginaries* and *platform infrastructures*. This will be the basis of critical enquiry into the security imaginaries and infrastructures that we have identified through fieldwork.

Platform imaginaries and infrastructures

This section discusses the literature on platform studies and draws out its relevance for security studies. The purpose here is not to offer a full overview but to distill several elements of platform imaginaries and infrastructures that act as thematic guides to the empirical analysis that follows.

Though the literature on platforms does not offer one definition of what a platform is and how it works, it broadly argues that the digital platform is *a mode of power*. As Christofari shows, the platform is an important metaphor and model of power, rather than purely an objective description of technical infrastructure or company model.[31] Different aspects of platform power are discerned. For Culpepper and Thelen, it is the 'tight, even intimate, connection to their users' that underpins 'distinctive form of power' of large platforms, which have unprecedented 'scale and influence'.[32] Another approach stresses that platforms are 'active political actors in their own right' because they have considerable 'opinion power' in shaping how platform users retrieve information and engage with news.[33] Platforms make important choices about the way in which information is curated, shared, connected and made (in)visible. These choices are inscribed in the technical affordances of platforms and, as such, shape and constrain the behaviour and options of users. For Aradau and Blanke then, the crux of platform power is that it materially constitutes 'algorithmically constituted relations'.[34] They argue that platform power is not (just) about platforms' abilities to 'conquer new territories and integrate new populations' but also about new modes of algorithmic classification that govern populations.[35] The following discussion of platform imaginaries and infrastructures builds on the core notion of the digital platform as a mode of power.

[27] Anneroos Planqué-van Hardeveld, 'Securing the platform: how Google appropriates security', *Critical Studies on Security*, 11:3 (2023), pp. 161–75.

[28] Hoijtink, 'Prototype Warfare',

[29] Sarah T. Roberts, *Behind the Screen* (Yale: Yale University Press, 2019); Gillespie, *Custodians of the Internet*.

[30] Rocco Bellanova and Marieke de Goede, 'Co-Producing Security: Platform Content Moderation and European Security Integration', *JCMS: Journal of Common Market Studies*, 60:5 (2022), pp. 1316–34.

[31] Gianmarco Christofari, *The Politics of Platformization: Amsterdam Dialogues on Platform Theory* (Amsterdam: Institute of Network Cultures, 2023).

[32] P.D. Culpepper and K. Thelen, 'Are we All Amazon Primed? Consumers and the Politics of Platform Power,' Comparative Political Studies, 53:2 (2020), pp. 288–319 (p. 290).

[33] Natali Helberger, 'The political power of platforms: How current attempts to regulate misinformation amplify opinion power', *Digital Journalism*, 8:6 (2020), pp. 842–54 (p. 842).

[34] Claudia Aradau and Tobias Blanke, *Algorithmic Reason: The New Government of Self and Other* (Oxford: Oxford University Press, 2022), p. 93.

[35] Aradau and Blanke, *Algorithmic Reason*, p. 112; also Louise Amoore, 'Machine learning political orders', *Review of International Studies*, 49:1 (2023), pp. 20–36.

https://doi.org/10.1017/eis.2025.14 Published online by Cambridge University Press

Platform imaginaries

First, it is well-known that the platform economy offers a powerful imaginary that has only recently become broadly contested.[36] The platform economy was built on a powerful imaginary of a 'sharing economy'. Early participants in the digital economy speak of the online sphere as one of bottom-up self-organisation and technical experimentation. In particular, the notion of the 'the platform' does important 'discursive work' to position large digital companies as neutral 'intermediaries', as argued by Tarleton Gillespie.[37] 'The broad connotations' of the term platform include, as Gillespie summarises them, an 'open, neutral, egalitarian, and progressive support for activity'.[38] For Gillespie, the logic of platform 'implies a neutrality with regards to the activity'.[39] Paul Langley and Andrew Leyshon similarly explore the 'distinctive intermediary logic of the platform' as it emerges from memoirs, media, popular literature and personal accounts of internet pioneers.[40] They find that these sources celebrate the platform economy for its 'disintermediated, collaborative, and even democratising qualities'.[41] The platform imaginary is one of emergent self-organisation and decentralised connectivity. It emphasises a dream of global connectivity and disintermediation by which users themselves are in control of content and collaboration.

Enabling data connectivity is one crucial aspect of the platform imaginary noted in most definitions: modern platform companies like Twitter, Facebook, and AirBnB curate and transmit 'communication and information data' that they have not themselves produced or commissioned.[42] In van Dijck's succinct terms, platforms are not simply in the business of intermediating *connections*, but of actively curating *connectivity*.[43] As Gillespie writes about social media platforms:

> They don't make content, but they make important choices about that content: what they will distribute and to whom, how they will connect users and broker their interactions, and what they will refuse.… We have to revisit difficult questions about … what rights and responsibilities should accompany that.[44]

In short, two elements are taken from the literature on platform studies to inform the empirical analysis of platform imaginaries. First, the platform imaginary emphasises neutrality and decentred connectivity. This entails a disavowal of power and obfuscates how platforms are infused with power: they actively curate content, prioritise visibilities, and shape connectivities. Second, the platform imaginary entails new organisational forms whereby decentralised data are connected and curated in particular ways. Digital platforms shape the ways in which citizens and consumers see content, read news, interact with friends, and receive advertising content. Below, I will explore how the imaginary of platforms is embraced and redeployed by security practitioners and institutions.

