國立臺灣大學法律學院法律學系

碩士論文

Department of Law

College of Law

National Taiwan University

Master's Thesis

歐美跨境資料傳輸法制之衝突：歐美資料隱私權框架的前景及美國情報及隱私法制修法建議

Conflicts in EU-US Cross-Border Data Transfer Regulations: Prospects of the EU-US Data Privacy Framework and Recommendations for Reforming US Intelligence and Privacy Laws

廖廷碩

Ting Shuo Liao

指導教授：楊岳平 博士

Advisor: Yueh-Ping Yang, S.J.D.

中華民國 114 年 10 月

October 2025

doi:10.6342/NTU202504586

國立臺灣大學碩士學位論文

口試委員會審定書

歐美跨境資料傳輸法制之衝突：歐美資料隱私權框架的前景及美國情報及隱私法制修法建議

Conflicts in EU-US Cross-Border Data Transfer Regulations: Prospects of the EU-US Data Privacy Framework and Recommendations for Reforming US Intelligence and Privacy Laws

本論文係廖廷碩君（學號 R11A21090）在國立臺灣大學科際整合法律學研究所完成之碩士學位論文，於民國 114 年 10 月 3 日承下列考試委員審查通過及口試及格，特此證明

指導教授：

口試委員：

doi:10.6342/NTU202504586

摘要

有鑑於數位貿易之持續發展，跨境資料傳輸議題之影響力也愈發重要。歐洲聯盟（下稱「歐盟」）與美國之間在資料隱私保護上之本質區別自 1990 年代起即難以調和。歐盟原則禁止、例外允許之資料傳輸規範造成美國機構將資料自歐盟傳輸至美國之障礙，雙方之間嘗試透過建立資料傳輸架構作為例外合法傳輸之管道。此外，雖然歐美資料保護立法與觀念的差異是阻礙雙方合作的重要因素，但是有鑒於歐洲聯盟法院在過去的相關法律程序中，大幅度聚焦於美國的情報法規，故美國主要的改革方向與各方意見多聚焦在歐洲聯盟法院對情報法規立下的標準，以及美國在此方面的改革與回應。美國情報法規在立法之初授權情報機構廣泛之監視權力，以及其並未設立實質有效之救濟管道等問題，均被歐洲聯盟法院認定為不應授予歐美資料傳輸架構適足性認定的重要因素。在安全港協議與隱私盾協議相繼喪失適足性認定，以及雙方再次透過 Data Privacy Framework（下稱「DPF」）的過程中，美國相關法制也有長足的發展。本文透過分析過去之失敗經驗，探討若欲維持現行 DPF 之存續所需進行之改革，其中包括情報法規的修正，以及美國聯邦資料隱私保護法律的立法前景。惟本文分析美國現行政策與川普的行政立場後，認為完整的法規改革難以實際達成，故借鑑情況類似的英國情報法規，以釐清美國與其餘依適足性認定與歐盟進行跨境資料傳輸的國家之間，在情報授權體系上有何區別。本文認為，美國若仍願意進行一定程度之改革，先行改革外國情報監控法院的審查範圍

doi:10.6342/NTU202504586

及審查密度應能帶來最大的效益。另一方面，本文亦認為歐洲聯盟法院在潛在的法律程序中，應重新思考其在資料隱私保護上的標準，以期能緩和歐美之間在跨境資料傳輸議題上的衝突。

關鍵字：資料隱私、跨境資料傳輸、情報活動、監視、數位貿易、歐盟一般資料保護規則、歐美資料隱私權架構、國家安全、調查權力法案

doi:10.6342/NTU202504586

Abstract

With the continuous development of digital trade, cross-border data transfer has become increasingly vital. Since the 1990s, the fundamental divergences between the European Union (hereinafter "EU") and the United States of America (hereinafter "the U.S.") regarding data privacy protection have been proven difficult to reconcile. The regulatory approach of the EU is to prohibit cross-border data transfers in principle, which creates persistent obstacles for U.S. entities to transfer data across the Atlantic Ocean. Although the European Commission and the U.S. agreed on several data transfer frameworks, the adequacy decision of the previous frameworks has been declared invalid due to the extensive surveillance powers of U.S. intelligence agencies and the lack of effective remedies. At the same time, the provisions regulating intelligence activities have also evolved accordingly. This thesis examines past shortcomings and identifies the necessary reforms for sustaining the current Data Privacy Framework. However, this thesis also argues that the comprehensive reform in the U.S. remains unlikely under current policy conditions. Referring to the Investigatory Powers Act 2016 of the United Kingdom, this thesis suggests that if the U.S. remains willing to undertake certain reforms, prioritizing reform of the Foreign Intelligence Surveillance Court's scope of review would yield the greatest benefit. Conversely, it contends that the Court of Justice of the European Union should reconsider its standards for data privacy protection with the aim of alleviating transatlantic tensions over cross-border data transfer issues.

doi:10.6342/NTU202504586

KEYWORDS: *Data Privacy, Cross-Border Data Transfer, Intelligence Activities, Surveillance, Digital Trade, General Data Protection Regulation (GDPR), Data Privacy Framework, National Security, Investigatory Powers Act*

doi:10.6342/NTU202504586

目　次

doi:10.6342/NTU202504586

doi:10.6342/NTU202504586

縮寫表

中文名稱	英文名稱	縮寫
美國隱私權法案	American Privacy Rights Act	APRA
	Better Business Bureau	BBB
德國聯邦情報局	Bundesnachrichtendienst	BND
歐洲聯盟法院	Court of Justice of the European Union	CJEU
公民自由保護專員	Civil Liberties Protection Officer	CLPO
法國資訊自由委員會	Commission nationale de l'informatique et des libertés	CNIL
安全港協議適足性決定	Decision 2000/520	Decision 2000/520
標準化合約條款決定	Decision 2010/87	Decision 2010/87
隱私盾協議適足性決定	Decision 2016/1250	Decision 2016/1250
愛爾蘭資料保護委員會	Irish Data Protection Commission	DPC
歐美資料隱私權框架	Data Privacy Framework	DPF
DPF 適足性認定決定	Decision 2023/1795	DPF 決定
資料保護審查法院	Data Protection Review Court	DPRC
歐洲人權公約	Convention for the Protection of Human Rights and Fundamental Freedoms	ECHR

