MASTER THESIS

Titel der Master Thesis / Title of the Master's Thesis

„Failing Forward in Digital Europe: The Surveillance Crisis and the Role of Europol in Data Exchange and Cooperation with Private Companies“

verfasst von / submitted by

Hope Schulz LL.B.

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Advanced International Studies (M.A.I.S.)

Wien 2022 / Vienna 2022

Studienkennzahl lt. Studienblatt Postgraduate programme code as it appears on the student record sheet:	A 992 940
Universitätslehrgang lt. Studienblatt Postgraduate programme as it appears on the student record sheet:	Internationale Studien / International Studies
Betreut von / Supervisor:	Professor Patrick Müller M.A., Ph.D.

diplomatische akademie wien
Vienna School of International Studies
École des Hautes Études Internationales de Vienne

On my honour as a student of the Diplomatische Akademie Wien, I submit this work in good faith and pledge that I have neither given nor received unauthorized assistance on it. HOPE SCHULZ

Abstract

This thesis aims to broaden the scope of the failing forward theory of European integration by examining the emerging role of Europol in data exchange and technological innovation. The surveillance crisis, stemming from technological advancements and incomplete digital security policy, including the Cambridge analytica scandal, the 2015 Bataclan terror attack, the EDPS finding on Europol's breach of its mandate, and the encryption crisis are examined in relation to the triggering of the failing forward cycle in the EU security policy. This therefore aims to add to the literature not only on the failing forward theory but also to contribute to ongoing discussions on the privacy versus security debate in the context of cross-border exchange of data and the cooperation of public bodies such as Europol with private companies. Until the recent amendment of the Europol Regulation to strengthen the agency's mandate, there was a stalemate between concerns for the protection of personal data, and the operational needs of law enforcement agencies to tackle terrorism and online crime. This thesis concludes that failing forward mechanisms are both applicable and necessary in the field of digitalisation where there appears to be constant crises, and constant pressures to reform.

Abstrakt

Diese Dissertation zielt darauf ab, den Geltungsbereich der Failing-Forward-Theorie der europäischen Integration zu erweitern, indem sie die aufkommende Rolle von Europol beim Datenaustausch und bei der technologischen Innovation untersucht. Die Überwachungskrise, die auf technologische Fortschritte und eine unvollständige digitale Sicherheitspolitik zurückzuführen ist, einschließlich des Cambridge-Analytica-Skandals, der Terroranschläge von 2015, die Feststellung des EDSB zur Mandatsverletzung von Europol und die Verschlüsselungskrise werden im Zusammenhang mit der Auslösung des Versäumnisses untersucht Vorwärtszyklus in der EU-Sicherheitspolitik. Damit soll nicht nur die Literatur zur Failing-Forward-Theorie ergänzt, sondern auch ein Beitrag zu den laufenden Diskussionen über die Debatte zwischen Datenschutz und Sicherheit im Zusammenhang mit dem grenzüberschreitenden Datenaustausch und der Zusammenarbeit öffentlicher Stellen wie Europol mit privaten Unternehmen geleistet werden . Bis zur jüngsten Änderung der Europol-Verordnung zur Stärkung des Mandats der Agentur herrschte ein Patt zwischen den Bedenken hinsichtlich des Schutzes personenbezogener Daten und den operativen Anforderungen der Strafverfolgungsbehörden zur Bekämpfung von Terrorismus und Online-Kriminalität.

Table of Contents

INTRODUCTION

The EU's Data Strategy released in 2020, 'aims to make the EU a leader in a data-driven society.'[1] In many aspects of society, including in the health, environment, and business sectors, the use of data to innovate is largely being embraced. Particularly, when it comes to digital trade, there is a growing encouragement for an open international market. The EU's trade policy published in 2021, has emphasised 'supporting Europe's digital agenda is a priority for EU trade policy. The objective is to ensure a leading position for the EU in digital trade and in the area of technology, most importantly by promoting innovation.'[2] It therefore recognizes the importance of the flow of data across borders for EU companies, but does also focus on data protection and privacy as fundamental rights of EU individuals. Yet when it comes to security, and the involvement of security organisations, there is a reluctance to allow for this engagement. A data driven society has numerous implications for security organisations and how investigations, operations, and intelligence gathering are carried out.

A new era of security cooperation between law enforcement and the private sector in Europe is emerging. In the US, this engagement has been longer established, and is more prevalent in discussions about strengthening the powers on the use of data, and cooperation in private data exchanges. In 2013, the Snowden document exposed the extent of the relationships between the NSA and private companies and how many intelligence reports it generated as a result of the data collected from these companies.

The EU is at a crossroads. There are two stories to be told here. The first is one about the regulatory challenges of control and access to data. The second one is one about how law enforcement agencies need to increasingly rely on private actors. It needs to determine how it will go about the data openness movement at the same time as ensuring its security interests are maintained, and its agencies have the capacity to manage the digital demands of cyberspace. Its needs now encompass more mass collaboration with private companies, and the existing framework surrounding data

[1] "European Data Strategy," European Commission, February 19, 2020. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.
[2] "Digital Trade - Trade - European Commission." https://ec.europa.eu/trade/policy/accessing-markets/goods-and-services/digital-trade/.

sharing is not equipped to deal with it. In a previous research paper, I found that 'the current framework of cyber-policies and regulations on governmental agencies with regards to surveillance and data gathering, has actually increased the privatisation of intelligence activities through secret partnerships in the communications industry, and thus, there is a relationship between policy makers, security agencies, private companies, and individuals to be explored here.'[3] Europol as the agency 'being primed to become the centre of machine learning and AI in policing,' will be of a significant focus of this thesis, in terms of evaluating how the EU adopts new strategies for engaging with data collection, processing, and collaboration with private companies. There is a growing need to reframe the privacy versus security debate, and the way we think about and use data, if the security sector is to be able to succeed in an increasingly data-driven society.

The role and powers granted to security organisations and the treatment of personal data is an increasingly important area of study. Particularly in Europe, the attitude towards and treatment of personal data is continually having to adapt and respond to the needs of the security sector. This is seen as companies implement encryption technologies into their digital communications services, while security and intelligence agencies have a growing demand for access to these communications. Thus, increasingly, private non-state actors (such as Alphabet Inc (Google), and Meta (previously known as Facebook)), are becoming more and more relevant in international affairs. As digitalisation parallels globalisation, the flow of data across borders is becoming more significant.

Previously there has been a strained relationship between the security community and the private sector when it comes to the control of and access to data. Firstly, the finding of the European Data Protection Supervisor (EDPS) that Europol has collected a large amount of personal data unlawfully, and that it must delete it. And secondly the development of new EU legislation in the form of an amendment to the Europol Regulation (Regulation 2016/794) which would give Europol a legal basis to expand its data processing powers. These two developments highlight 'deep political divisions

[3] Hope Schulz, 'Reframing the Privacy versus Security Debate: From Operation Rubicon to the Crowd- Sourced Intelligence Agency' Submitted to the DA for Seminar: Intelligence and Diplomacy in Times of Crises

among Europe's decision-makers on the trade-offs between security and privacy'[4] as well as emphasises the relevance of the legal framework to shape the direction of the EU's attitude towards data. The current proposal to amend the Europol Regulation (Regulation 2016/794) signifies a transition in the EU's approach. It remains to be seen whether this initiative signifies a transition from secretive data collection and the privatisation of intelligence activities to an increase in the need to publicly acknowledge the need for such collaborations. In this regard it could be argued that Europol started by outsourcing and now it's becoming more and more of an actor itself. It comes at a difficult time though, as the recent scandal involving the military grade Pegasus Spyware developed by Israel's NSO group was found to have been used by various governments to gain access to encrypted data held by journalists and human rights activists. The consequent pushback against government access to data leaves a gap to examine how the EU continues to shape the role of Europol in its digital strategy.

This is a story of integration and transfer of competences which primes Europol for becoming an emerging/prominent actor in the field. The research will aim to assess the extent to which the failing forward theory of European integration can explain the current shift in the EU's approach to the handling of data in the security sector, both in terms of enhancing Europols powers and in better facilitating the cooperation between private firms and security organisations. The thesis will use a multidisciplinary approach incorporating considerations of international relations and law. It will look qualitatively at the development of the approaches taken towards data in the European Union and how this has changed over time. The legal dynamic here is explored through an analysis of the legislative and regulatory framework surrounding data exchange. There is the political and international relations aspect of cross-border collaboration, and specifically harmonisation within the EU. And there is also an element of economic factors, which frames the broader picture of the topic, as the EU moves towards open data, digital trade, and an emphasis on the digital economy. The framework will look specifically at Europol as a security organisation, and the development of its powers in the field of data collection and private collaborations. This

[4] Apostolis Fotiadis, and Daniel Howden, "A Data 'black Hole': Europol Ordered to Delete Vast Store of Personal Data." *The Guardian*. January 10, 2022. https://www.theguardian.com/world/2022/jan/10/a-data-black-hole-europol-ordered-to-delete-vast-store-of-personal-data.

will fall within the scope of analysis of the trends in the EU's data strategies and the movements towards open data and the push and pull dynamic between security and privacy. There is a need to understand the balance of power between the citizens, the private firms, and the state, in light of the potential expansion of digital surveillance and data sharing.

The thesis seeks to answer the question: to what extent mechanisms of "failing forward" have contributed to core developments in the EU's approach to the use of data in the security industry?

CHAPTER 1: Literature Review

The existing literature on the topic of data exchange and the current challenges and risks associated with it are extensive. There is an acknowledgement of an emerging need for a legal and policy framework for public private cooperation. In this regard the proposals for the EU Data Act and the Europol Regulation, provide for an emergence in literature on the topic. The gaps in the literature are found in that there is no coherent agreement on an approach to collaboration on data exchange between the public and private sector. Furthermore, discussions about privacy vs security tend to be broad and presented as mutually exclusive. On the other side of things, there is more of a focus on data exchange for economic, health, environmental purposes. In terms of EU content, generally speaking, there is often an excess of information on policies, which can be difficult to keep track of.

Published in a report by the Information Technology & Innovation Fund, Cory and Dascoli (2021) focus is primarily on economic impacts of measures relating to cross-border data flows, it provides useful insight into how policy makers should address the trade-off between concerns over data sharing with the societal and economic benefits. The authors give an overview of data localisation measures, and assess them comparatively with various countries around the world. They highlight how 'misguided data privacy and cybersecurity concerns remain common, but cyber sovereignty and censorship are newer, and in many ways, more-troubling motivations given they are

broader and more ideologically driven.'[5] They argue that trade restrictions on data limit the potential of the digital economy and refer to the use of privacy and national security concerns as a frequently used basis for implementing such restrictions. This argument will be addressed in the thesis to analyse potential for data sharing cooperation between private companies and security organisations. The article, again in its focus on economic aspects, makes recommendations for digital interoperability as a key component for global data governance, whereby the idea is that countries enact broadly similar laws and regulations, which would mean the flow of data across borders would be afforded similar levels of protection (even if countries have different legal frameworks and mechanisms for doing so).