Platform infrastructures

Furthermore, digital platforms encompass not just a specific (capitalist) imaginary but also specific material-technical modes of organisation. As Anne Helmond put it, it is important to examine the

[36]Paul Langley and Andrew Leyshon, 'Platform Capitalism: the intermediation and capitalisation of digital economic circulation', *Finance and Society*, 3:1 (2017), pp. 11–31; Lizzie Richardson, 'Performing the sharing economy', *Geoforum*, 67 (2015), pp. 121–29.

[37]Gillespie, Tarleton, 'The politics of 'platforms'', *New Media & Society*, 12:3 (2010), pp. 347–64. (p. 348).

[38]Gillespie, 'The politics of 'platforms'', p. 352.

[39]Gillespie, 'The politics of 'platforms'', p. 350.

[40]Langley and Leyshon, 'Platform capitalism', p. 14.

[41]Langley and Leyshon, 'Platform capitalism', p. 13.

[42]van Dijck, *The Culture of Connectivity*, p. 6

[43]van Dijck, *The Culture of Connectivity*.

[44]Tarleton Gillespie, 'Regulation of and by platforms', in J. Burgess, A. Marwick, and T. Poell (eds.) *The SAGE Handbook of Social Media* (London: SAGE, 2018), pp. 254–78 (p. 254).

https://doi.org/10.1017/eis.2025.14 Published online by Cambridge University Press

'work that platforms do' not only 'in a rhetorical sense … but from a material–technical perspective'.[45] How are the material-technical propensities of platform infrastructures defined and analysed in the relevant Media Studies literatures?

Here, I draw out two common themes on how digital platforms exercise power infrastructurally, both juridically and technologically. First, digital platform companies build infrastructures that allow them to disavow responsibility and evade regulation. This is illustrated by expanding further on the example of AirBnB ECJ case, as mentioned in the introduction to this paper. The case was brought by the French Tourist agency to ask whether property rental platform AirBnB should be classified as an estate agency, which would need a license to operate under French law.[46] The core question in this case was whether the company is a 'lodging corporation' or whether it is a 'sharing economy platform'.[47] The French state argued that AirBnB is a lodging corporation because it does *more* than digitally connect owners of property with those seeking accommodation: it also offers services such as photography and insurance to support the rental transaction. AirBnB itself argued that it offers a digital intermediation service that connects hosts with guest but does not influence pricing or other conditions of the rental transaction. Therefore, it is to be regarded as an 'information society service' that is not liable to licensing and taxation, and that is protected under the EU regulations on E-commerce.[48] In this case, the ECJ found in favour of AirBnB and confirmed that the platform is not considered a property company but an information company, and it is therefore not required to hold a estate agent's license in France and not liable to the same type of regulation and taxation that applies to estate agents.

The juridical-technical infrastructures of digital platform companies are structured as 'mere connectors' and information services, thereby enabling the avoidance of regulation. Regulation *avoidance* is different from deliberate (and illegal) regulation *evasion*: it works with technical-juridical structures that aim to ensure that regulation does not apply, which is fundamentally different from non-compliance. A first key aspect of platform infrastructures, then, is regulation avoidance through technical-juridical decentralisation.

Second, digital platform companies build infrastructural bases of operation on which other applications need to run, generating important lock-in effects.[49] Plantin *et al.* show that some platforms – like Google – have become infrastructural, i.e. indispensable to the core functioning of everyday life in contemporary society.[50] Platform power partly operates through the technical features that make platforms programmable and scalable.[51] Programmable platforms form the infrastructure on which other applications need to run. Platformisation works through lock in, whereby technical extensions generate business partnerships.[52]

These processes of interlocking and programmability is why Helmond theorises the power of platforms '*like a squid* whose tentacles function as locking mechanisms'.[53] Key elements of the

[45] Anne Helmond, 'The platformization of the web: Making web data platform ready', *Social Media + Society* 1:2 (2015), pp. 1–11 (p. 2).

[46] InfoCuria, C-390/18 – AirBnB Ireland, December 19, 2019, at: https://curia.europa.eu/juris/liste.jsf?num=C-390/18, accessed January 4, 2024.

[47] Dorgu et al, 'Airbnb 2.0.'

[48] Chris Fox, 'AirBnB is not an Estate Agent, EU Court Rules', *BBC online*, 19 December 2019, https://www.bbc.com/news/technology-50851419, accessed January 4, 2024.