doi:10.6342/NTU202504586

中文名稱	英文名稱	縮寫
歐盟個人資料保護委員會	European Data Protection Board	EDPB
行政命令 12333	Executive Order 12333	EO 12333
行政命令 14086	Executive Order 14086 – Enhancing Safeguards for United States Signals Intelligence Activities	EO 14086
行政命令 14117	Executive Order 14117 - Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern	EO 14117
歐洲聯盟基本權利憲章	Charter of Fundamental Rights of the European Union	EUCFR
	Facebook Ireland Ltd	Facebook Ireland
外國情報監視法	Foreign Intelligence Surveillance Act	FISA
外國情報監控法院	United States Foreign Intelligence Surveillance Court	FISC
外國情報監控審查法院	United States Foreign Intelligence Surveillance Court of Review	FISCR

doi:10.6342/NTU202504586

中文名稱	英文名稱	縮寫
美國聯邦交易委員會	Federal Trade Commission	FTC
一般資料保護規則	General Data Protection Regulation	GDPR
調查權力法案	Investigatory Powers Act 2016	IPA
	Meta Platforms Ireland Limited	Meta Ireland
美國國家安全局	National Security Agency	NSA
隱私與公民自由政策官員	Privacy and Civil Liberties Policy Official	PCLO
隱私與公民自由監督委員會	Privacy and Civil Liberties Oversight Board	PCLOB
總統政策指令 28 號	Presidential Policy Directive 28: Signals Intelligence Activities	PPD 28
稜鏡計劃	Planning Tool for Resource Integration, Synchronization, and Management	PRISM
改革情報和保護美國法案	Reforming Intelligence and Securing America Act	RISAA
標準化合約條款	Standard Contractual Clauses	SCCs
	Maximilian Schrems	Schrems

doi:10.6342/NTU202504586

中文名稱	英文名稱	縮寫
	Maximillian Schrems v Data Protection Commissioner	Schrems I
	Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems	Schrems II
美國司法部情報監督辦公室	Intelligence Oversight Offices at the Department of Justice	司法部情報監督辦公室
	Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after *Schrems II*	白皮書
愛爾蘭高等法院	An Ard-Chúirt	高等法院
美國國務卿	United States Secretary of State	國務卿
美國監察長	Inspector General	監察長
德國聯邦國防軍	Bundeswehr	德國國防軍
歐洲聯盟	European Union	歐盟
歐洲聯盟執行委員會	European Commission	歐盟執委會
歐盟指令第 95/46/EC 號	Directive 95/46/EC	隱私指令

doi:10.6342/NTU202504586

第壹章 緒論

第一節 研究動機與問題意識

歐洲聯盟[1]（European Union，下稱「歐盟」）從 1990 年代開始就在隱私規範領域佔有一席之地[2]，而歐盟具有廣大之市場以及經濟實力，對美國來說有相當的吸引力[3]。2023 年美國商務部（United States Department of Commerce）估計資料流動帶來之跨大西洋數位貿易每年促成超過 1 兆美元的貿易和投資，同時支撐著 7.1 兆美元的歐美經濟夥伴關係[4]，故解決歐美之間之隱私規範衝突即成為重要之議題。

歐盟與美國在資料隱私與安全的立法有共同的歷史。1980 年代雙方就共同參與制定了第一套國際同意的隱私原則，以作為經濟合作與發展組織（Organisation for Economic Co-operation and Development，OECD）的隱私保護及個人資料之國際傳輸指導指引（OECD Guideline on the Protection of Privacy and Transborder Flows of Personal Data）的一部分，這些準則中如保護個人資料、確保隱私保護法律不應過度限制跨境資料流動以及其帶來之經濟和社會效應等原則，至今仍對隱私保護法

---

[1] 歐盟成員國與冰島、列支敦斯登以及挪威共同組成歐洲經濟區（European Economic Area，EEA），並共同適用 GDPR，為求精簡，以下將均以歐盟稱之。*Countries in the EU and EEA*, GOV.UK, https://www.gov.uk/eu-eea (last visited Apr. 7, 2025); Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 Amending Annex XI (Electronic Communication, Audiovisual Services and Information Society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022], 2018 O.J. (L 183) 23.

[2] Paul Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1968 (2013).

[3] Fabien Terpan, *EU-US Data Transfer from* Safe Harbour *to* Privacy Shield*: Back to Square one?*, 3(3) EUR. PAPERS 1045, 1057 (2018).

[4] Kyler Schardein, *Transatlantic Tech Tensions-The Future of the U.S.-EU Data Privacy Framework*, ASP (Mar. 21, 2025), https://www.americansecurityproject.org/transatlantic-tech-tensions-the-future-of-the-u-s-eu-data-privacy-framework/.

doi:10.6342/NTU202504586

律帶來影響。

雖然有相同之起點，但歐盟與美國在看待隱私保護以及相關立法上仍走上了不同的道路[5]。歐美跨境資料傳輸議題之合作及分歧主要肇始於歐盟指令第95/46/EC 號（下稱「隱私指令」），以及其中創設之「適足性認定（Adequacy Decision）」規定[6]。適足性認定設下了歐盟對跨境資料傳輸的基本原則，即原則禁止將資料傳輸至缺乏適足的隱私保護規範的國家[7]，並被隨後之一般資料保護規則（General Data Protection Regulation，下稱「GDPR」）承繼[8]。

歐美資料傳輸架構的一大問題出在歐盟與美國對於隱私權的定位有本質上的不同，歐盟採取「綜合立法（Omnibus Legislation）」的方式來規範資料隱私[9]；美國則沒有聯邦等級之隱私保護法律，而是以特定部門法律內包含之隱私規範，以及監

[5] Vanessa Perumal, *The Future of U.S. Data Privacy: Lessons from the GDPR and State Legislation*, 12(1) NOTRE DAME J. INT'L & COMPAR. L. 99, 103-04 (2022).