Similarly, the World Economic Forum 2020 report rightly acknowledges that 'no single organisation has visibility over the entire problem space, making collaboration and information sharing essential.'[6] It sees information sharing as both a platform for collective resilience as well as collective action. The report acknowledges that 'the most successful information sharing models that are emerging in the global community and which can detect and disrupt cybercrime are between law enforcement and the private sector.'[7] Its discussion around public-private information sharing is limited, although it gives a brief outline of some examples of such initiatives (such as Europol's Cybercrime Centre) and does attribute the difficulties surrounding privacy and data protection concerns with creating more public-private initiatives. This source outlines the 7 key barriers to digital data sharing which, if addressed, could lead to a more effective collective security. These are, 'gaps in jurisdictions and cross-sector collaboration; Skills and capabilities; Trust and privacy; Legislation, policy and data fragmentation; Operational costs; Lack of clear incentives; and Operational, interoperability and technology barriers.'[8]

[5] Nigel Cory and Luke Dascoli, ''How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them,' ITIF, July 19,2021,https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost
[6] World Economic Forum. "Cyber Information Sharing: Building Collective Security." October 2020, 5
[7] ibid, 7
[8] ibid, 12-13

This view was echoed in (Misuraca, Gianluca, and others 2012)[9], where, in the conclusion of the report, the authors note how their scenarios 'identify the need for developing and applying ICT tools and applications that fully exploit the potential of mass collaboration and the open and participatory paradigm underpinning future technological developments and policy directions in Europe.'[10] valuable in terms of its research methodology in that it utilised a method of scenario thinking, whereby it developed 'a vision of the role of ICT research in shaping a digital European society in 2030 through four thought-provoking visionary scenarios.'[11] This notion of a scenario framework is useful in that it takes current and future challenges and foresees various directions and alternatives which the world could go in. Although conducted in 2010, the scenarios outlined in the report (open governance, leviathan governance, privatised governance, and self-service governance), offer useful insights into research design on ICT and European governance. Furthermore, it is useful to place the current state of Europe and its relationship to digitalisation, in the scenarios envisaged by the authors in 2010. This acknowledgement of mass collaboration and the application of ICT tools, is what this thesis aims to explore. Again there was little mention of the specific means of collaboration between public and private institutions, let alone in the security arena, and it is this area which the thesis aims to explore.

In 2019, the Organisation for Economic Co-operation and Development (OECD), issued a report titled 'Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies.'[12] In the report, the OECD takes a more critical perspective of the current movement towards increased access to and sharing of data. The report weighs heavily, the risks associated with the costs, intellectual property, and privacy of accessing and sharing data. It focuses more on the business and economic models of sharing data, which is of limited use for the security application and focus of this thesis. It does however, identify a so-called 'data-policy pitfall' as 'the tendency to look for one silver-bullet solution to a multidimensional

[9] Misuraca, Gianluca, and Others. "Envisioning Digital Europe 2030: Scenarios for ICT in Future Governance and Policy Modelling." *European Foresight Platform. 2012.* http://www.foresight-platform.eu/brief/efp-brief-no-194-envisioning-digital-europe-2030-scenarios-for-ict-in-future-governance-and-policy-modelling/

[10] ibid

[11] Misuraca, Gianluca, and Others. "Envisioning Digital Europe 2030: Scenarios for ICT in Future Governance and Policy Modelling." *European Foresight Platform. 2012*

[12] OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris, https://doi.org/10.1787/276aaca8-en.

problem,'[13] and goes further to acknowledge that 'flexible data-governance frameworks that take due account of the different types of data and the different context of their re-use, while doing justice to domain and cultural specificities, are crucial.'[14] This notion again validates the direction that this thesis will go in.

Also to be found in the literature, is a currently very light but growing discussion on expansion of powers for agencies in the security sector. As demonstrated by Sarah Eskens,[15] there is useful insight into some of the attitudes and opinions held by academics on the expansion of powers for Europol's data processing and collaboration with private parties. The author brings into question the conflict between Europol's legally mandated role with the new amendments being proposed by the Commission. She questions the reasoning in the explanatory memorandum, that just because Europol receives large data sets does not mean it should be made a norm that they are able to process them. The author describes concerns of oversight issues for the EDPS and of the weakening of the rule of law, when voluntary transfers of data by private parties are incentivised by Europol. The legal analysis of the implications of data transfers are valuable and form part of an important aspect of the thesis' discussion on how sharing data should be realised.

The theory of failing forward speaks to the 'incomplete nature of European integration.'[16] Although initially developed within the context of the eurozone crisis and the Economic and Monetary Union, there is room in the literature to analyse the EU's digital security sector. When it comes to existing applications of the failing forward mechanism to different policy areas, at the outset of this thesis it is recognized that, 'apart from areas like trade and competition, where EU authority is very extensive, and areas like defence and foreign policy, where it is minimal, most other policy domains the EU is engaged with…fall into the middle of the spectrum where policy

[13] OECD. "Risks and Challenges of Data Access and Sharing." In *Enhancing Access to and Sharing of Data*. OECD, 2019. https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en
[14] ibid
[15] Sarah Eskens, *New and extensive data processing powers proposed for Europol*, 2021, European Law Blog https://europeanlawblog.eu/2021/07/30/new-and-extensive-data-processing-powers-proposed-for-europol/
[16] Erik Jones, Daniel R. Kelemen, Sophie Meunier, "Failing forward? The Euro crisis and the incomplete nature of European integration." *Comparative Political Studies*, 49 no. 7, (2016) 1010–1034, https://doi.org/10.1177/0010414015617966

competences are shared between the EU and the Member States. It is in this middle terrain where we expect failing forward to be most prevalent.'[17] Literature applying the failing forward framework thus far has been done in the case of the euro crisis, of EU Migration Policy[18], of the development of Common Commercial Policy development[19], of EU Competition Policy[20], of the Economic and Monetary Union[21], the response to Covid-19[22], of citizenship rights and Brexit[23], of the rule of law[24], of the European Neighbourhood policy[25], and of the Common Security and Defense Policy[26]. The area which this thesis examines, namely Europe's digital industry and security sector is deemed, at the outset, to fall within this middle terrain. The complexities of the balance between data innovation, security, and privacy is not a strictly new dilemma, however the mechanism through which this balance is struck in the EU is incomplete, and its contribution to (whether positively or negatively) to European integration is largely unexamined within the conceptual framework. There is an incomplete policy response to the crisis of surveillance and data protection currently facing the EU. The emerging theory of failing forward within European integration theory, is one that is underexplored in the context of digital policy and strategy responses to the data and security crises in the industry which have manifested themselves over the past 6 years.

[17] Jones, Erik, R. Daniel Kelemen, and Sophie Meunier. "Failing forward? Crises and patterns of European integration." *Journal of European Public Policy* 28 no. 10 (2021): 1530, DOI: 10.1080/13501763.2021.1954068

[18] Marco Scipioni (2018) Failing forward in EU migration policy? EU integration after the 2015 asylum and migration crisis, Journal of European Public Policy, 25:9, 1357-1375, DOI: 10.1080/13501763.2017.1325920

[19] Christian Freudlsperger "Failing forward in the Common Commercial Policy? Deep trade and the perennial question of EU competence," *Journal of European Public Policy*, 28 no.10, (2021) 1650-1668, DOI: 10.1080/13501763.2021.1954059

[20] Adriaan Dierx & Fabienne Ilzkovitz "EU competition policy: an application of the failing forward framework," *Journal of European Public Policy* 28, no. 10, (2021) 1630-1649, DOI: 10.1080/13501763.2021.1954063

[21] David Howarth & Lucia Quaglia "Failing forward in Economic and Monetary Union: explaining weak Eurozone financial support mechanisms," *Journal of European Public Policy,* 28 no. 10, (2021) 1555-1572, DOI: 10.1080/13501763.2021.1954060

[22] Martin Rhodes "'Failing forward': a critique in light of covid-19," *Journal of European Public Policy*, 28, no. 10, (2021) 1537-1554, DOI: 10.1080/13501763.2021.1954067

[23] Lisa Conant (2021) "Failing backward? EU citizenship, the Court of Justice, and Brexit," *Journal of European Public Policy*, 28, no. 10, (2021), 1592-1610, DOI: 10.1080/13501763.2021.1954061

[24] Cassandra Emmons & Tommaso Pavone, "The rhetoric of inaction: failing to fail forward in the EU's rule of law crisis," *Journal of European Public Policy* 28 no. 10, (2021)1611-1629, DOI: 10.1080/13501763.2021.1954065

[25] Maryna Rabinovych, "Failing forward and EU foreign policy: the dynamics of 'integration without membership' in the Eastern Neighbourhood," *Journal of European Public Policy* 28, no. 10, (2021)1688-1705, DOI: 10.1080/13501763.2021.1954066

[26] Julian Bergmann & Patrick Müller, "Failing forward in the EU's common security and defense policy: the integration of EU crisis management," *Journal of European Public Policy* 28 no. 10, (2021)1669-1687, DOI: 10.1080/13501763.2021.1954064

Some of the initial authors of the failing forward theory, Jones, Kelemen and Meunier, from the outset themselves, questioned the merits of the failing forward approach. The two main points made by the authors, as to why the mechanism of failing forward are inefficient, pertain firstly to the limited consensus reached following the use of too many resources which 'delivers too little payoff in terms of making the world a better place.'[27] Secondly, the approach, in its reliance on generating incremental policy in response to crises, which then fails, could lead to a perception of incompetence of EU leaders which then 'undermines support for the European project.'[28] They thus consider the approach of failing forward, as one which works in the short-term rather than in the long-term.