[49] Tobias Blanke, Tobias and Jennifer Pybus, 'The material conditions of platforms: Monopolization through decentralization', *Social Media + Society, 6*:4 (2020).

[50] J-C. Plantin, C. Lagoze, P.N. Edwards and C. Sandvig, 'Infrastructure studies meet platform studies in the age of Google and Facebook', *New Media & Society*, 20:1 (2018), pp. 293–310.

[51] J-C. Plantin and A. Punathambekar, 'Digital media infrastructures: pipes, platforms, and politics', *Media, Culture & Society*, 41:2 (2019), pp. 163–74.

[52] Fernando N. van der Vlist and Anne Helmond, 'How partners mediate platform power: Mapping business and data partnerships in the social media ecosystem', *Big Data & Society*, 8:1 (2021), p. 2.

[53] Anne Helmond, 'The infrastructures and data flows of social media platforms', in Gianmarco Christofari, *The Politics of Platformization: Amsterdam Dialogues on Platform Theory* (Amsterdam: Institute of Network Cultures, 2023), p. 110, emphasis added.

https://doi.org/10.1017/eis.2025.14 Published online by Cambridge University Press

'squid-like' power of platforms are their decentralised connectivity and their programmability. 'Having to work with a proprietary platform over which the great majority of the players have no control has become the fate of most actors in the digital realm' Aradau and Blanke also conclude.[54]

In sum, we take two elements from the literatures on platforms-as-infrastructure for the purposes of our analysis of security practices. First, platforms infrastructures comprise decentralised, 'mere' connectivity, which enables regulation avoidance. Second, platforms are programmable and often form a basis on which other participants and applications run. This means that platforms have a 'lock-in' effect that shape and limit participants' future choices. In the empirical sections, I examine how security practices similarly operate with regulation avoidance and through lock-in effects.

Methodological note

The remainder of this paper teases out the analogy between platform imaginaries and infrastructures on the one hand, and contemporary security practices on the other. The empirical parts of the paper are based on interviews and participant observations in the broad field of CTF in Europe between 2016 and 2022. Empirical examples are drawn from observations and documents of several security institutions, including European Police Agency Europol; the Financial Action Task Force (FATF), that is responsible for developing transnational regulation and guidelines in the field of Anti-money Laundering and Counterterrorism Financing; and the public–private datasharing initiatives centring around terrorism financing, including the Dutch Terrorism Financing Platform (TF Platform) and British Joint Money Laundering Intelligence Taskforce (JMLIT). These actors are crucial transnational institutions/authorities, with significant impact on the shape of national law and regulation concerning terrorism and terrorism financing, while largely remaining beyond political purview.

Analytically, the method was inductive: the analogy to platform imaginaries and infrastructures was not a primary research objective of the fieldwork, but arose as a theme throughout observations and interviews. The methodological approach in the larger project – of which this paper is a part – was to 'immerse' ourselves into the life-worlds of financial security practitioners, 'learning the daily language, plotting the struggles, … understanding the deep well of commonsense beliefs'.[55] This entailed approaching the professional field without judgement.[56] Though there was a thematic focus for the fieldwork, there was also space for new themes to arise inductively by 'travel[ling] back and forth between the part and the whole, experience and text, fieldwork and theory'.[57] It is in this 'travelling back and forth' that the platform analogy took shape: I started to recognise a theme when interviewees regularly described their work in terms of facilitation, technical assistance and building connectivity, while minimising their own role. Once I started noticing the platform metaphors and models in professional security discourses – from 2017 onwards – I remained attentive to the theme, and steered interview questions in this direction.

All examples are drawn from security practices relating to countering terrorism, terrorism financing and financial intelligence sharing, which was also the focus of our larger research project.[58] Though the focus on CTF seems to address a very specific (and perhaps not very significant) problem-space, it is in this empirical practical domain that we find advanced experimental

[54] Aradau and Blanke, *Algorithmic Reason*, p. 96.

[55] Mark B. Salter, 'Expertise in the aviation security field', in M. B. Salter and C. E. Mutlu (eds) *Research Methods in Critical Security Studies* (New York: Routledge, 2013) p. 105; Pieter Lagerwaard (2020) 'Flattening the international: producing financial intelligence through a platform', *Critical Studies on Security,* 8:2 (2020), pp. 160–74.

[56] Marieke de Goede, 'Engagement all the way down', *Critical Studies on Security*, 8:2 (2020), pp. 101–15.

[57] Wanda Vrasti, 'Travelling with ethnography', in M. B. Salter and C. E. Mutlu (eds) *Research Methods in Critical Security Studies* (New York: Routledge, 2013), p. 61.

[58] Marieke de Goede, 'The chain of security', *Review of International Studies*, 44:1 (2018), pp. 24–42.

https://doi.org/10.1017/eis.2025.14 Published online by Cambridge University Press

security and policing techniques at the limits of law.[59] The political urgency of CTF, and its data-led nature, produces security practices that push existing and institutional and legal boundaries. Consequently, this problem space is a relevant site of empirical observation, with the potential to reveal the cutting edge of security practices and imaginaries.