[6] 適足性認定並不一定必須以國家整體為單位，例如歐美間的安全港協議（Safe Harbour Agreement）、隱私盾協議（Privacy Shield）以及現在的 Data Privacy Framework 均以自我認證並加入的機構為範圍，另外日本個人資料保護委員會（Personal Information Protection Commission）在個人資料保護法下制定的補充細則所涵蓋者也僅以私部門作為範圍。而美國向來是以創設資料傳輸框架以獲取適足性認定，故僅有加入框架之機構得直接進行跨大西洋之資料傳輸，而非涵蓋所有美國機構。劉靜怡（2019），〈淺談 GDPR 的國際衝擊及其可能因應之道〉，《月旦法學雜誌》，286 期，頁 24-25。惟應注意者為，歐盟執委會認為日本會設置調查並解決日本公部門近用歐盟資料時可能會有之爭議，故此部分尚有爭議。Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31 [hereinafter Directive 95/46/EC].

[7] Schwartz, *supra* note 2, at 1966.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 [hereinafter GDPR].

[9] Schwartz, *supra* note 2, at 1973-76.

doi:10.6342/NTU202504586

管和自律之混合方式[10]來構建隱私法律規範[11]，規範相當零散，不管是立法或是監管部門，均未有完整的整合[12]。

自數據貿易蓬勃發展開始，兩者之間之合作及調和即產生問題。美國主要所採用的行業自律的方法，以及在當時飛速發展的數位貿易與相對滯後的政策及法律發展之間的差異逐漸形成了衝突[13]。當時歐洲與美國對於隱私權保護有概念上、本質上的差異，美國將隱私權保護交由市場處理，期望透過市場自律的方式來達成，人民所受到的隱私保護是基於個別情況來給予[14]，而歐洲則是將隱私權作為基本人權來保障[15]。此差異對雙方的合作造成巨大阻礙。

另外，美國情報機構廣泛之監視權力亦是阻礙跨大西洋資料傳輸之重要因素。在歐洲聯盟法院（Court of Justice of the European Union，下稱「CJEU」）確認授予適足性認定並不以有相同之隱私規範架構為前提，而是以是否能夠提供實質相當（Essentially Equivalent）的保護，並非要求有與歐盟相同之規範後，問題即聚焦在美國是否能提供充分之保護水準。

---

[10] Commission Implementing Decision EU 2023/1795 of 10 July 2023 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data Under the EU-US Data Privacy Framework, annex I, art. I(1), 2023 O.J. (L 231) 118 [hereinafter Decision 2023/1795].

[11] *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework*, EDPB 1, 9 (Feb. 28, 2023), https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en [hereinafter EDPB Opinion].

[12] Maria Tzanou, *Schrems I and Schrems II/ Assessing the Case for the Extraterritoriality of EU Fundamental Rights*, *in* DATA PROTECTION BEYOND BORDERS: TRANSATLANTIC PERSPECTIVES ON EXTRATERRITORIALITY AND SOVEREIGNTY, 1, 5 (Federico et al. eds., 2021).

[13] Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38(3) HOUS. L. REV. 717, 718-19 (2001).

[14] Niklas Jung, *Abolition of the Safe Harbor Agreement – Legal Situation and Alternatives*, 17 EIKV-SCHRIFTENREIHE ZUM WISSENS- UND WERTEMANAGEMENT [EIKV SERIES KNOWLEDGE & VALUE MGMT.] 1, 31 (2016).

[15] Reidenberg, *supra* note 13, at 730-31.

doi:10.6342/NTU202504586

隨著數位貿易之發展，資料保護以及傳輸之議題愈發重要[16]，美國對於資料是否應自由傳輸之立場亦有所改變。雖然 GDPR 內尚有若干除適足性認定之外之跨境資料傳輸管道，但如果跨大西洋的資料傳輸只能仰仗私人之間協調機制始得合規，可能會對歐美之間的關係造成不利的影響[17]，包括交易成本之上升[18]等。截至 2025 年 8 月為止，僅有標準化合約條款（Standard Contractual Clauses，下稱「SCCs」）經過 CJEU 之司法審查而能在一定條件下合法，其他之傳輸管道仍可能在潛在的訴訟中存在法律不確定性。

本文認為，分析歐盟與美國之間的衝突可以探明美國所面臨之困境，亦可以重新審視 CJEU 的審查標準，並試圖尋找雙方均可以接受的平衡點，以持續透過適足性認定合作。

第二節 研究對象與範圍

本文之研究對象包括歐美資料傳輸架構在歐盟法下之合法性問題，以及雙方合作之前景。具體而言，CJEU 認為美國的缺陷主要係，其認為美國情報法規對個人資料隱私的侵害過於嚴重，故本文將高度聚焦於美國情報法規的制度設計，包括情報行動的授權範圍、事前的授權程序，以及事後的救濟機制[19]。此外，本文也詳

[16] 簡毓寧、張馨云、王世明（2019），〈我國面對歐盟 GDPR 個資保護浪潮之因應與挑戰：日本經驗之借鏡〉，《經濟前瞻》，186 期，頁 53。

[17] Terpan, *supra* note 3, at 1048.