CHAPTER 2: Background

The History of Europol

The development of Europol to become not only Europe's prime police agency but also Europe's hub for security cooperation, information exchange, and now 'the centre of machine learning and AI in policing,'[29] is one that is worthy of examination within the framework of European integration, particularly when assessing the extent to which it has elements of being a 'half-baked institution' within the failing forward theory. The European Police Office, later shortened to Europol, was established by Article K3 of the Maastricht Treaty and became fully operational in 1999 in response to a growing need to combat transnational organised crime. Although the 2001 9/11 attacks, strengthened the institutions mandate surrounding counter-terrorism, at the time many Member States, notably the United Kingdom, still favoured their national investigative authorities. Furthermore, information shared with Europol over the years, although under the guise of cooperation, continued to be of limited value. There was indeed, a 'a deep fracture…between the reiterated intentions to cooperate and the outcomes of

[27] Erik Jones, R. Daniel Kelemen and Sophie Meunier 'Is Europe failing, or is it 'failing forward'?, Washington Post, July 5, 2016 https://www.washingtonpost.com/news/monkey-cage/wp/2016/07/05/is-europe-failing-or-is-it-failing-forward/
[28] ibid
[29] Fotiadis, and Howden, "A Data 'black Hole'"

this endeavour'[30] which 'was generated to a large extent by the national security and intelligence service's failure to share information and intelligence due to various barriers, including bureaucracy-related ones.'[31] This attitude prevailed, and Europol was not fully supported by Member States until the EU Decision of 2009/371/JHA on the 6th of April 2009 which transitioned Europol into an EU agency. This also paralleled the entry into of the Lisbon Treaty which also impacted the Europol's legal and operational framework. In fact, this was the main legal framework under which the agency operated, until the 2016 Europol Regulation. The Europol Regulation then drastically changed the dynamic of how it operates with external members. As of the Europol regulation, Europol did not have the competence to enter into new cooperation agreements of its own will. Any international cooperative agreements involving the exchange of personal data would be subject to article 218 TFEU. This is significant for the discussions of this thesis, as it highlights the reforms the institution has undergone over the last two decades and the subsequent impacts these developments have had on European and security integration. Compared to its role under the EU Council Decision of 2009, the new Regulation meant that Europol was no longer 'leading the initiation, the negotiation and the conclusion of the cooperation agreements,'[32] and the exchange of personal data whereas the Council and the EU Commission's role in this regard was strengthened. If one were to place this development on the continuum of intergovernmentalism and supranationalism, 'one can argue that the application of the Europol Regulation has led to a further move towards more supranationalism in Europol's external relations.'[33] This is found in the new design of the institution and in its legal basis. This being said, there still remain aspects of intergovernmentalism, as the institution still finds itself at the hands of Member States, though this has arguably 'been invoked to describe European integration since Maastricht."[34] Ultimately, the nature of Europol's role has shifted from one that was primarily focused on data

[30] Ruxandra L. Bosilca, "Europol and Counter Terrorism Intelligence Sharing." Europolity : Continuity and Change in European Governance 7, no. 1 (2013), 7
[31] ibid
[32] Sarah Léonard, and Christian Kaunert. "The Development of Europol's External Relations: Towards Supranationalism?" *Maastricht Journal of European and Comparative Law* 28, no. 2 (April 2021): 243 https://doi.org/10.1177/1023263X211005162.
[33] ibid, 241
[34] Kerttuli Lingenfelter, and Samuli Miettinen. "Obstacles to Supranational Operational Police Powers in the European Union: Europol Reform and the Construction of Trust between National Police Authorities." *Maastricht Journal of European and Comparative Law* 28, no. 2 (April 2021): 191 https://doi.org/10.1177/1023263X211005160

collection, to one of ‘a more integrated data management between public and private actors.’[35]

The first of Europol’s six strategic priorities is to ‘be the EU criminal information hub.’[36] Though initially, it could be said that Europol focused mainly on collecting data, over the years, as globalisation and advancements in technology and innovation have placed increased pressures on security services to progress alongside such advancements, it seems that now it has evolved to connecting data. There is a growing desire from within the institution to advance its ‘information management architecture and rapidly embrac[e] new methods and technologies as they become available.’[37] Furthermore this transition from processing to producing knowledge and information is what contributed to the transition from a ‘from a systems-based organisation to a specialised law enforcement service provider.’[38] This falls within the emphasis of strategic priority 3 of becoming a platform for European policing solutions. As it takes on the role of brokering law enforcement knowledge, Europol aims to connect Member States through its hub, and in doing so strengthen both the EU standards of analysis in general and analytical capabilities for law enforcement specifically. They further highlight the aim to provide the products of their analysis including actionable intelligence in a manner in which is both recognisable and usable across the jurisdictions of Member States.[39]

Data Processing

The collection, processing, retention, use, and exchange of data, involves numerous stages, procedures and actors. This is particularly the case in the security sector, where a secure system for information exchange is crucial to the trust and cooperation of Member States, third countries, and other parties involved. It is important to distinguish between data and personal data. Personal data pertains to information

[35] Ethem Ilbiz & Christian Kaunert “Europol and cybercrime: Europol’s sharing decryption platform,” *Journal of Contemporary European Studies*, (November 2021): 2 DOI: 10.1080/14782804.2021.1995707
[36] “Our Thinking,” Europol, https://www.europol.europa.eu/about-europol/our-thinking
[37] ibid
[38] ibid
[39] ibid

which relates to an identifiable person either directly or indirectly.[40] Non-personal data, is thus any information which does not relate to a data subject. It is important to note that Europol may only collect and process personal data it receives from EU bodies, third country authorities, international organisations, and private parties, if it is necessary and proportionate for it to do so to fulfill the legitimate performance of its tasks.[41] Collecting and processing personal data is one of Europol's core functions. The implementation of GDPR and of the 2016 Europol Regulation sparked a significant change in the data industry and in the protection of data. Here began the shift towards technology neutral legislation and towards a so-called 'privacy by design'[42] approach. For Europol for instance, there was then no more reference to the specific information systems and how each are regulated, but instead there is an importance placed on the purposes for which personal data are processed. Under the 2016 Europol Regulation these purposes are: '(i) cross-checking aimed at identifying connections or relevant links between information; (ii) analyses of a strategic or thematic nature; (iii) operational analysis; and, (iv) facilitating the exchange of information.'[43] There was thus a more holistic approach taken, where the purposes of data collection also align with the forms of analysis used by Europol: strategic analysis, where 'the overall priorities can be distinguished and justified;'[44] thematic analysis, where 'specific crime areas cases and approaches can be identified;'[45] and operational analysis, where 'concrete investigations and operations will be conducted.'[46]

The Role and Competence of Different EU Actors

The exchange of data involves many of Europol's various stakeholders. These include, the national law enforcement agencies of Member States, other EU institutions and agencies, international organisations, non-EU countries, and various parties within the private sector. It is also important to recognise and distinguish between European countries, EU Member States, Schengen Associated Countries, and third countries.

[40] Europol Regulation, Art 2(h-i)
[41] Europol Regulation, Art 23(5)
[42] Europol Regulation, Explanatory Memorandum, p. 7
[43] Europol Regulation, Article 17
[44] "Processing of Personal Data," Europol, https://www.europol.europa.eu/processing-of-personal-data
[45] ibid
[46] ibid

With EU Member States for example, each law enforcement agency has a dedicated unit (Europol National Unit) to liaise with various authorities in the country and with Europol. This being said, there are numerous non-EU countries with liaison officers at Europol.[47]

It is important to note that although Europol enters into partnerships and agreements which take various forms, overall there are two main types of cooperative agreements which Europol can have with non-EU members and institutions: operational and strategic. Whilst operational agreements can entail the exchange of information including personal data, strategic agreements are limited to exchanging general intelligence and technical and strategic knowledge. There are currently 20 operational agreements in place with non-EU European nations as well as with Australia, Canada and the US, and with Eurojust, Frontex, and Interpol.[48] Europol has 13 strategic agreements of which are in place with Brazil, China, Russia (currently suspended), Turkey, the United Arab Emirates and the remaining 8 are with the European Central Bank, the European Commission, the European Centre for Disease Prevention and Control, the EU Agency for Law Enforcement Training, the EU Agency for Network and Information Security, the EU Intellectual Property Office, the UN Office on Drugs and Crime, and the World Customs Organisation.[49] Europol maintains three main channels for communication: the Secure Information Exchange Network Application (SIENA), the Europol Information System (EIS), and the European Platform for Experts (EPE). It is through the SIENA system, which Europol, the liaison officers from EU Member States, non-EU Member States, and law enforcement agencies, communicate and exchange both operational and strategic information and intelligence. Both the strategic and operational component of the analysis of the information communicated via SIENA is supported by Europol's Analysis System (EAS) which produces 4 products of strategic analysis: Serious and Organised Crime Threat Assessment (SOCTA), Internet Organised Crime Threat Assessment (IOCTA), EU Terrorism Situation and Trend Report (TE-SAT), early warning notifications.[50]

[47] "Partners and Collaboration," Europol, https://www.europol.europa.eu/partners-collaboration
[48] "Operational Agreements," Europol, https://www.europol.europa.eu/partners-collaboration/agreements/operational-agreements
[49] "Strategic Arrangements," Europol, https://www.europol.europa.eu/partners-collaboration/agreements/strategic-agreements
[50] "Strategic Analysis," Europol, https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/strategic-analysis

These products allow decision makers to identify priorities to which law enforcement officers can tailor operational work on a national, regional and local scale.[51]

Part of Europol's role, as outlined by its Operational and Analysis Centre (OAC), is to be the 'single point of contact for information sharing within the law enforcement community as well as the European Union.'[52] When one speaks of Europol as the hub of information exchange, it is at the Operational Centre, where there is a continuous exchange of information and intelligence by Member States and third parties, and where the data which is sent and received is controlled for quality.[53] It processes and analyses large volumes of operational information and produces analytical reports, threat assessments, intelligence and warning notifications, for Member States and third parties.

The European Union Agency for Cybersecurity (ENISA) was established by the Parliament and Council's Regulation (EU) 2019/881. It aims to prevent and address network and information security in cyberspace, by contributing to 'EU cyber policy, enhanc[ing] the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperat[ing] with Member States and EU bodies, and help[ing] Europe prepare for the cyber challenges.'[54] Though its role in information exchange was not recognised in the 2016 Europol Regulation, in the amendment to the Regulation, it is mandated that Europol will specifically cooperate with ENISA in the area of information exchange and analysis (in addition to the Union bodies and OLAF with whom it is already mandated to cooperate with). This signifies a response to the increase in multi-jurisdictional cyberattacks on both public and private entities both within and outside of the Union.