Platform security imaginaries

This section focuses on the ways in which the platform imaginary manifest itself in the professional self-representations and justifications of security actors. Core elements of the platform imaginary, as identified above, include an emphasis on neutrality and decentred connectivity. In addition, the platform imaginary gives rise to new organisational forms whereby decentralised data are connected and curated in particular ways. This section shows that, as with the platform economy, the socio-technical imaginaries of 'security platforms' help efface or disavow their active roles in curating particular connections and in selecting, shaping, and presenting content.

During fieldwork at a range of security institutions, interviewees actively sought to put their work into a modest perspective, emphasising their lack of executive power, and foregrounding their mediating and facilitating role. For example, in our visit to the FATF secretariat, it was emphasised that the secretariat has a subservient role, that it is at the service of member states, that it does not have an independent authority to shape agendas or deliver policy content. Security practitioners seek to present their work as primarily intermediating the work of sovereign authorities, or facilitating connections between decentred investigations or databases. Such self-representations are not simply a pose, but are themselves productive of specific security practices and technologies. It is important to analyse on their own terms the arguments and justifications that policy practitioners put forward about their work, which tells us something about 'the concern for the good that persons are moved by'.[60] An interview or public event confronts the security professional with 'an imperative of justification' – and I assume that such justifications tell us something important about the positioning of organisations and their sense of doing things well.

Take the FATF, an important international organisation that sets standards for governance, regulation, and best practices in the field of AML/CFT. The FATF as an organisation emphasises its facilitating and even subservient role vis-à-vis its members. A lot of its work is cast in terms of technical assistance and voluntary mutual evaluations.[61] Interviewees emphasise that they do not have 'a mandate for technical guidance' but that this always happens under the auspices of a presidency by a particular country.[62] For example, a representative of the secretariat, when asked about his views on whether a particular type of public-private data-sharing is a model for the future, said that he 'does not have any views'.[63] In this manner, the secretariat of the most prominent organisation in developing standards and best practices for AML/CTF, sought to express that this is a member-driven organisation, that in itself lacks a strong agenda or strong views, but that acts in the service of its member states' agendas and priorities. Yet at the same time FATF plays an incredibly important role in the ways in which member states practice financial rule making, and is closely involved in the design of national law and regulation.

[59]For example, see Anthony Amicelle, 'Towards a new political economy of financial surveillance', *Security Dialogue,* 42:2 (2011), pp. 161–78; Lisa Bhungalia, *Elastic Empire: Refashioning War through Aid in Palestine* (Stanford: Stanford University Press, 2023).

[60]Luc Boltanski and Laurent Thévenot, 'The reality of moral expectations: A sociology of situated judgement,' *Philosophical* Explorations, 3:3 (2000), pp. 208–31 (p. 208); also Christian Bueger and Frank Gadinger, 'The play of international practice', *International Studies Quarterly*, 59:3 (2015), pp. 449–60.

[61]Mark T. Nance, 'The regime that FATF built: an introduction to the Financial Action Task Force,' *Crime, Law, and Social Change,* 69:2 (2018), pp. 109–29; Pieter Lagerwaard and Marieke de Goede, 'In trust we share: The politics of financial intelligence sharing,' *Economy and Society,* 52:2 (2023), pp. 202–26.

[62]Interview, FATF secretariat, Paris, February 2019.

[63]Ibid.

https://doi.org/10.1017/eis.2025.14 Published online by Cambridge University Press

In another example, in our fieldwork at a European police organisation, a lot of emphasis was placed on their facilitating and interconnecting role, especially where it concerns cross-checking police data transnationally. This Europol Internet Referral Unit (IRU), which has the mandate to 'detect and refer the core disseminators of terrorist propaganda'.[64] IRU's mode of operation is one of close connection with and facilitation of, private company decisions to remove suspect content. IRU does not itself remove online content or police the digital public sphere, but it works with platform companies and on the basis of company 'Terms of Service' documents in order to suggest content removals. The security decision to remove content or close accounts remains a private one, yet it is facilitated and technically supported by the Europol. Companies themselves identify, select, search, interpret suspicious transactions; they monitor, regulate, restrict, and expel client groups. Here, the modus operandi is one of technical enforcement and privileged communications with platform companies themselves. As one interviewee put it, 'you have the terms of service and then you have the capacity of the company to enforce these terms and services and that's where it's complicated'.[65] The police agency does not collect or store or retain police data centrally, but emphasises its facilitating role:

> honestly it's not rocket science … [when you report a suspicious utterance] you give context if requested by the platform, you give the URL, … the dates. If it's language that they [the companies] cannot understand you translate and, but it, I mean, *this is about informing them and having enough information for them to take a decision*, so, if you just send to URL without any context of course this will never work.[66]

IRU works with and through the platform model of the companies themselves; offering technical support in terms of curation, presentation, and translation. In these practices of countering extremism online, we see a positioning of law enforcement as *facilitator* of company removal processes and *connector* of commercial databases, which has parallels with the socio-technical imaginary of the platform.