[18] 廖淑君（2020），〈論我國因應 GDPR 施行之措施－以個人資料之跨境傳輸為核心議題〉，《商業法律與財金期刊》，3 卷 1 期，頁 134。

[19] 美國政府自行獲取歐盟人民資料之行為是否影響適足性認定之判斷存在爭議。美國認為只有透

doi:10.6342/NTU202504586

細說明歐盟方面的立場，主要聚焦於CJEU先前的兩次先行裁決（Preliminary Ruling）中立下的標準。

另外，因為CJEU的審查對象是歐美資料傳輸架構的適足性認定，為歐盟法下的法律的爭議，其主要的審查對象亦為美國的國內法，故本文主要聚焦於美國法與歐盟法，不包括國際協定以及國際組織的規範與標準。

最後，本文之討論範圍限於傳輸至美國商業組織之資料之相關問題，討論內容多與數位貿易發展、消費者隱私保護相關，故不涵蓋雨傘協定[20]（Umbrella Agreement）等與執法機構之間資料傳輸相關之法律架構。

第三節 研究方法

第一項 文獻回顧及分析法

本文回顧既有的相關學術文獻，匯聚歐美跨境資料傳輸議題的各方意見，以及

過美國機構間接自國內機構獲得之資料始應納入適足性評估範圍，而美國政府自行直接蒐集之資料應以歐洲聯盟條約第4條第2款之國家安全例外作為依據，並提出CJEU之相關判決作為支持；但相反的CJEU認為歐洲聯盟條約之國家安全例外條款與向第三國轉移個人資料無關，無論資料是否可能被用於國家安全目的，GDPR均適用。另外，相關之討論文獻亦均未進行區分而將所有相關法規一同討論。基此，為免爭議，本文對於美國政府之直接獲取資料之相關法律以及實踐均會一同說明，以期完善。Jan Helge Brask Pedersen, *The EU-US Data Privacy Framework and the Schrems Saga: Is there Light at the End of the Tunnel?*, 2024(2) ZEITSCHRIFT FÜR EUROPARECHTLICHE STUDIEN [J. EUR. LEGAL STUD.] 213, 221-24 (2024).

[20] 雨傘協議係指美國與歐盟間關於預防、調查、偵察和起訴刑事犯罪之個人資訊保護協議，係關於歐盟與美國官方間之資料交換協議。*See generally* Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses, EU-U.S., May 18, 2016, https://www.hunton.com/privacy-and-information-security-law/assets/htmldocuments/uploads/sites/18/2016/06/ST_8557_2016_INIT_EN.pdf.

doi:10.6342/NTU202504586

雙方合作的歷史，以瞭解雙方合作的主要癥結點，並針對各點提出意見。在理清癥結點後，本文亦針對其中的美國情報法規的演進逐一探究，總結出具體的法制問題，並逐一評價。此外，本文也透過回顧雙方的官方文件，以釐清雙方在實務層面的想法以及可能的動向。

第二項 比較法研究法

情報法規以及適足性認定均非美國所獨有，英國亦有相似之法規以及問題。本文透過分析英國的情報法規，並與美國的情報法規對比，以指出兩個在情報行動領域有重要影響力的國家的差異，並說明美國可能的改革方向。

第三項 歷史分析法

本文透過說明歐美雙方過去與現存的資料傳輸架構，以及美國在與歐盟合作期間所進行的法律改革，以分析雙方在合作期間難以解決的問題，以及歐盟內部不同機構間的立場差異。

第四節 研究架構

本論文分為六章。第一章為緒論，說明歐美雙方主要的法規範差異，以及待解決的問題。第二章介紹主要的相關法規及其演變的歷史，包括歐盟的資料隱私與傳輸的相關規範，以及美國的情報法制。

第三章首先回顧過去兩個已失效的資料傳輸架構，以及使其失效的兩個先行

doi:10.6342/NTU202504586

裁決，以釐清 CJEU 在判斷一國的資料保護水準是否具備適足性時所採取的標準。隨後，本章亦介紹現行的資料傳輸架構，以及其立法程序，並分析其與前兩個資料傳輸架構的異同。

第四章聚焦於現行的美國法規與資料傳輸架構的法律爭議。本章透過分析其中重要的制度設計，將之與 CJEU 的標準比較，以確認兩者之間的差距，並提出將美國情報法規修正至得以符合 CJEU 標準的構想。此外，本章亦探討美國聯邦資料隱私立法的可能性，以及現行立法討論的前景，並分析其對歐美在跨境資料傳輸議題上的影響。

第五章討論在 2025 年的時代背景下，美國在相關議題的態度，以分析美國在與歐盟合作上可能的走向。此外，本文亦分析 CJEU 在資料隱私保護議題上所立下的標準，以討論其標準的合理性，以及其對歐美跨境資料傳輸議題的影響，並給予建議。

第六章為結論，總結本文的主要觀點，並指出未來的觀察方向。

doi:10.6342/NTU202504586

第貳章 美國情報法規與歐盟隱私保護規範

本節為背景介紹。首先，本章說明美國情報法規的立法歷史，以及各法律以及行政命令的特質與論者對其的評價。其次，本章說明歐盟限制跨境資料傳輸的法源基礎與其沿革，以及 CJEU 審查美國法規時引用的相關法律規定。雖然歐美之間的資料隱私保護法規的差異為一難以協調之問題，惟在雙方合作的過程中，CJEU 亦詳細分析了美國情報法規的不足，而後續美國的改革，以及 Data Privacy Framework（下稱「DPF」）的談判過程亦以之為主要的討論對象，故本論文在美國法規方面以介紹情報法規為主。

第一節 美國情報法規之演變

第一項 Foreign Intelligence Surveillance Act

自 1960 年代起，美國開始使用國家安全例外，為保護國家安全而限制個人權利，而此等例外造成了許多權利侵害之問題，於是美國國會通過了外國情報監控法[21]（Foreign Intelligence Surveillance Act of 1978，下稱「FISA」），是對於總統與外國情報蒐集及電子監視相關之美國憲法第二條權力進行規範之法典[22]，並首次允許為情報目的為非刑事監控[23]。

[21] Foreign Intelligence Surveillance Act, 50 U.S.C. § 1881 (2018) [hereinafter FISA].
[22] Mark M. Jaycox, *No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333*, 12 HARV. NAT'L SECURITY J. 58, 71 (2021).
[23] Stephen Gemar, *A Crucial Aspect of National Security in Need of Reform: Section 702 of the FISA Amendments Act*, 65 S.D. L. REV. 489, 492 (2020).