[51] ibid
[52] "Operational and Analysis Centre," Europol https://www.europol.europa.eu/about-europol/operational-and-analysis-centre
[53] ibid
[54] 'About ENISA - The European Union Agency for Cybersecurity,' ENISA https://www.enisa.europa.eu/about-enisa

The Role of Private Parties & Data Exchange

The 2016 Europol Regulations defines private parties as 'entities and bodies established under the law of a Member State or third country, in particular companies and firms, business associations, non-profit organisations.'[55] Already in the Regulation, it was acknowledged that 'since companies, firms, business associations, non-governmental organisations and other private parties hold expertise and information of direct relevance to the prevention and combating of serious crime and terrorism, Europol should also be able to exchange such information with private parties.'[56] However, under Article 26, Europol may only process personal data it receives from private parties via ENU's, and may not of its own accord, contact private parties to request personal data to be sent to them.[57] Europol receiving data from a private party via an intermediary is considered the most traditional method of data exchange.[58] This is the case because when private parties share data with national law enforcement agencies, it is typically, because they are under the obligation to respond to requests made for criminal investigations. Although, 'no statistical data are collected on the matter, it seems that large volumes of personal data are shared by private parties with national LEAs.'[59] The law enforcement agencies may only then transfer this data to ENUs which may then transfer it to Europol. This is an issue because, 'only a fraction of the personal data shared by the private parties are transferred further from the LEAs to the ENUs'[60] and similarly from ENU's to Europol. This is deemed to be the result of a lack of legal basis and competence to act on it.[61] The fact that the data has to go from private parties to law enforcement agencies to ENUs and then to Europol also creates issues of time and the speed of such data transfers. Not only this but if personal data is sent directly from private parties to Europol, Europol must send back to the ENU, who must send it to the LEA, who can then resubmit the personal data back to Europol through the ENU. This issue of resubmission creates both a significant extent of missed opportunities for Europol to

[55] Europol Regulation, Art 2(f)
[56] Europol Regulation, para 30
[57] Europol Regulation, Art 26(9)
[58] Milieu, "Study on the practice of direct exchanges of personal data between Europol and private parties," Final Report, HOME/2018/ISFP/FW/EVAL/0077, September 2020, 8
[59] ibid
[60] ibid
[61] ibid

receive data from private parties which would be of operational need. It is also an indication of some of the issues which might be hindering the effectiveness and functioning of the system.[62]

CHAPTER 3: The Failing Forward Theory: Observable Mechanisms

Crisis-led European integration is becoming an increasing focus within the theories of European integration. It is sometimes perceived that the European Union is constantly in crisis and in constant need of reform to keep the Union from disintegrating. Jean Monnet wrote in his Memoirs in 1976 that 'Europe will be forged in crises and will be the sum of the solutions adopted for those crises.'

In the failing forward mechanism of European integration there are three main processes which take place. First, there is a significant crisis or external event (or several) which leads to the reassessment of existing arrangements and pressure to reform them alongside intergovernmental bargaining over the scope of such innovations.[63] Second, there are functional interdependencies and pressures, supranational entrepreneurship and experiential learning emanating from such policy reassessment.[64] Third, there is deeper integration and progress, but it is not complete and intergovernmental constraints make it prone to future failures.[65] Thus this is a cyclical mechanism wherein failing forward manifests itself initially, where the, 'lowest common denominator intergovernmental bargains [leads] to the creation of incomplete institutions, which in turn sowed the seeds of future crises, which then propelled deeper integration through reformed but still incomplete institutions – thus setting the stage for the process to move integration forward.'[66] Ultimately, the main conditions for failing forward are suggested as follows: 'the intensity of the crisis, the existing competence of European institutions, and the costs of unwinding European arrangements in order to pursue national solutions.'[67]

[62] ibid
[63] Bergmann & Müller "Failing forward," 1674
[64] ibid
[65] ibid
[66] Jones, Kelemen, and Meunier. "Failing forward?" (2021), 1519
[67] ibid, 1525

Another clarification made throughout the development of the theoretical framework, is the meaning of 'failing' and 'forward'. Failing could mean a policy does not achieve the objectives or attain its goal but it could also be a case of a policy that was working (or appeared to be working) breaks down.[68] Generally speaking, 'sometimes that failure results from dynamics unleashed by the policy itself; sometimes it results from a recurrence of problems that policymakers could have addressed in their initial agreement but chose not to because doing so would be too controversial.'[69] Overall it involves deeper integration through increased authority on the EU level, whether this is in new policy areas, or in areas of already existing competence. Where institutions are deemed to be incomplete, it can be seen as a cause for policy failure and thus it is the bolstering of such institutions which can propel integration in a given area of EU competence.

So, if failing forward takes place within the context of the surveillance crisis and the reformation of Europol the following dynamics should be observed. Firstly, that lowest common denominator bargains have led Europol to become an incomplete institution in relation to what it was set out to achieve by Member States. Secondly, that it is perceived that the incomplete structure of Europol will prove inadequate. Thirdly, that this will generate functional spillovers which spark future crises. Lastly, that this will create more pressure to further reform and thus the cycle repeats itself. Along the way there should also be policy feedback and experiential learning to identify the institutional shortcomings. [70]

CHAPTER 4: Failing Forward in Digital Europe? Application of Failing Forward Mechanisms

Chapter 3 highlighted the main observable steps of the failing forward mechanism. In this chapter, the role of failing forward mechanisms will be established in the context of Digital Europe.

[68] ibid
[69] Ibid, 1523
[70] Bergmann & Müller "Failing forward," 1682

In the digital decade, it seems as though the nature of the crisis-induced integrative reforms are increasingly responding to numerous multi-faceted crises of varying intensities. As these issues have emerged, and not been adequately addressed thus far, so too have the pressures to upgrade Europol. As part of the EU's Third Progress Report on the EU Security Union Strategy, among the emphasis on enhanced cross-border police cooperation, it was highlighted that 'swift agreement on the proposal to amend the Europol regulation would allow Europol to better support Member States in fighting organised crime and terrorism.'[71] In the explanatory memorandum of the proposal to amend the Europol Regulation, several key points and references were made. There was initially an acknowledgement of the changing security landscape in which one can observe a digital transformation with new technological capabilities at the disposal of criminals. This falls within the realms of globalisation, and the increasing 'inter-connectivity and blurring of the boundaries between the physical and digital world.'[72] It then acknowledges the Covid-19 crisis, as one which has added to the pressures facing security in the Union though the observable implications will likely only be seen in the mid-long term. It also states in the memorandum, that the new threat environment changes the extent of support that Member States expect from Europol 'in a way that was not foreseeable when the co-legislators negotiated the current Europol mandate.'[73]

On 4th May 2022, MEPs in the European Parliament voted 480 in favour, 143 against, 20 abstaining on the proposed reform of the Europol Regulation which was negotiated by the Council and the Parliament in February. This process began when 'following calls from the Council of the EU, as well as the European Parliament…the European Commission announced a legislative initiative in its 2020 work programme to strengthen the [Europol's] mandate…[which] was also included in the new EU security union strategy of July 2020.'[74]

[71]COM(2021) 799 final, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL 'on the Third Progress Report on the implementation of the EU Security Union Strategy' 8.12.2021, 17
[72] Proposal for a: REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, para 1
[73] ibid
[74] Sofija Voronova, "Strengthening Europol's Mandate" European Parliamentary Research Service, March 2022, 2

The fact that the Europol Regulation is being reformed so soon after its initial adoption in 2017, signifies a process within the failing forward framework. The initial regulation, though a substantial leap forward from the 2009 Council Decision, was incomplete. The development of the powers proposed to be given to Europol, indicate integration out of a crisis. Moving from police cooperation when needed to police cooperation by default.

The first condition for failing forward to take place is about the intensity of the crisis As outlined by Jones, Kelemen and Meunier, 'all things being equal, the failing forward dynamic is more likely to take place depending upon the extent of the policy crisis generated by the 'failure'... .'[75] To address the issue of how integration out of a crisis can explain the developments in the role of Europol and the development in the regulation of data, one first needs to examine what the crises in the context of EU digital and data strategies have been. Furthermore, Jones, Kelemen, and Meunier, established the following attributes of a crisis in the context of failing forward: firstly, that the crisis is all encompassing in that it affects many Member States;[76] secondly, that the crisis is unfamiliar, to the extent that European leaders deviate from their conventional ways of approaching problems 'and into the realms of Knightian uncertainty;'[77] and lastly that the crisis is perceived to pose an existential threat to the existing EU institutional arrangements and the survival of the Union itself.[78]

First there was the Cambridge Analytica scandal, where approximately 90 million Facebook users had their personal data harvested without their knowledge and consent by Cambridge Analytica. This data was then used to target users with political campaigns at the time of the US presidential election and Brexit in 2016. This was a major scandal which exposed deep flaws in the data privacy framework. This preceded the entry into force of the General Data Protection Regulation (GDPR) which enforces strict collection and processing regulations of personal and sensitive data, the recognition of data subjects and controllers and third parties, as well as notification procedures and punishments for data breaches. Although the GDPR, upon its

[75] Jones, Kelemen, and Meunier. "Failing forward?" (2021), 1525
[76] ibid, 1526
[77] ibid
[78] ibid

enforcement into Union law, was widely seen as the gold standard for data protection, recent developments have indicated Europe is in a surveillance crisis. The threats posed to security and data privacy have continued to test the effectiveness and resiliency of the EU's approach to data, public-private cooperation, and cross-border data exchange. This crisis has prompted a shift in attitude and a reform of the use of data and the role of Europol within the industry. This new wave of digital policy and the increase of powers for Europol indicates a theory of integration through crisis, and of failing forward. In this digital security sector, measures to address the crisis of surveillance thus far have been incomplete. In this regard, 'the EU appears to "fail forward"; again and again responding to the failures of incremental reforms by taking new steps to expand the scope and intensity of integration.'[79]

Terror Attacks

A key crisis for information and data exchange occurred when the Paris terror attacks in November 2015 where 130 people were killed and hundreds more injured.[80] This attack brought to light an so-called intelligence black hole in Europe resulting from a reluctance to share data. At the time of the attacks, 'only half of the European Union's 28 countries participated in a formal information exchange among member nations and third-party organisations and countries through Europol.'[81] Since the Paris attacks however, the apparent failure of EU security cooperation led to increasing calls for Europol to be able to harvest more data, and for more Member States to engage in cross border data exchange. It signified a shift from secrecy and mistrust when it comes to sharing terrorism information towards a broader and deepter integration of information exchange, counter terrorism and security policy. Ultimately, integration in the digital age, and when it comes to the handling of personal data, and exchange across borders is based on trust. And it is through Europol, that this trust and deeper integration is being fostered. In considering the above listed attributes to a crisis (as outlined by Jones et al) a couple of things can be noted about the terror attacks as contributing to the surveillance crisis. First, it can be determined that the these attacks

[79]Jones, Kelemen, & Meunier, S. "Failing Forward?" (2016), 1012
[80] BBC News, 'Paris attacks: What happened on the night', 9 December 2015, https://www.bbc.com/news/world-europe-34818994
[81] Giulia Paravanci, 'Paris attacks prompt EU to share secrets', POLITICO, January 20, 2016, https://www.politico.eu/article/paris-attacks-prompt-share-secrets-eu-security-forces-eurodac-schengen-information-system-terrorism-isis-isil-islamic-state-bataclan/

did affect many Member States as it concerned the cross border movements of terrorists, and the information (or lack thereof) exchanged between agencies. On the second attribute of unfamiliarity, this is not necessarily the case with these terror attacks, as attacks of this nature have of course occurred in the past. However, although the head of Europol at the time Rob Wainwright acknowledged that he had 'been talking with people like me for 10 years about improving information sharing, so it's not a new idea or concept for [him]...but this is the first time where [he] can remember it becoming a mainstream issue.'[82] Thus EU leaders were now pushed to engage with the matter on a newer, unprecedented level, therefore arguably fulfilling the second criteria to a certain degree. The last aspect of an existential threat to the survival of the Union or of particular institutional arrangements is difficult to apply here. It could be said that the November 2015 terror attack was one which signified the failings of the current framework for security cooperation and information sharing to the extent that, the head of Interpol at the time Jürgen Stock, called it a 'decisive stage in the fight against terrorism.'[83] Following on from the attack, on November 20th (7 days after the attack), the EU's justice and interior ministers held an emergency meeting in which it was decided to connect both Europol's regional criminal database as well as the databases which police on the borders of the Schengen zone, to the Schengen Information System.[84] Prior to the attack, these two systems were not being sufficiently cross-checked. Ultimately the Bataclan terror attack, was encompassing, to a certain extent unfamiliar, and overall, demonstrated an existential threat to the trust within the Union.