In other instances, we observed a socio-technical imaginary of being the technical connector and digital node in the field of European counterterrorism. One interviewee described how, in the wake of the Bataclan attacks of 2015, the European police agency played a pivotal role in connecting police data across borders. In this context, the interviewee notes, the European police agency was '*not a driver*' for more data exchange, but a technical *facilitator* with the capacity to handle the data:

> Not driver. Everyone saw the necessity to exchange more but not everyone can handle the data.… We cannot manage everything but the level of exchange increased in a very good way, in quality and quantity, meaning that the data available in the C[ounter] T[errorism] area, in the CT database … now is massive.[67]

In this sense, the interviewee emphasises the technical capability and connectivity of the police agency. At the same time, the role of the police agency is understood in terms of analytical support, connecting information, providing leads and suggestions.

In the context of a discussion about the analytical work of the police agency, there was mention of the production of a 'beautiful report', understood as a compelling presentation to be handed to the frontline police organisation to work with. We questioned the interviewee on this notion of the 'beautiful report': what analytical work is being done here? The interviewee was talking about

[64]EU-IRU Internet Referral Unit, *Transparency Report*, (2019) p. 4, via: https://www.europol.europa.eu/publications-events/publications/eu-iru-transparency-report-2019, accessed January 11 2024.

[65]Interview, law enforcement officials, November 14 2018, emphasis added. All law enforcement interviews were undertaken together with Dr. Rocco Bellanova.

[66]Interview, Interview, law enforcement officials, 14 November 2018.

[67]Interview, law enforcement official, 7 November2018.

https://doi.org/10.1017/eis.2025.14 Published online by Cambridge University Press

the complexity of cross-matching a multitude of data points, including financial trails, GPS signals, geospatial locations, car number plates, personal information. To make such information and analytical hypotheses presentable to frontline police units (in a nationally sovereign context), the interviewee notes,

> you need to have visualisation … in the report, we were talking about geography analysis with GPs of cars, with telephony, with locations, with, a car running from one place to another, … you do a picture of the map with a point, with the dates, with hours and what you write in your report and make it visual.[68]

Indeed, 'sometimes when you have big dataset with a lot of hits, ... [a suspect] appears in this one, this one, this one, phone, … name, bank account, then it goes all over the place and then it makes a report impossible to understand'.[69] In such a case, a 'beautiful report' can be a solution,

> because we can write a sixteen pages report but then you need to [use your] brain and not to be tired and not to have your wife, children bother you on the evenings.… So you need to have visualisation and sometimes you don't have time to do it but it's very useful.[70]

The example of the beautiful report illustrates how European law enforcement understands its task in terms of the presentation, connection, and digitisation of information – not unlike the work that platforms do in the digital economy.

Transnational institutions like FATF and Europol use expressions that minimalise their own positions and represent themselves as mere facilitators. They seem to disavow power. Despite these modest self-descriptions, however, both Europol and FATF are powerful organisations in the contemporary security landscape, especially as they drive forward agendas for sharing and analysing financial and social media data in the name of countering terrorism. Like platform companies, their power is lodged in the ways in which they curate content and digitally analyse, present, and visualise data. The significance of the 'beautiful report' is that it offers particular data curations that are made readable and compelling for particular courses of action, while appealing to a mere technical and aesthetic ordering of data. Just like the connection and curation practices of social media platforms, the 'beautiful report' of the police agency does more than neutrally present datafied content that is collected or delivered by others. Instead, data are curated, selected, presented, prioritised, and analysed in ways that make particular narratives and actions plausible.

Platform security infrastructures

The platform is simultaneously an imaginary and a technology. Put differently, the imaginary of the platform, as a neutral intermediary and connector, enables and is shaped by particular technological choices and operations. As discussed above, two technological features typify platform infrastructure: first, the way in which modes of decentralised connectivity enables avoidance of or withdrawal from regulation. Second, the way in which the programmability of platforms provides the infrastructure basis on which other applications and businesses run – generating 'lock-in' effects. This section offers several empirical examples that show how contemporary security actors seek to build security infrastructures inspired by a platform model, similarly generating avoidance of regulation and lock-in effects. How do the two elements of platform infrastructure (decentralised connectivity and programmability) play out relation to security technologies? How do these technological models affect the ways in which responsibility is claimed or denied in relation to security practices?