doi:10.6342/NTU202504586

第一款 基本架構

FISA 第一章規定四種被授權可以進行監視之情況：(1)獲取美國境內之美國人發送或意圖接收之訊息，除非此等內容係有意針對該美國人獲取者，否則需要搜索令[24]、(2)獲取在美國境內通訊之內容[25]、(3)獲取有意接收之無線通訊內容，並且雙方均在美國境內，且須獲得搜索令[26]、(4)在美國境內安裝設備進行監控以獲取訊息，而非來自有線或無線通訊之訊息，並且需要搜索令[27]。

外國情報監控法院（United States Foreign Intelligence Surveillance Court，下稱「FISC」）負責授權透過 FISA 進行之監視行動，並確保行動係針對在美國境外之人士並防止獲取發送者或接收者位於美國境內之任何通訊，並且得以獲得外國情報[28]。FISC 之審查內容包括目標選定程序、最小化程序[29]以及符合 FISA 第 702 條中之其他限制等，最後給出認證，情報機構始得為監視行動[30]。對於 FISC 之決定，政府或被針對之電子通訊服務提供商可以向外國情報監控審查法院（United States Foreign Intelligence Surveillance Court of Review，下稱「FISCR」）上訴以審查該決定[31]。

在 9/11 恐怖攻擊過後，FISA 於 2008 年被修正並制定第 702 條。FISA 第 702

---

[24] FISA, *supra* note 21, § 1801(f)(1).
[25] *Id.* § 1801(f)(2).
[26] *Id.* § 1801(f)(3).
[27] *Id.* § 1801(f)(4).
[28] *Id.* §§ 1881a(h)(1)-(2).
[29] 最小化程序在電子監控之範疇下，係指應由司法部長採納程序以盡量減少蒐集與保存未公開之美國人訊息。*Id.* § 1801(h).
[30] *Id.* § 1881a(h).
[31] *Id.* § 1881a(h)(6).

doi:10.6342/NTU202504586

條授予政府監視權力，允許對合理認為位於美國境外的外國公民蒐集外國情報。FISA 第 702 條創造一個新的框架，使政府可以尋求 FISC 授權監控外國情報，以獲得位於外國之外國人的通訊內容[32]。

FISA 第 702 條之蒐集對象為位於國外之非美國人的通訊內容，監控之目的必須是為獲取外國情報訊息，包括與戰爭威脅、恐怖主義、大規模殺傷性武器擴散、間諜活動與國際毒品販運有關的訊息，或「其他對美國國防、安全或開展美國外交事務所必須的訊息」，此概括條款之存在使其對情報蒐集活動之限制變得毫無意義，因此也被戲稱其唯一的真正限制是蒐集者的創造力[33]。

FISA 主要透過兩種方法獲取位於外國之非美國人的通訊內容。其一是美國國家安全局（National Security Agency，下稱「NSA」）可以強制自管理電信傳輸基礎設施的公司所管理的設施中獲取通訊內容[34]；其二是透過強制服務提供商交出相關通訊內容以獲得情報[35]。

FISA 第 702 條之特點係其得阻止私部門在客戶之資料受到蒐集時通知客戶[36]，另外其對於監控之申請要求更加模糊，不需指名特定之監控目標，其手段也不需明確化[37]，而僅有合理性要求，包括目標選定程序以及最小化程序[38]。

進行情報蒐集時，NSA 之分析人員首先會識別位於外國之外國人，並認定進

---

[32] *Id.* § 1881; Gemar, *supra* note 23, at 490-94.
[33] Noah C. Chauvin, *Increasing Congressional Oversight of FISA Section 702 After RISAA*, 92 TENN. L. REV. (forthcoming 2025) (manuscript at 7) (on file with SSRN).
[34] *Id.* manuscript at 6-7.
[35] Gemar, *supra* note 23, at 494.
[36] *Id.* at 496.
[37] *Id.*
[38] Decision 2023/1795, *supra* note 10, recital 144.

doi:10.6342/NTU202504586

行監控會獲得指定之外國情報後，透過目標之通信設施進行監控。一旦目標不再滿足選定之標準時，即應停止監控。司法部情報監督辦公室（Intelligence Oversight Offices at the Department of Justice）人員每兩個月會審查是否目標之選定符合程序，並對 FISC 以及美國國會報告違規行為[39]。

FISA 第 702 條授予美國政府寬泛之監視權力，其監視範圍廣泛，因此引起可能不足以保障美國人權利之質疑[40]。為平衡合法安全需求和個人隱私，國會要求需要重複對此規範進行更新——也就是日落條款，否則規範期限屆至即會失效[41]。但即使有落日條款存在，時至今日美國政府仍然持續通過延長其效力之更新[42]，故對於監視過廣之問題，美國政府僅能用一系列之命令來解決。

第二款 2024 年的重新授權——Reforming Intelligence and Securing America Act

美國國會在 2024 年通過了改革情報和保護美國法案（Reforming Intelligence and Securing America Act，下稱「RISAA」）以重新授權 FISA 第 702 條。RISAA 在部分方面限制了監控授權，但在其它層面卻也擴大了範圍[43]。

就限制監控行動而言，支持者認為 RISAA 是歷來最重要之改革，但實際上其新增之限制許多均已是情報界原有的內部政策之法規化，整體而言不被認為會為

[39] *Id.* recital 147.
[40] *See generally* Gemar, *supra* note 23.
[41] Chauvin, *supra* note 33, manuscript at 3-4.
[42] Ted Barrett et al., *Senate passes, Biden signs surveillance bill despite contentious debate over privacy concerns*, CNN (Apr. 21, 2024), https://edition.cnn.com/2024/04/19/politics/fisa-senate-negotiations/index.html.
[43] Chauvin, *supra* note 33, manuscript at 35.