EDPS Case

Following an initial inquiry from 2019, on January 3rd 2022, in an unprecedented ruling, the European Data Protection Supervisor, determined that Europol was required to delete large data sets on individuals with no links to criminal activity (a data subject categorisation for data retention) for periods longer than 6 months which is what its current mandate had allowed for. The data sets were collected from national authorities over six years, in a series of data dumps from various criminal investigations, and 'among the quadrillions of bytes held are sensitive data on at least

[82] ibid
[83] ibid
[84] ibid

a quarter of a million current or former terror and serious crime suspects and a multitude of other people with whom they came into contact.'[85]

The case of the EDPS demanding Europol delete certain large data sets, was arguably what specifically triggered the move to revisit the Europol Regulation and use it to find solutions to issues accumulated over the years. It was actually a development which came up alongside the discussions of reform of the Europol mandate. Although the EDPS had found that Europol had breached the standards set out in its mandate and requested that they come up with an action plan to mitigate the concerns for data protection raised in the findings, the action plan produced, did instead called on the Commission to revise their mandate so as to allow them to continue their current practices. The discussions which followed then did not necessarily favour the stricter data retention but rather favoured giving Europol more powers to handle data, longer retention periods to process data, and capabilities to cooperate in better data exchange with private companies. The Commission viewed the EDPS's findings as providing a unique opportunity to address Europol's legal structure. This was a crisis which demonstrated not only a tension between the EDPS and Europol but rather, and more importantly, a disconnect, in the entire framework. In consideration of the three main attributable aspects of a crisis as outlined by Jones et al, the following can be said about the EDPS case. This case concerns the cooperation of Europol with Member States, and thus the practices of the organisation and the extent to which they are affected by decisions taken by the EDPS are indeed encompassing. Equally, the manner in which the agency collects and processes the data of citizens, spans across the whole Union, and all Member States have an interest in the developments of data use and data protection. This case itself is to a great extent unprecedented, as Europol has never before been faced with having access to and making sense of such large complex data sets. It has also never before been as reliant on such data sets to assist national law enforcement agencies in their criminal investigations as well as cross-border cooperation on the exchange of information. The case also brought to the forefront, discussions on data protection and privacy, and the question of whether the

[85] Apostolis Fotiadis, and Daniel Howden, "A Data 'black Hole': Europol Ordered to Delete Vast Store of Personal Data." *The Guardian*. January 10, 2022. https://www.theguardian.com/world/2022/jan/10/a-data-black-hole-europol-ordered-to-delete-vast-store-of-personal-data.

direction of Europol towards a more AI-based and data-driven model of policing, is the best way forward. The findings of the EDPS with the response of Europol, various lawmakers, and the European Parliament, with no clear-cut solution has meant European leaders have had to think about models of law enforcement and cross-border cooperation in an unconventional way.

The Encryption Crisis

In an increasingly digital-reliant society, where communication technologies are continually advancing, an encryption crisis has ensued. Encryption is the process by which information becomes encoded, and presented as random data, to conceal the original text so that it is only accessible to the person who has the decryption key.[86] It was developed as the solution to preventing malicious actors from gaining unauthorised access to the private data of both individuals and states in cyberspace. However, the increased protection from cyberthreats also means there are complications to the access to data which is linked to criminal activity as law enforcement agencies encounter issues with collecting evidence from devices and networks which have been encrypted.[87] Encryption involves a trade-off between privacy and security on the one hand and law enforcement on the other. This conflicting perception of encryption has led to a debate within the EU on how to move forward and address challenges created by technology, with technological solutions.[88] A significant challenge to be addressed is the extent to which law enforcement agencies should be given special back-door access to encrypted networks and under what conditions.

There have already been instances where there have been public demands for access to encrypted communications, notably in October 2020 by the United States, the UK,

[86] Maria Koomen, "The Encryption Debate in the European Union" Carnegie Endowment for International Peace,
May 30, 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-european-union-pub-79220

[87]Ethem Ilbiz & Christian Kaunert, "Europol and cybercrime: Europol's sharing decryption platform," *Journal of Contemporary European Studies*, (November 2021) DOI: 10.1080/14782804.2021.1995707, 1

[88] "EU Internet Forum Ministerial : Towards a Coordinated Response to Curbing Terrorist and Child Sexual Abuse Content on the Internet," European Commission, January 26, 2021, https://ec.europa.eu/home-affairs/news/eu-internet-forum-ministerial-towards-coordinated-response-curbing-terrorist-and-child-sexual_en

Australia, New Zealand, Canada, India, and Japan, who released a joint international statement on 'End-to-End Encryption and Public Safety,'[89] emphasising collaboration between governments and tech companies. In December 2020, Europol launched its project of innovating a decryption platform together with the European Commission's Joint Research Centre. The project aimed to provide Europol and national law enforcement authorities with the ability to decrypt information gathered (lawfully) from criminal investigations. In the area of encryption, the failing forward mechanism is effective. The crisis, involves all Member States, it is unfamiliar to EU leaders, requiring them to come up with unconventional solutions, is perceived as a significant threat to the Union and its institutional arrangements in the domain of cyberspace; The competences to deal with encryption is shared between national law enforcement agencies and EU bodies, but the financial and technical capacities, as well as the participation of private decryption companies vary between Member States, which makes an EU-level approach a favourable and desirable solution for all Member States.[90] Over the years, the stalemate between the privacy rights and risks of weakening the system of encryption, has led the discussion between Member States on the option of giving law enforcement agencies back-door access to encrypted communication networks, being shelved. Instead, and in favour of a more innovative and integrative approach on the EU-level as opposed to the national one, 'EU member states agreed on enhancing Europol's decryption capabilities to support national authorities,'[91] with the launch of the decryption platform operated by Europol's European Cybercrime Centre (EC3). This, in the absence of competent decryption providers employed in-house in law enforcement agencies, and in the absence of the necessary financial resources, the more sustainable solution found in the form of the EC3 decryption platform, reduces the outsource of services to private companies and the related trust issues for national authorities, whilst building trust and fostering European integration. It is precisely this encryption crisis, and the subsequent shift towards using Europol as a hub for innovation and technical solutions with the launch of the decryption platform, which paved the way for more substantive discussions on strengthening Europol's mandate and providing with them with a more comprehensive

[89] "International Statement: End-To-End Encryption and Public Safety" The United States Department of Justice, October 11, 2020, https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety
[90] Ilbiz & Kaunert, "Europol and cybercrime", 2
[91] ibid

authority and legal basis to 'integrate data management between public and private actors.'[92]

Second Condition: Existing Competences

The second condition of the failing forward framework pertains to the existing competences of EU institutions. Indeed, it is suggested that, 'all things being equal, the failing forward dynamic is more likely to take place depending upon…. the degree to which EU institutions already hold competence in the area in question (and so perceive the crisis as an opportunity to push integration 'forward').'[93]

In this case of course, a mandate for Europol and the regulation of its activities with regards to their use and collection of data already exists. Thus, there is already an established area of competency here. What needs to be examined here, is the extent to which the above-mentioned crises have been perceived as an opportunity to push integration forward. The discussions around the role of Europol, and data processing powers, fall within a deeper discussion of a wide spread data-driven approach within the Union. The issues raised by the terror attacks, the EDPS findings, the Encryption crises, as well as overall dependencies on technology and data to combat crime and terrorism, has presented EU leaders with a difficult decision. To further integrate their technology and security arrangements, or to disintegrate them in favour of the protection of data and the privacy of individuals. On the one hand there are lawmakers in the European Parliament such as leftist MEP Clare Daly who, in response to the EDPS findings stated that, 'the admonishment of Europol by the EDPS is extremely serious, and Europol's Action Plan in response is inadequate, but the problems with this data-driven approach go much deeper,'[94] expressing concern for the discriminatory consequences of AI-based policing and machine-learning. This view is similarly expressed by those in the legal profession and human rights and privacy activists who suggest that now is the time to protect fundamental human rights and restore the rule of law. On the other hand, the crises which have surrounded EU's

[92] ibid
[93] Jones, Kelemen, and Meunier "Failing forward?" (2021), 1525
[94]Samuel Stolton, "Europol on defensive as concerns raised over 'illegal' Big Data tactics," *EURACTIV*, February 2, 2021, https://www.euractiv.com/section/digital/news/europol-on-defensive-as-concerns-raised-over-illegal-big-data-tactics/

security sector and digital industry, have led to increasing calls to take this as an opportunity to bolster Europol's activities and bring the EU forward in digital innovation and cooperation. Indeed the amendment to the Europol Regulation and increasing its mandate was seen by the Commission as falling 'under the Promoting our European way of life priority.'[95] In October 2020, the European Parliament, not only stressed the added value of Europol but also argued for a focus on strengthening the agency's core tasks.[96] Moreover, it highlighted that mechanisms to exchange information with third countries must be rendered more effective, thus reemphasising that this competence already exists for Europol but it is not functioning as effectively as it could and should be. As mentioned in Chapter 2, the 2016 Europol Regulation prohibits Europol from directly contacting private companies in order to retrieve personal data. Europol may only receive personal data from private companies if the data is received via either, a national authority, a third country or international organisation with an existing cooperation agreement prior to May 2017 in line with Article 23 of Decision 2009/371/JHA, or a third country or international organisation authority subject to an adequacy decision.[97] The problem is that private parties such as online service providers like Meta (formerly Facebook), tend to hold personal data which are subject to different national jurisdictions both within and outside of the EU. Subsequently, although this data may be of relevance for Europol investigations, because there is personal data that falls within the competence of multiple jurisdictions, it is not easily attributable, which leads to the difficulties of Member States to effectively analyse data that would be of operational need. In this domain of data and information exchange, national authorities are given too much competence where they are unable to operate as effectively as Europol. Europol is much better equipped to deal with the analysis of multi-jurisdictional and non-attributable data sets, and to manage the exchange of data with private parties in various jurisdictions, than national authorities are.[98] Equally private parties themselves would require more assistance as it is often a challenge for them to manage multi-jurisdictional requests for data. Whilst national authorities lack the time and technological resources to process large data sets effectively, Europol lacks the legal framework. Thus, with the new amendment to the Europol Regulation,