[68]Ibid.
[69]Ibid.
[70]Ibid.

https://doi.org/10.1017/eis.2025.14 Published online by Cambridge University Press

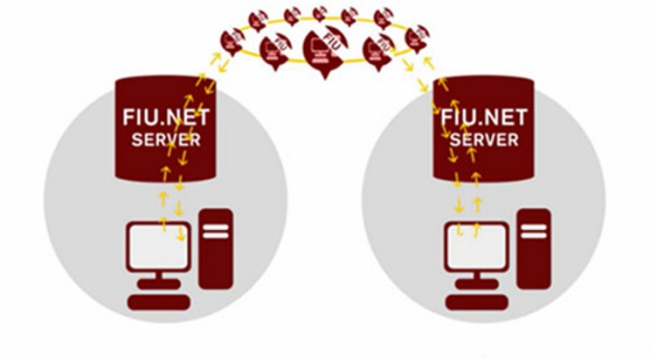


Figure 1. Still from Ma3tch Video, see: https://vimeo.com/145121509.

Consider the ways in which European Financial Intelligence Units (FIUs) exchange information transnationally.[71] Financial transaction data are particularly privacy sensitive because they have the capacity to reveal 'information about individuals' activities, purchases and geographical movements', which can be used to derive 'sexual orientation, health status, religious and political beliefs'.[72] Within the EU context, sharing financial transactions data is increasingly done through sophisticated platform infrastructures, that promise connectivity coupled with decentralised data ownership, and thus avoid the need to integrate financial databases.

An important example here is Europe's FIU.NET, which interconnects the databases of national FIUs. FIU.NET does not integrate national databases, or transfer them wholesale to a European server. Instead, it renders national databases interoperable through a hit/no hit system called Ma3tch, so that it can be known whether data on a suspect are held on the database of a sister organisation (see Figure 1). It allows the FIU investigators to 'follow the lead' of social network analysis beyond the national database, without requiring supranational integration of databases. Mat3ch technology supposedly shapes 'a virtual enterprise and information architecture without infringing upon local governance, privacy, security confidentiality'.[73] It works as a decentralised computer network that allows data requests to partner institutions without sharing personal data: through a hit/not hit system, it is possible to assess whether data about a subject are or are not held by a partner institution. As an online propaganda film of the technology puts it: 'When FIUs exchange sensitive information via FIU.net with each other, the data is only stored in the FIU net database at premises of the FIUs involved. There is no central database in Europe'.[74]

Mat3ch offers a '*decentralised information oriented architecture*' whereby 'information owners' retain 'full governance over the information they connect to the system'.[75] Through a process of layering whereby personal data are 'virtualised', the comparison, standardisation and exchange of data are enabled while 'guarantee[ing] local autonomy' and retaining 'local data

[71] Foivi Mouzakiti, 'Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive,' *New Journal of European Criminal Law,* 11:3 (2020), pp. 351–74; Lagerwaard, 'Flattening the international.'

[72] Valeria Ferrari, 'Crosshatching privacy: Financial intermediaries' data practices between law enforcement and data economy,' *European Data Protection Law Review,* 6:4 (2020), pp. 522–35 (p. 522).

[73] Paolo Balboni, Udo Kroon and Milda Mecenaite, 'Data Protection and Data Security by Design Applied to Financial Intelligence.' In *ISSE 2013 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2013 Conference*, edited by Helmut Reimer, Norbert Pohlmann and Wolfgang Schneider (Vieweg: Springer Verlag, 2013), pp. 73–86 (pp. 75–76).

[74] FIU.NET and Mat3ch, Vimeo at 00'50" to 1'06", https://vimeo.com/145121509.

[75] Udo Kroon, 'Ma3tch: Privacy AND Knowledge: Dynamic Networked Collective Intelligence,' *IEEE International Conference Big Data*, (2013), pp. 23–31 (p. 24, emphasis in original).

https://doi.org/10.1017/eis.2025.14 Published online by Cambridge University Press

storage'.[76] Mat3ch and similar technologies do not entail the creation of an integrated, transnational database at European level, as privacy watchdogs have feared of an EU-FIU. But they do enable 'virtual information integration … *without* the need to bring the information physically together'.[77]

Yet Mat3ch entails a significant acceleration of transnational data exchange, with possible governance implications. Several factors about Mat3ch technologically-enabled platformed intelligence exchange are crucial: first, it can be (near) instantaneously and thus circumvents cumbersome and time-consuming Mutual Legal Assistance (MLAT) request, that are traditionally the way in which security authorities exchange personal data. As Mat3ch filters can operate continuously and instantaneously, they facilitate exchange of personal data that is fundamentally different from the traditional, cumbersome work of the MLAT. Second, data remain decentrally stored yet they are rendered communicable – in other words, the Ma3tch technology avoids the need for an *integrated* FIU database. An integrated EU-FIU database was a dream of European integration that has been deemed politically unrealistic. However, the mode of platform security as exemplified in Ma3tch *evades* the need for a central European database, with central supranational checks and balances. In this sense, Ma3tch is an example of the way in which data infrastructure effects the avoidance of EU central privacy regulation, precisely because databases are not centrally collected and stored.