doi:10.6342/NTU202504586

FISA 第 702 條帶來實質性的重要改革[44]。另外 RISAA 針對 FISA 第 702 條之監督和透明度亦有改變，增加了審計要求，使國會更清楚了解情報機構對 FISA 第 702 條之實行情況，以及提高對公眾的解密要求，但似乎並不能完全解決存在的法律和政策問題[45]。

而在對於監控的擴展方面，最重大的變更是對於電子通訊服務提供商的定義被擴展，新的定義範圍將覆蓋任何的服務提供商，並且有權存取正在或可能用於傳輸或儲存有線或電子通訊的設備。此種變更可能會涵蓋大量企業，包括自助洗衣店、健身中心、牙醫診所，以及每天租賃辦公空間給數千萬美國人上班的商業房東。寬泛的定義不僅在跨境資料傳輸下造成影響，對美國人也會帶來巨大影響並引發討論。目前影響的程度尚不明瞭，但美國司法部表示擴展定義僅係欲涵蓋提供雲端計算服務的資料中心，故其影響仍待觀察[46]。

最後，RISAA 創建了一個 FISA 改革委員會以審查 FISA 實施的有效性並制定立法行動建議以進行改革，意在有效開展情報活動，以及保護隱私與公民自由，但其功能和效用則有待觀察[47]。

整體而言，RISAA 很大程度係將 FISA 第 702 條之實務現狀編入法律，並未帶來實質之改變。本文認為，雖然其並未對整體授權以及監督體系進行大幅度的改革，但是以國會制定之法律對情報活動進行限制，可以帶來更高之穩定性以及降低法

[44] *Id.* manuscript at 36-39.
[45] *Id.* manuscript at 43-45.
[46] *Id.* manuscript at 41-43.
[47] *Id.* manuscript at 46-47.

doi:10.6342/NTU202504586

律風險，對管制情報行動有助益，值得肯定。

第二項 Executive Order 12333——United States Intelligence Activities

行政命令 12333[48]（Executive Order 12333，下稱「EO 12333」）是時任雷根總統（Ronald Reagan）在 1981 年簽署，關於行政部門間諜權力之總體政策框架[49]。EO 12333 係美國憲法第二條規定總統作為三軍統帥以及行政部門首長之權力之法規化，其授予情報機構進行對美國外交關係和國家安全保護所必需之活動[50]，並強調在外國進行之情報活動，以獲取重要的外國情報，並用於偵測和打擊外國勢力開展之恐怖活動和間諜活動[51]。關於傳播以及保存蒐集之訊息，則由機構負責人制定程序，並由司法部長批准，始得進行蒐集、保留或傳播有關美國人之訊息[52]。

EO 12333 與 FISA 不同，其不僅是規範電子監視，而是包括所有的監視行為[53]。第一部分規定了關於各個情報機構之職責，其中關於訊號情報之權限劃分予 NSA，授權其為訊號情報之主責機關[54]，規定其應「蒐集、處理、分析、製作並傳播用於外國情報及反情報目的之訊號情報資訊與數據，以支援國家及部門之任務[55]」，以及「掌控訊號情報的收集及處理活動，包括將資源分配給適當的代理機構，以滿

---

[48] *Id.*¶60; 行政命令 12333 允許美國國家安全局（National Security Agency，下稱「NSA」）在資料仍在大西洋底部之電纜時存取之，並且不受法律監管，*Id.*¶63; Exec. Order No. 12,333, 46 Fed. Reg. 59941 (Dec. 8, 1981) [hereinafter EO 12333].

[49] Jaycox, *supra* note 22, at 62.

[50] *Id.* at 61-62.

[51] EO 12333, *supra note* 48, ¶2.2.

[52] *Id.*¶2.3. 另應提及者為，EO 12333 多有「Information」之用字，故譯作「訊息」以明確分別之。

[53] Jaycox, *supra* note 22, at 75-76.

[54] EO 12333, *supra* note 48, § 1.7.

[55] *Id.* § 1.7(1).

doi:10.6342/NTU202504586

足直接支援軍事指揮官所需的任務和時間要求[56]」。

第二部分規範了情報活動之實施以及範圍，並施加了特定限制，規範了情報機構可以蒐集、保留和共享之內容。情報機構得蒐集公開或經當事人同意之資訊、外國情報或反情報資訊、合法外國行動中獲得之資訊、為保護個人或組織安全所需之資訊、為防止洩漏情報所需之資訊、用以評估合理認為可能成為情報來源或聯絡人之個人之資訊、因合法的內部調查而產生之資訊、高空偵察獲得之資訊、附帶獲得之資訊，以及行政管理所需之資訊[57]。在得蒐集之資訊中，與本文關聯性最大者為第 2.3 條(b)項之屬於外國情報或反情報之資訊，因其包括與企業或其他商業組織相關的此類資訊，以下之分析亦將針對商業組織蒐集外國資料而可能收到情報機構蒐集、使用以及傳輸之情況。

EO 12333 賦予情報機構廣泛之權限以執行外國情報蒐集活動，也要求情報機構在授權範圍內制定指導方針並經過司法部長批准[58]。一般來說，只要合理的認為可以獲得外國情報，情報機構即可以合法的啟動搜索程序[59]，無須經過獨立機構之審查授權。

在大規模蒐集上，EO 12333 之授權相當廣泛，其係自源頭，經由電信公司、電網等途徑直接獲取全部傳輸之內容，而不針對特定之目標[60]，再配合實務上寬鬆之授權範圍，會大量蒐集不相關個人之資料。實際上，EO 12333 之隱私保障甚至

[56] *Id.* § 1.7(3).
[57] *Id.* §§ 2.3(a)-(j).
[58] *Id.* § 2.4.
[59] Jaycox, *supra* note 22, at 83.
[60] *Id.* at 90-96.