[95] Sofia Voronova, "Strengthening Europol's Mandate" European Parliamentary Research Service, March 2022, 5
[96] ibid, 4
[97] Europol Regulation, Art 26(1)
[98] Voronova, "Strengthening Europol's Mandate" 5

there is an ambition to solve the multi-jurisdictional challenges faced by private parties, who are becoming increasingly important actors in the field of counter-terrorism and organised crime, by making Europol a 'single point of contact for private parties who decide to lawfully and voluntarily share data sets with competent authorities of Member States.'[99] The concept of voluntary data sharing by private parties to Europol relevant to terrorism and serious crime, as expressed in the new mandate, needs to be highlighted as it goes against traditional perceptions of data exchange and as such is perhaps part of the unconventional ideas as understood within the failing forward mechanisms drawn up to address the surveillance crisis. Policy feedback and experiential learning of relevant stakeholders in the data exchange process, highlighted an increased willingness of private parties such as online service providers to take their own initiative in sharing personal data with Europol.[100] It was this demonstrated willingness which prompted the idea of making Europol a single point of contact for private parties.

Experiential Learning and Policy Feedback: between 2016 Europol Regulation and the amended 2022 Regulation

There was and still is a gap between the data exchange and cooperation framework provided to Europol within its mandate, and the policy objective of investigating and prosecuting crime in the digital age. Relevant stakeholders have arguably played a significant role in generating policy feedback leading to the latest Europol Regulation. The report commissioned by the EU Commission's Directorate-Generate for Migration and Home Affairs (DG HOME) on the 'study on the practice of direct exchanges of personal data between Europol and private parties,'[101] in September 2020, led to the proposal of several solutions to the current challenges being faced. The report covered consultations with representatives from DG HOME, Europol, Europol's National Units, national law enforcement agencies, various contact points and authorities from international organizations or third countries, national internet referral units, national data protection units, and private parties, covering all EU Member States (including

[99] Regulation Amending Regulation (EU) 2016/794, (para 34)
[100] Milieu, "Study on the practice of direct exchanges of personal data between Europol and private parties," Final Report, HOME/2018/ISFP/FW/EVAL/0077, September 2020,
[101] ibid

the UK). Following on from these consultations, the following options were suggested as potential solutions. Firstly, amending the Europol Regulation to strengthen Europol's capacity for direct data exchange with private parties and allowing them to process the data for analytical purposes. Secondly, to amend the regulatory frameworks on national and EU levels, so as to expand the grounds upon which private parties are able to share personal data with law enforcement agencies. Thirdly, to allow the exchange of personal data amongst private parties themselves through an established platform with more intensive dialogues between private parties and law enforcement agencies. Fourthly, to designate individuals within private parties whose role it is to coordinate personal data exchanges with national law enforcement agencies. Lastly, to raise awareness of the current system in place to reinforce its use by stakeholders.

There were in fact, several calls for amending the Europol Regulation prior to the draft proposal published in December 2020. In December of 2019, the Council of the EU, in its Conclusions on Europol's cooperation with private parties report, not only acknowledged, 'the urgent operational need for Europol to request and receive data directly from private parties'[102] but also called on the Commission to consider adapting the schedule of review of the Europol Regulation which, under Article 68 of the Europol Regulation, should take place every 5 years. The call comes in light of 'the need for European law enforcement to address ongoing technological developments.'[103] Following on from this in July of 2020, the European Parliament also called for reinforcing Europol's mandate to incorporate capabilities 'to request the initiation of cross-border investigations'[104] which particularly in the case of attacks against journalists and whistleblowers, 'should be a priority.'[105] The acknowledgement of such pressing operational needs, led to further calls from the co-legislators of the mandate, as well as a legislative initiative of the 2020 Commission Work Programme, the 2020 EU Security Union Strategy, and the Political Guidelines, to 'strengthen the Europol

[102] Council of the European Union 14138/19, "Council conclusions on Europol's cooperation with Private Parties" ,
December 2, 2019, 5
[103] ibid
[104] European Parliament resolution of 10 July 2020 on a comprehensive Union policy on preventing money laundering and terrorist financing – the Commission's Action Plan and other recent developments (2020/2686(RSP)), para 10
[105] ibid

mandate in order to reinforce operational police cooperation.' The newly released 2022 Europol Regulation, echoes these sentiments. It also emphasises that the new tasks given to Europol to better support Member States, would fully preserve Member States' responsibilities involved in the area of national security as laid down in Article 4(2) of the Treaty on European Union.[106] It furthermore states, that 'to allow Europol to fulfil its reinforced mandate, it should be provided with adequate human and financial resources to support its additional tasks.'[107]

Third Condition: Lock-in Effect & Cost of Going Backwards

The third condition within the failing forward theory suggests that, 'all things being equal, the failing forward dynamic is more likely to take place depending upon….the cost of unwinding the incomplete EU arrangements in question rather than moving 'forward' by granting them more authority.'[108] The cost of unwinding the EU's arrangements for data collaboration and the involvement of Europol in cross-border cooperation and innovation, would immensely affect the EU's ability to face the technological advancements being taken advantage of by terrorists and criminals. It would arguably be a step back in the EU's ambition to lead innovation and digitalisation efforts in the security industry. Thus the notion that the greater the cost to unwinding the institution, the more likely it is that EU leaders will respond to a crisis by bolstering the arrangements and transferring the given institution more power and authority in a particular domain. Furthermore, there is also a consideration of the particular features of EU institutions which may lead to a tendency to further integration with more authority. Existing research on institutions have shown that, for example, those institutions which involve 'large fixed costs, learning effects, coordination effects, and adaptive expectations are more prone to produce positive feedback, lock-in, and path dependence making the costs of reversal very high.'[109] In terms of such features of Europol, it is important to consider its structure of differentiation.

[106] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, para 4
[107] ibid
[108] Jones, Kelemen, and Meunier "Failing forward?" (2021), 1525
[109] ibid, 1531

Differentiated integration can be defined as 'any modality of integration or cooperation that allows states (members and non-members) and sub-state entities to work together in non-homogeneous, flexible ways.'[110] For Europol, since the entry into force of the Lisbon Treaty, it has been a clear case of differentiated integration in terms of its current design which 'incorporates integrated cooperation frameworks for the majority of member states, opt-outs for others and intensified cooperation with non-EU partner states.'[111] There are several key points to highlight here. Firstly, the 5 layers which comprise of Europols differentiated integration: '(1) cooperation with non-EU, non-Schengen members which are not candidates for accession, like the US; (2) cooperation with non- EU, non-Schengen members which are candidates for accession, like the Western Balkans (WB); (3) cooperation with non-EU, Schengen members, like Switzerland; (4) cooperation with EU, Schengen members which have an opt-out, like Denmark; and (5) cooperation with outgoing non-Schengen EU members, like the United Kingdom.'[112] Secondly, considering Europol as an institution of differentiated integration, where its operations are based on flexible arrangements and differentiated access to data exchange as outlined above, one must look at how the 2016 Regulation affected the way differentiated integration works. Since the Regulation, Europol has become subject to increasing bureaucracy, as partnerships which it used to be able to negotiate with non-EU countries on its own, now involve negotiation by the Commission, and approval by the Council of the EU and the Parliament. Since the increased participation of other EU bodies on its operational matters, and increased supervision of its activities by the EDPS, Europol is now faced with increased accountability but reduced effectiveness in sealing operational deals.[113] Ultimately one must of course acknowledge 'as is true for any law enforcement body, Europol finds it easier to work when away from the political spotlight.'[114] However, in an increasingly scrutinised domain of privacy and digital security, it is unavoidable that an institution which carries out activities such as Europol does, that it would avoid the increased participation and oversight of other EU bodies.

[110] Sandra Lavenex, and Ivo Križić, "Conceptualising Differentiated Integration: Governance, Effectiveness and Legitimacy," *EU IDEA Research Paper* No. 2. (November 2019), 3
[111] ibid, 4
[112] Camino Mortera-Martínez, Zoran Nechev and Ivan Damjanovski, "Europol and Differentiated Integration" *EUIDEA*, Policy Papers no.13, (January 2021), 3
[113] ibid
[114] ibid

In terms of the cost of unwinding arrangements, EU leaders in this regard, have the departure of the United Kingdom from the European Union, as a possible foresight into what those might be. In fact Brexit was indeed a partial unwinding of Europol's arrangements. According to a policy paper for the EU Integration and Differentiation for Effectiveness and Accountability (EUIDEA), in which interviews with officials from the US, Norway, Switzerland, Canada, and Australia were conducted, post-Brexit negotiations between Europol and other non-EU partners have been more complicated, and sometimes halted altogether.[115] This is the case with both the US and Canada, who are considered main security partners for the EU, and Schengen members Switzerland and Norway. Although the latter have requested more access to Europol's databases, the European Commission has been arguably stricter with non-EU countries than it would have been if it were not for Brexit. Indeed the report suggests that 'officials at Europol feel that cooperation between Europol and Denmark has suffered as a result of an agreement that was politically motivated - and left both parties less able to react to threats in a timely manner.'[116] Therefore, when considering the third condition of the failing forward mechanism, one must also account for the ways in which both integrating and disintegrating, and the costs of each, materialise in an differentiated institution such as Europol.

Privacy versus Security Debate in Digital Europe's Failing Forward Framework

Europol is not failing, but the privacy vs security debate/framework is failing. The current privacy vs security debate is framed in a way which is mutually exclusive. Yet this mutual exclusivity is not compatible with the digital age and the transition to data-driven security strategies. This framework is outdated and is a potential contributor to the crises which the EU has been facing in the last decade when it comes to digital policies and data frameworks particularly in the security industry. Europol has arguably been half baked in the digital age. Current frameworks have limited its capabilities to be competitive in this digital age, with an incomplete compromise being struck between privacy and security. There has been an unwillingness to give Europol the powers it would need to operate at maximum efficiency and effectiveness, followed by

[115] ibid 15
[116] ibid 16

incremental reforms adopted in response to the data and surveillance crises through intergovernmental bargaining between preferences towards security oriented vs privacy oriented approach to security agency access to and use of data.