Another and final example of new security infrastructures with strong parallels to the platform economy, is provided by the ways in which private financial institutions and police authorities collaborate to CTF through novel quasi-juridical forms such as a 'Taskforce' or a 'Platform'. For example, the Dutch TF Taskforce and the British JMLIT are new organisational forms of public-private partnerships, that make it possible for police authorities to directly request information on named 'persons of interest' from financial institutions. Such collaboration takes place at the limits of law and through innovative 'techno-legal gateways'.[78] These platforms allow the proactive search of information on named 'persons of interest' who are however not necessarily suspects in a police investigation.[79] As with Mat3ch, the technical form of these platforms is different from an integrated database: it revolves around decentralised connectivity whereby bank and police databases are carefully kept separate. Queries from police are made sharable with bank personnel – sometimes in very low-tech fashion. For example, bank and police operatives may meet in person to share names and discuss files. In this manner, databases are not integrated but remain separate, while connectivity is made through interpersonal or anonymised technical means.[80] When this results in a hit, banks follow established routes of making a suspicious transaction report to the national Financial Intelligent Unit, which is the regular legal route for such reports. Police authorities would not otherwise have access to financial transactions data from private banks, unless they deposit a formal data-request within an ongoing investigation into a designated suspect, or when they are alerted through an FIU.

In sum, decentalised but interconnectable databases are emerging as a key technical form through which security practices operate. Taken together, this type of security infrastructure has major consequences for responsibility and regulatory control, just as in the AirBnB example. At

[76]Kroon, 'Ma3ch,' p. 25.

[77]Balboni, Kroon and Mecenaite, 'Data Protection and Data Security by Design,' p. 82, emphasis added.

[78]E. Esmé Bosma, *Banks as Security Actors: Countering terrorist financing at the human-technology interface*, Unpublished PhD thesis (University of Amsterdam, 2021).

[79]Nick J. Maxwell and David Artingstall, *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime,* Royal United Services Institute for Defence and Security Studies, Occasional Paper (London, 2017), https://static.rusi.org/201710_rusi_the_role_of_fisps_in_the_disruption_of_crime_maxwell_artingstall_web_4.2.pdf; Maja Dehouck and Marieke de Goede, *Public-Private Financial Information-Sharing Partnerships in the Fight Against Terrorism Financing: Mapping the Legal and Ethical Stakes,* Project CRAAFT Report, (University of Amsterdam, 2021, https://www.projectcraaft.eu/reports/new-publications-from-university-of-amsterdam.

[80]Bosma, *Banks as Security Actors*; Laurent Bonelli and Francesco Ragazzi, 'Low-tech security: Files, notes, and memos as technologies of anticipation,' *Security Dialogue,* 45:5 (2014), pp. 476–93.

https://doi.org/10.1017/eis.2025.14 Published online by Cambridge University Press

the same time, because FIU.net and Ma3tch are housed at Europol, these technologies generate specific lock-in effects that strengthen Europol's platform power.

Conclusion: Platform security and public values

This paper has argued that there is an emerging mode of platform security that, akin to platform economy, exercises power through technical connectivity while disavowing power. Media studies research has shown how public values are challenged and reworked through platforms' technical choices, programmability and (lack of) responsibilisation. Platform companies like Uber and AirBnB change whole sectors, challenge shared responsibilities for consumer protection and accessibility, and avoid the impact of regulation and taxation in – for example – urban rental markets. This 'disavowal' of ownership and responsibility over collective urban space is effected through the platform metaphor and model, that claims to be a mere information service and that operates on an infrastructural model that is typified as 'decentralised centralisation'.

Examining new practices of platform security through the lens of the platform economy brings questions of regulation and public values to the fore. If my argument is correct and the platform metaphor and model are now also shaping security practices, the question arises: how does platform security challenge public values? How does it affect existing protections, values, and responsibilities that security actors are committed to and regulated by? If we understand the platform as a metaphor and a mode of power – instead of purely as a business model – then we need to ask how the power of platform security operates and what specific governance challenges it poses.

As I have shown, platform security is typified by ambitions of 'decentralised centralisation', where regulatory initiatives and technical systems appear *not* to be centrally driven, stored, or integrated. This 'lack' of centrality poses specific governance challenges. In conclusion, we may say that platform security acts as a practice of obfuscation,[81] whereby responsibility over authoritative practices and decisions is (1) discursively disavowed and (2) technically obfuscated. First, this paper has shown several examples of how power is discursively disavowed or minimised by important transnational security institutions. If an institution minimises its role, it refuses to be held accountable in this role. In decentralised centralisation, the 'hub' of power appears to be empty. This disavowal does not just *deny* something but also *produces* something: it produces a particular arrangement of opacity whereby regulatory change is enacted without accountability or redress. Where can citizens, civil society groups, or other parties anchor objections, questions, and (juridical) responsibility, if the centre of power appears to be empty? This was the case in the ECJ case about AirBnB – with which we started this paper – and it appears also to be the case, for example, in relation to transnational security institutions like FATF. These issue important guidelines and rules concerning the combat against terrorism financing, some of which directly impact national lawmaking, bank's policies and citizen's financial inclusion. But they refer any questions about the impact of its work to national government authorities, which, in turn, refer to their obligations under international treaties and cooperation, or to the independent decisions of private sector parties.