doi:10.6342/NTU202504586

較 FISA 第 702 條不足，被批評其未設計救濟與監督機制來抑制其無限制之監控措施[61]。

第三項 Presidential Policy Directive 28——Signals Intelligence Activities

第一款 PPD 28 之規範

2014 年時任美國總統歐巴馬（Barack Obama）在斯諾登（Edward Snowden）事件[62]發生的七個月後發表了稱為 Signals Intelligence 的演講（下稱「演講」），並且發佈了總統政策指令 28 號 Presidential Policy Directive 28: Signals Intelligence Activities（下稱「PPD 28」），以表彰情報工作對美國國家安全之貢獻，以及承認爭議問題並進行改革[63]。

PPD 28 旨在保護因為美國情報機構之監控行為而偶然被蒐集資料之外國人民之權利[64]，其承認單一的全球通訊基礎設施會導致個人情報以及重要的外國情報難以在蒐集時被分離，故尋求闡明美國進行情報活動之基準，並作出對民主原則、人權、貿易、隱私以及公民自由上之承諾[65]。

PPD 有六個主要的部分：

---

[61] Matthew Connolly, *Will the EU-US Data Privacy Framework Survive Schrems III?*, 27 TRINITY COLL. L. REV. 87, 122 (2024).

[62] Edward Snowden 為一名前美國中央情報局之承包商，其於 2013 年曝光了美國情報機構的大規模監控計劃。*Edward Snowden: Leaks that Exposed US Spy Programme*, BBC (Jan. 17, 2014), https://www.bbc.com/news/world-us-canada-23123964.

[63] Peter G. Machtiger, *Fixing PPD-28: Implementation Issues and Proposed Revisions for Privacy Protections in Signals Intelligence*, J. LEGIS. & PUB. POL'Y 227, 229-30 (2020).

[64] *Id.* at 231.

[65] *Id.* at 231-32.

doi:10.6342/NTU202504586

1. 管理訊號情報蒐集之原則——訊號情報（Signals Intelligence）之蒐集應有法規、行政命令、公告或是其他總統命令授權，並依據憲法以及上述授權規定執行[66]。蒐集訊號應考量隱私以及公民自由，並僅得將訊號作為外國情報或反情報目的使用[67]，以及盡可能量身定作[68]。

2. 對大規模蒐集訊號情報之利用限制——透過大規模蒐集訊號情報以辨別威脅是無可避免的，但美國對於訊號情報之使用會施加限制，以保護所有人的隱私及公民自由[69]。大規模蒐集訊號情報之用途應限於以下六種目的：(1)外國勢力或其情報部門針對美國及其利益進行的間諜活動和其他威脅和活動；(2)恐怖主義對美國及其利益的威脅；(3)開發、擁有、擴散、或使用大規模殺傷性武器對美國及其利益所造成的威脅；(4)網路安全威脅；(5)對美國或盟軍武裝部隊，或其他美國或盟軍人員的威脅；以及(6)跨國犯罪威脅，包括與本節所述其他目的相關的非法融資和逃避制裁，並且不得作為實施歧視之工具或是為商業目的[70]。另外本段也建立了對於訊號情報之使用目的之審查規範[71]。

3. 完善蒐集訊號情報之流程——美國情報蒐集活動若遭不當披露，可能帶來國家安全損害，因此國家安全決策者必須在這些活動所涉及風險的背景下，謹慎考

---

[66] *Presidential Policy Directive -- Signals Intelligence Activities*, NAT'L ARCHIVES, sec. 1, § (a), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [hereinafter PPD 28].
[67] *Id.* sec.1, § (b).
[68] *Id.* sec.1, § (d).
[69] *Id.* sec.2.
[70] *Id.*
[71] *Id.*

doi:10.6342/NTU202504586

慮訊號情報活動的價值，並作出謹慎的判斷[72]。

4. 保護通過訊號蒐集之個人資料——本段規定對於隱私之保護分為四點：(a)政策與程序：最小化個人資訊之傳播和保存，僅得在符合 EO 12333 相關規定之情況下始得保存以及傳播，並且僅在情報總監明確認定符合美國國家安全利益之情況下，始得保存超過五年，以確保資料的安全並且只供被授權之專業人員存取、確保資料的準確性和客觀性、有效的監督機制等[73]；(b)在 PPD 28 公布起之一年內，情報機構應與情報總監協調以更新與之相配合之政策和程序，並最大程度地公開之[74]；(c)建立隱私與公民自由政策官員（Privacy and Civil Liberties Policy Official，下稱「PCLO」），以與情報機構之高級官員、司法部長等合作，以共同制定相關之政策和程序[75]；(d)美國國務卿（United States Secretary of State，下稱「國務卿」）應指定一名高級官員負責協調相關之外交工作，並提出美國情報活動之疑慮[76]。

5. 報告——要求相關機構在一定時限內報告其依據 PPD 28 之要求所需之評估報告[77]。

6. 一般原則——PPD 28 之內容並不減損總統之憲法權力、美國政府人員之法律上權力，而僅是補充外國情報以及反情報活動之現有流程及程序[78]，PPD 28 應適

[72] *Id.* sec. 3.
[73] *Id.* sec. 4(a).
[74] *Id.* sec. 4(b).
[75] *Id.* sec. 4(c).
[76] *Id.* sec. 4(d).
[77] *Id.* sec. 5.
[78] *Id.* sec. 6, §§ (a)-(b).

doi:10.6342/NTU202504586

用美國法律[79]，且並不會創造任何實體上之權利義務[80]。

第二款 PPD 28 之疑慮

論者對於演講以及 PPD 28 之評論是否可有效改善美國情報活動在斯諾登事件暴露出的問題，存在意見分歧[81]。有論者認爲其在隱私保護方面作出了重大的進步，亦有人認為其最終幾乎沒有改變情報機構之行為模式[82]，並未對美國在蒐集情報上之行為產生實質性之影響。