European integration is a much more desirable outcome than privatisation and unregulated public-private cooperation in the security sector. There is more of a legal basis upon which to operate on, rather than covertly through private companies, which are not subject to as many jurisdictional limitations. The aversion to state-led surveillance does not prevent them from engaging in such activities but has rather led to arrangements made with private companies. In a more integrated framework with measures of protection for data and privacy, there is more public awareness and accountability. The development of new frameworks or of existing ones, must from the outset, incorporate the role and engagement with private actors in order to be successful in the digital age. As it currently stands, 'the private sector is faster, less constrained, and more agile with these tools of mass analysis.'[117] There is a growing paradox between security and privacy which began to manifest itself in the different perceptions towards the use of data when it came to economic and commercial purposes as opposed to security purposes. Ultimately this is a zero-sum game in which privacy and data are seen as mutually exclusive, which is 'making the privacy fight a battle it is no longer (or perhaps never was) equipped to win outright.'[118] This being said, there is perhaps an argument that the concerns for privacy and the protection of personal data, facilitate the development of an integrated European approach with a stronger framework for oversight and accountability of security agencies. This all falls within the realms of globalisation and the expansive demands placed on security agencies, arguably sparked by the 9/11 attacks in 2001. The new Europol mandate initiates a change in the nature of the privacy vs security debate, as well as establishing a new framework for data analysis, cooperation with the private sector, and for European integration in a data-reliant society.

[117] Cyber Persistence, Intelligence Contests, and Strategic Competition," *Texas National Security Review: Special issue on Cyber Competition* (September 2020). https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/

[118] Sun-ha Hong, "Criticising Surveillance and Surveillance Critique: Why Privacy and Humanism Are Necessary but Insufficient." *Surveillance & Society* 15, no. 2 (2017): 191

The scope for cooperation between the public and private sector, to the extent that under the 2016 Europol Regulation, Europol could exchange data with private parties, was arguably a case where the lowest common denominator of intergovernmental bargaining was reached. As an institution this left Europol incomplete, and ultimately, instead of its scheduled review 5 years from the initial implementation of the Regulation, it was widely considered that Europol needed further reform much sooner. The reform of Europol's mandate in the 2022 amendment, will likely lead to deeper integration, as national law enforcement agencies and private parties will be able to rely on Europol as a single point of contact for data exchanges as well as for the development of new innovative technological projects which will help all Member States to make use of digital tools and systems which can make the Union safer and better able to tackle terrorism and organized crime. This being said, in reality, the expansion of cooperation with private parties is still limited. Europol can now request that Member States obtain personal data from private companies via their ENUs to share with Europol.[119] Also, if it receives data directly from private parties, it may process the data for purposes other than solely to identify the national unit, contact point, or authority concerned, which are outlined in Article 18, but it must also do so for the purpose of such identification to forward the data and the results to the relevant national units.[120] This does make it easier for private parties to share data with national law enforcement agencies via Europol, as they have a single point of contact with whom they can share data. This also improves the likelihood that data can be received in its entirety and not just partially by removing the judicial or jurisdictional limitations.

This policy area within the digital industry is different. There is a significant element of hypernormalisation and social silence which is present here. Hypernormalisation is a concept which describes the phenomenon of knowing that a system is failing, but being unable to come up with a deviation from the status quo, and therefore both citizens and politicians resign themselves to maintaining this system.[121] Similarly, the anthropological notion of social silence has been applied to digital encryption in the sense that, 'a fundamental part of our lives (we depend on it whenever we bank online,

[119] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, para 19(f)(6b) amending Article 26
[120] REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794, para 19(b) amending Article 26
[121] Alexai Yurchak, *Everything Was Forever, Until It Was No More*. Princeton University Press, 2013.

send confidential messages or use Telehealth) but most of us don't have any idea how it actually works. Encryption is taken for granted and widely ignored, hence the silence.'[122] Technological advancements and their impact on public and private life require a degree of translation. Digital transformation has come with uncertainty. Not only for the general public but also for governments and policy makers themselves. Following on from the public sector breakthrough development of the World Wide Web by Sir Tim Berners-Lee whilst working at the European Organisation for Nuclear Research, the digital transformation has been predominantly led by private sector actors. In this respect, there is a difficulty for governments, even like-minded ones, to take a joint approach to implementing technological upgrades to systems and digital innovations alongside ethical standards, and regulatory frameworks. The dominance not only in developing these upgrades, but also of understanding them, brings into question a matter of access. This manifests itself where such new and unprecedented technology is developed, it is certain individuals or companies which hold unconcentrated power. This was brought to attention in 2020, by co-founder and CEO of Palantir Technologies Inc, (a company founded in 2003 to help intelligence agencies with counterterrorism investigations), who stated that tech engineers in Silicon Valley, 'may know more than most about building software, but they do not know more about how society should be organized or what justice requires.'[123] This speaks to the outsourcing of significant ethical decisions about artificial intelligence and digitalisation, 'to a tiny coterie of technocrats who neither wanted nor deserved that power.'[124] The fear of the unknown and uncertainty is what prompts 'the public to pay attention to what is happening in the silence.'[125] Thus one can arguably see here that EU institutions follow an "efficiency" and technically-based logic in order to foster integration in realms that can be politically sensitive.

[122] Gillian Tett 'Encryptogeddon is coming for us all' *Financial Times Magazine,* June 1 2022, https://www.ft.com/content/a8204a7d-2922-4944-bdff-5449a8f3aee9
[123] Ari Levy, 'Palantir CEO rips Silicon Valley in letter to investors,' *CNBC,* August 26, 2020 https://www.cnbc.com/2020/08/25/palantir-ceo-rips-silicon-valley-in-letter-to-investors.html
[124] Gillian Tett 'Encryptogeddon is coming for us all' *Financial Times Magazine,* June 1 2022, https://www.ft.com/content/a8204a7d-2922-4944-bdff-5449a8f3aee9
[125] ibid

CONCLUSION

This thesis aimed to answer the research question: to what extent mechanisms of "failing forward" have contributed to core developments in the EU's approach to the use of data in the security industry? This thesis looked specifically at this dynamic with Europol and at how the security versus privacy dynamic is changing, specifically how the push and pull between the two is being altered by the developments in the powers and competences of Europol. In Chapter One, the literature on the topic of data exchange and on the theory of failing forward was reviewed and relevant gaps highlighted. In Chapter Two, there was a background on the history of Europol, so as to demonstrate how it has developed into the institution which is at the forefront of EU security actors; a brief overview on the field of data exchange, specifically of personal data, and how the legal framework as well as the role and competences of different EU actors has developed. In Chapter 3, the main observable elements and core components of the failing forward theory of European integration are summarized. In Chapter 4, the role and application of the failing forward mechanisms was applied to Digital Europe. This entailed a breakdown of each of the conditions in which failing forward takes place, and an application of these conditions to the surveillance crisis and to Europol as the institution of primary focus.

The logic of failing forward is that a cycle of crisis will lead to incremental and incomplete reforms of incomplete institutions, which leads to further policy failure and efforts to remedy the failure with more incomplete reforms. This thesis has argued that, in the case of the EU's approach to the use of data in the security industry, there is justification to apply the failing forward mechanisms to the developments in reforming Europol and its capabilities to become a hub for integration and innovation of data exchange and management. The incomplete nature of European integration in the EU's security union, has led EU leaders to be confronted with the same issues time and time again. It is likely that they will continue to be faced with these issues. This is why the mechanisms of failing forward are perhaps an effective means of progressing in the digital and security industry. The surveillance crisis is continuous, and leaders have continuously faced the choices of managing privacy concerns vs security expectations. At the time when it emerged that cooperation with private

parties, and gaining access to personal data for analysis in criminal investigations and crime prevention, EU leaders opted to give Europol the minimum allowance to do so.

The series of incremental reforms adopted in response to the surveillance crisis, have included creating a decryption platform which national law enforcement agencies can use instead of relying on private decryption service providers, increasing the safeguards put in place to protect data and supervise activities which involve the processing of personal data, establishing Europol as the centre for innovation and research in security and policing, and bringing the value and significance of data exchange to the forefront of policy discussions and cooperative agreements. It is, however, important to discuss the extent to which, in the area of digitalisation and security policy, whether solutions can even be complete, and thus maybe the only solutions are incomplete? This could be because technology and digitalisation are rapidly expanding and new innovations are developed continuously. This makes it more likely that EU leaders will simply adopt policies which are footholds to the current crisis in question but still likely to cause further crises and further pressures for policy reform. This being said, Europol is an institution which Member States see as vital to the security of the Union, even more so in the digital age and therefore with Europol's operational and analytical capabilities as vital to their own security interests. However, though they realise that Europol's capabilities to collect, process, and analyse personal data and their cooperation with private parties is increasingly vital, they still struggle and hesitate to embrace reforms which are more comprehensive, because of opposing interests and preferences towards more fundamental and comprehensive protections of privacy and personal data.

Furthermore, in this case, it is not that EU leaders do not want to delegate more authority to Europol, because they have shown that they do, it is that they face resistance from the public, human rights activists, and data protection bodies such as the European Data Protection Supervisor on the data protection front. The strengthening of the Europol mandate, as outlined in the amending Regulation of the 2016 Europol Regulation, is determined to be an example of EU decision makers bolstering an incomplete institution, by delegating more powers to the European level to propel integration. It was clear that decision-makers thought Europol's existing architecture in respect of public-private cooperation, research and innovation,

processing large quantities of data, was lacking and that a deeper integration was needed. Since the implementation of the 2016 Europol Regulation, policy feedback was continuous, and the experiential learning which took place as Eurpool struggled to get access to the vast amounts of important data held in the private sector, (which under the principles of necessity and proportionality it would have been entitled access to), practical and bureaucratic limitations meant this did not occur, contributed to informing the incremental reforms of the 2022 amending Regulation.

The European Commission aims to make the success of the data economy a priority for Europe. In this regard it looks at how access to data can improve economic, health, and environmental aspects of society, but the topic of data sharing in security seems to be relatively taboo. At the moment there is a lack of / limit to the trust dynamic between a private company or civil-society organisation and the public-sector. Within the cycle of crisis and policy failure which the failing forward approach prescribes, there is a possibility that the EU's response to the surveillance crises of strengthening Europol's mandate in enhancing its cooperation with private parties, broadening its ability to process personal data, and strengthening its role in technological innovation and research may lead to the next crisis with the rule of law.