Second, in platform security, the operation of power is *technically obfuscated*. As the empirical examples have shown, the interconnection of decentralised databases implies that there is no central data repository. This is welcomed by civil rights groups and others who are critical of centralised (EU) data storage and the dangers this might entail to privacy. Yet interoperability of databases still makes certain connectivities possible, while entailing a new arrangement of opacity. In a technical model like Mat3ch, for example, the process of matching itself is technical and anonimised. Mat3ch operates on the production of suspicion: only if an anonimised query is matched by a hit

[81] Clare Birchall, 'Introduction to 'secrecy and transparency': The politics of opacity and openness,' *Theory, Culture & Society,* 28: 7–8 (2011), pp. 7–25; Debbie Lisle, 'Failing worse? Science, security and the birth of a border technology', *European Journal of International Relations*, 24:4 (2018), pp. 887–910.

https://doi.org/10.1017/eis.2025.14 Published online by Cambridge University Press

in the partner database, can the records be shared. A shareable record, then, is one that is inherently suspect because it appears in more than one database or investigation. Yet this production of suspicion in the fact of a match is not accountable, and not even visible, to the suspect subject themselves. Because privacy rights and responsibilities remain delegated to the owner of the database (the national police authority or private company), the subject's exercise of rights remains oriented toward the individual (and decentalised) database or data owner. As such, the process of matching itself, and the inferences drawn through these technical practices, remain invisible.[82] Usually, a match can result in a follow-up action via a police authority or a private company (e.g., an investigation or an account closure). However, for the persons affected, it is not at all evident how such security action is initiated or how it could be contested. How could responsibility be anchored not in the database itself, but in the production of connectivities and suspicions? How can the lateral relations between interoperable databases be governed and rendered accountable?

In platform security, decisions and actions remain dispersed and decentralised. It identifies datasets, renders them interoperable, and generates leads. Those leads and analyses, in turn, are rerouted to national security officials and local police so that security interventions can remain national and local. However, the provenance and analytical practices of such leads often remains unknown to those who use them in the national context, as well as to those affected by the actions. It raises questions concerning rights and responsibilities – who is responsible when decisions to remove content or close accounts are wrongly targeted?

In this paper, I have shown a deep analogy between the imaginaries and infrastructures of platform economy and platform security. Like the platform economy, the EU's self-described 'information hubs' seek to connect, collate, and mediate, while minimising their own role. The paper has analysed parallels between the imaginaries and infrastructures of platform economy and the contemporary security practices of organisations like FATF and Europol, to show how practices of decentralised centralisation are crucial to both. Platform security seeks to mobilise and connect local participants, but disclaims responsibility for the content of connectivity. The 'beautiful report' produced by a law enforcement analyst, the technical legal support offered by FATF, the suspect match enabled through Mat3ch, are forms of connectivity that are rendered technical and depoliticised. They potentially have great impact on security interventions, but avoid accountability through their decentred nature. Unpacking the parallels between platform economy and platform security fosters a much-needed dialogue between media studies and critical security studies, and helps raise critical questions about the latter, and help devise new ways to anchor accountability in the connection, the match and the report.

Acknowledgements. Many thanks to all members of the FOLLOW research team, in particular Rocco Bellanova, with whom much of the fieldwork for this paper was done. The paper benefited enormously from the generous comments of two anonymous reviewers. The paper was presented at the 2023 European Studies Association in Potsdam, the Roundtable on Security/Technology at the University of Copenhagen in May 2024, and the 2025 'Platform Warfare' workshop at the University of Antwerp. It received very helpful comments from Rebecca Adler-Nissen, Jonathan Luke Austin, Stefan Elbe, Lene Hansen, Marijn Hoijtink, Jasper van der Kist, Debbie Lisle, Elke Schwarz, Mikkel Rasmussen and others.

Funding statement. This publication has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme [grant agreement No. 682317].

Prof. Dr Marieke de Goede is Professor of the Political Science at the University of Amsterdam and Dean of the Faculty of Humanities. She has published widely on counterterrorism and security practices in Europe, with a specific attention to the role of financial data. She held a Consolidator Grant of the European Research Council (ERC) with the theme: FOLLOW: Following the Money from Transaction to Trial (www.projectfollow.org). De Goede is a co-editor of *Secrecy and Methods in Security Research* (2020). De Goede is Honorary Professor at Durham University (UK).

[82] Amoore, 'Machine learning political orders.'

Cite this article: Marieke de Goede, 'Imaginaries and infrastructures of platform security', *European Journal of International Security*, 11 (2026), pp. 247–261. https://doi.org/10.1017/eis.2025.14

https://doi.org/10.1017/eis.2025.14 Published online by Cambridge University Press