So far, there is a story of integration and transfer of competences which primes Europol for becoming an emerging/prominent actor in the field. What needs to be further examined is the EU-US umbrella agreement and the future direction of Europol and the extent to which it is perhaps becoming an institution more similar to the NSA than intended. The new powers given to Europol and its recognition as a dominant actor in the field, prompts a comparison with the US's National Security Agency, whose surveillance powers have long been criticised by Europe. The renewed comparison is now to determine the direction this nature of collaboration is going in and whether there is a divergence to be seen between the US and EU approach. Additionally, other arrangements for data sharing will emerge, and new technologies which disrupt existing arrangements such as the emergence of quantum computing will need to be addressed.

Bibliography

‘EU Internet Forum Ministerial : Towards a Coordinated Response to Curbing Terrorist and Child Sexual Abuse Content on the Internet,’ European Commission, January 26, 2021, https://ec.europa.eu/home-affairs/news/eu-internet-forum-ministerial-towards-coordinated-response-curbing-terrorist-and-child-sexual_en.

“About ENISA - The European Union Agency for Cybersecurity,” ENISA https://www.enisa.europa.eu/about-enisa

“Digital Trade - Trade - European Commission.” https://ec.europa.eu/trade/policy/accessing-markets/goods-and-services/digital-trade/.

“European Data Strategy,” European Commission, February 19, 2020. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en.

“International Statement: End-To-End Encryption and Public Safety” The United States Department of Justice, October 11, 2020, https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

“Operational Agreements,” Europol, https://www.europol.europa.eu/partners-collaboration/agreements/operational-agreements

“Operational and Analysis Centre,” Europol https://www.europol.europa.eu/about-europol/operational-and-analysis-centre

“Our Thinking,” Europol, https://www.europol.europa.eu/about-europol/our-thinking

“Partners and Collaboration,” Europol, https://www.europol.europa.eu/partners-collaboration

“Processing of Personal Data,” Europol, https://www.europol.europa.eu/processing-of-personal-data

“Strategic Analysis,” Europol, https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/strategic-analysis

"Strategic Arrangements," Europol, https://www.europol.europa.eu/partners-collaboration/agreements/strategic-agreements

BBC News, 'Paris attacks: What happened on the night', 9 December 2015, https://www.bbc.com/news/world-europe-34818994

Bergmann J & Müller P "Failing forward in the EU's common security and defense policy: the integration of EU crisis management," *Journal of European Public Policy* 28 no. 10, (2021)1669-1687, DOI: 10.1080/13501763.2021.1954064

Bosilca, R. "Europol and Counter Terrorism Intelligence Sharing." *Europolity: Continuity and Change in European Governance* 7, no. 1 (2013): 7–19

Conant, L, "Failing backward? EU citizenship, the Court of Justice, and Brexit," *Journal of European Public Policy*, 28, no. 10, (2021), 1592-1610, DOI: 10.1080/13501763.2021.1954061

Council of the European Union 14138/19, "Council conclusions on Europol's cooperation with Private Parties" December 2, 2019

COM(2021) 799 final, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL 'on the Third Progress Report on the implementation of the EU Security Union Strategy' 8.12.2021

Cyber Persistence, Intelligence Contests, and Strategic Competition," *Texas National Security Review: Special issue on Cyber Competition* (September 2020). https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/

Declaration of the Home Affairs Ministers of the EU ('Ten points on the Future of Europol'), October 21, 2020. https://www.eu2020.de/blob/2408882/6dd454a9c78a5e600f065ac3a6f03d2e/10-22-pdf-virtbrotzeit-europol-en-data.pdf

Dierx, A & Ilzkovitz, F, “EU competition policy: an application of the failing forward framework,” *Journal of European Public Policy* 28, no. 10, (2021) 1630-1649, DOI: 10.1080/13501763.2021.1954063

Emmons, C, & Pavone, T, “The rhetoric of inaction: failing to fail forward in the EU’s rule of law crisis,” *Journal of European Public Policy* 28 no. 10, (2021)1611-1629, DOI: 10.1080/13501763.2021.1954065

Eskens, S, *New and extensive data processing powers proposed for Europol*, 2021, European Law Blog https://europeanlawblog.eu/2021/07/30/new-and-extensive-data-processing-powers-proposed-for-europol/

Ethem Ilbiz & Christian Kaunert “Europol and cybercrime: Europol’s sharing decryption platform,” *Journal of Contemporary European Studies*, (November 2021) DOI: 10.1080/14782804.2021.1995707

European Parliament resolution of 10 July 2020 on a comprehensive Union policy on preventing money laundering and terrorist financing – the Commission’s Action Plan and other recent developments (2020/2686(RSP))

Fotiadis, A, and Howden D, “A Data ‘black Hole’: Europol Ordered to Delete Vast Store of Personal Data.” *The Guardian*. January 10, 2022. https://www.theguardian.com/world/2022/jan/10/a-data-black-hole-europol-ordered-to-delete-vast-store-of-personal-data.

Freudlsperger, C, “Failing forward in the Common Commercial Policy? Deep trade and the perennial question of EU competence,” *Journal of European Public Policy*, 28 no.10, (2021) 1650-1668, DOI: 10.1080/13501763.2021.1954059

Hong Sun-ha, "Criticising Surveillance and Surveillance Critique: Why Privacy and Humanism Are Necessary but Insufficient." *Surveillance & Society* 15, no. 2 (2017): 187-203

Schulz H, ‘Reframing the Privacy versus Security Debate: From Operation Rubicon to the Crowd- Sourced Intelligence Agency’ Submitted to the DA for Seminar: Intelligence and Diplomacy in Times of Crises

Howarth, D & Quaglia L , “Failing forward in Economic and Monetary Union: explaining weak Eurozone financial support mechanisms,” *Journal of European Public Policy,* 28 no. 10, (2021) 1555-1572, DOI: 10.1080/13501763.2021.1954060
https://www.cnbc.com/2020/08/25/palantir-ceo-rips-silicon-valley-in-letter-to-investors.html

“International Statement: End-To-End Encryption and Public Safety” The United States Department of Justice, October 11, 2020, https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety

Jones, E., Kelemen, R. D., & Meunier, S, ‘Is Europe failing, or is it ‘failing forward’?, Washington Post, July 5, 2016 https://www.washingtonpost.com/news/monkey-cage/wp/2016/07/05/is-europe-failing-or-is-it-failing-forward/

Jones, E., Kelemen, R. D., & Meunier, S, "Failing forward? Crises and patterns of European integration." *Journal of European Public Policy* 28, no.10 (2021): 1519-1536, DOI: 10.1080/13501763.2021.1954068

Jones, E., Kelemen, R. D., & Meunier, S, “Failing forward? The Euro crisis and the incomplete nature of European integration.” *Comparative Political Studies*, 49 no. 7, (2016) 1010–1034, https://doi.org/10.1177/0010414015617966

Lavenex S, and Križić I, “Conceptualising Differentiated Integration: Governance, Effectiveness and Legitimacy,” *EU IDEA Research Paper* No. 2. (2019) https://euidea.eu/wp-content/uploads/2019/12/euidea_rp_2.pdf.

Léonard, S, and Kaunert, C. “The Development of Europol’s External Relations: Towards Supranationalism?” *Maastricht Journal of European and Comparative Law* 28, no. 2 (April 2021): 229–44. https://doi.org/10.1177/1023263X211005162.

Levy A, ‘Palantir CEO rips Silicon Valley in letter to investors,’ *CNBC,* August 26, 2020,https://www.cnbc.com/2020/08/25/palantir-ceo-rips-silicon-valley-in-letter-to-investors.html

Lingenfelter, K, and Miettinen, S, “Obstacles to Supranational Operational Police Powers in the European Union: Europol Reform and the Construction of Trust between National Police

Authorities." *Maastricht Journal of European and Comparative Law* 28, no. 2 (April 2021): 182–91. https://doi.org/10.1177/1023263X211005160.

Maria Koomen, 'The Encryption Debate in the European Union' Carnegie Endowment for International Peace,
May 30, 2019, https://carnegieendowment.org/2019/05/30/encryption-debate-in-european-union-pub-79220

Milieu, "Study on the practice of direct exchanges of personal data between Europol and private parties," Final Report, HOME/2018/ISFP/FW/EVAL/0077, September 2020

Mortera-Martínez C, Nechev Z and Damjanovski I, "Europol and Differentiated Integration" *EUIDEA*, Policy Papers no.13, (January 2021)

Misuraca, Gianluca, and Others. "Envisioning Digital Europe 2030: Scenarios for ICT in Future Governance and Policy Modelling." *European Foresight Platform. 2012.* http://www.foresight-platform.eu/brief/efp-brief-no-194-envisioning-digital-europe-2030-scenarios-for-ict-in-future-governance-and-policy-modelling/

Nigel Cory and Luke Dascoli, ''How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them,' ITIF, July 19, 2021,https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost

OECD. "Risks and Challenges of Data Access and Sharing." In *Enhancing Access to and Sharing of Data*. OECD, 2019. https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en

Paravanci G, 'Paris attacks prompt EU to share secrets', POLITICO, January 20, 2016, https://www.politico.eu/article/paris-attacks-prompt-share-secrets-eu-security-forces-eurodac-schengen-information-system-terrorism-isis-isil-islamic-state-bataclan/

Proposal for a: REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) 2016/794

Rabinovych M, “Failing forward and EU foreign policy: the dynamics of ‘integration without membership’ in the Eastern Neighbourhood,” *Journal of European Public Policy* 28, no. 10, (2021)1688-1705, DOI: 10.1080/13501763.2021.1954066

Rhodes, M, “‘Failing forward’: a critique in light of covid-19,” *Journal of European Public Policy*, 28, no. 10, (2021) 1537-1554, DOI: 10.1080/13501763.2021.1954067

Stolton S, “Europol on defensive as concerns raised over ‘illegal’ Big Data tactics,” *EURACTIV*, February 2, 2021, https://www.euractiv.com/section/digital/news/europol-on-defensive-as-concerns-raised-over-illegal-big-data-tactics/

Tett G, ‘Encryptogeddon is coming for us all’ *Financial Times Magazine,* June 1 2022, https://www.ft.com/content/a8204a7d-2922-4944-bdff-5449a8f3aee9

Voronova S, “Strengthening Europol’s Mandate” European Parliamentary Research Service, March 2022

World Economic Forum. “Cyber Information Sharing: Building Collective Security.” October 2020

Yurchak Alexai , *Everything Was Forever, Until It Was No More*. Princeton University Press, 2013.