PPD 28 是首個將過去只有美國公民得享有之隱私權利擴展至外國國民之規範，這在世界範圍內都是首例，惟其仍有諸多缺陷。首先，PPD 28 對於多數術語與概念亦未有明確之定義，特別是其標題「訊號情報」。此等不明確造成不同情報機構之間之運作混亂和差異。多數定義方式以 EO 12333 內之電子監視（Electronic Surveillance）作為參考依據，但此等定義又過於廣泛，而 PPD 28 原有機會防止此等問題卻並未確實解決[83]。

其次，雖然 PPD 28 呼籲減少大規模蒐集，但是其授權進行大規模蒐集的情況幾乎包含了所有情報機構想蒐集資料之理由；此外對於大規模蒐集之限制僅適用於非公開資訊，故原本即公開的訊息，例如社交網路等，皆可被無限制的大規模蒐集，有論者認為 PPD 28 所施加之限制僅係排除了對於情報機構而言本即無用之資

[79] *Id.* sec. 6, § (c).
[80] *Id.* sec. 6, § (d).
[81] Machtiger, *supra* note 63, at 233-34.
[82] *Id.* at 233.
[83] *Id.* at 234-47.

doi:10.6342/NTU202504586

料[84]。

再者，透過過濾大規模蒐集而來之資料以尋找特定內容之方式，稱為臨時性之大規模蒐集。其在 PPD 28 中被定義為針對性蒐集，致使兩者之間區分不易，而針對性蒐集並沒有大規模蒐集所受之限制，可能造成實質上 PPD 28 限制大規模蒐集之效果相當有限[85]。

此外，傳播和保存資料之限制不論是對於提高訊號情報之效率，或是對於個人之資料隱私保護都相當重要，惟不論是 EO 12333 或 PPD 28 均未有嚴格之規定，反而幾乎所有被情報機構認為有用之資訊均會落入 EO 12333 第 2.3 小節之範圍，導致資訊被傳播之範圍極為廣泛，保存之時間也容易落入得以保存超過 5 年之例外範圍[86]。PPD 28 僅係要求應在保障國家安全之最大可行範圍內施加限制，而多數情報機構都認為原先之作法並不需要經過調整即可滿足此要求[87]。PPD 28 僅是要求應額外之保障措施，但實際上並沒有報告表明此等保障措施存在[88]。然而，即使要求相當寬鬆，情報機構在實行上也未能完全滿足 PPD 28 之要求[89]，使整體之改革效果並不顯著。

第三款 PPD 28 之撤銷與取代

PPD 28 傳達了大量之政策價值觀，但實質上只對美國情報機構監控權力造成

[84] *Id.* at 249.
[85] *Id.* at 250.
[86] *Id.* at 252.
[87] *Id.* at 253.
[88] *Id.* at 251-52.
[89] *See id.* at 253-56.

doi:10.6342/NTU202504586

小幅度之縮減[90]。PPD 28 改革不足的缺點隨著時間逐漸浮現，於是時任總統拜登（Joseph R. Biden Jr.）以國家安全備忘錄 14 號（National Security Memorandum on Partial Revocation of Presidential Policy Directive 28）將 PPD 28 部分撤銷，僅留下改善訊號情報流程之第三節以及第六節之一般規定[91]，並隨後以行政命令 14086（下稱「EO 14086」）取代之，發展出更接近歐盟標準之情報活動指南。

第四項 Executive Order 14086——Enhancing Safeguards for United States Signals Intelligence Activities

第一款 EO 14086 之規範

時任美國總統拜登在 2022 年 10 月 7 日簽署了 EO 14086，此指令很大程度是 PPD 28 之替代品[92]，約束了 FISA 及 EO 12333 所授權的廣泛的監視權力。其中第二節規範了情報機構之活動[93]，以下詳細介紹之。

(a)小節要求情報行為應由法規或行政命令、公告或其他總統指令授權，根據相關法規進行，並受到適當之保障措施約束[94]。因此，情報活動僅在評估所有相關因素後確定為必要之「經驗證之優先情報（Validated Intelligence Priority）」後，始得進行[95]，並應受到嚴格監督[96]。所謂「經驗證之優先情報」。係指情報總監以國家

[90] *Id.* at 242.
[91] Joseph R. Biden Jr., *National Security Memorandum on Partial Revocation of Presidential Policy Directive 28*, (Oct. 7, 2022), https://irp.fas.org/offdocs/nsm/nsm-14.pdf.
[92] Decision 2023/1795, *supra* note 10, recital 12
[93] Exec. Order No. 14,086, 87 Fed. Reg. 62283 (Oct. 7, 2022) [hereinafter EO 14086].
[94] *Id.* sec. 2, §§ (a)(i)-(ii).
[95] *Id.* sec. 2, §§ (a)(ii)(A)-(B).
[96] *Id.* sec. 2, § (a)(ii)(C).

doi:10.6342/NTU202504586

安全法（National Security Act of 1947）第 102A 條[97]設定之目標、優先事項和指導方針，並以國家情報優先框架（National Intelligence Priorities Framework，為保密狀態[98]）所規範之設立、管理和評估經驗證之優先情報之要點作成[99]，並由情報總監獲得公民自由保護專員（Civil Liberties Protection Officer，下稱「CLPO」）之評估後制定，並交給總統批准[100]。

(b)小節列舉了 12 個對國家安全造成威脅之合法蒐集訊號[101]之目標，情報機構僅於符合此目標內有一個或多個目標時始得合法進行訊號蒐集[102]，除此之外總統在有新的國家安全需求時得增加目標項目，並得在有國家安全考量時不公開之[103]。另外 EO 14086 也舉出了不得作為監控目標之項目，包括不得用以壓制人民之基本權利[104]、不得作為歧視之工具[105]，以及不得作為給予美國商業部門競爭優勢之工具[106]。是否為合法之情報活動應由 CLPO 進行評估，評估之內容包括(1)其是否為合法目標、(2)是否非非法目標、以及(3)是否適當考慮所有人之隱私以及公民自由後建立，無論其國籍或居住地[107]。

---

97 National Security Act, 50 U.S.C. § 3024(f).
98 Zoran Dimović, *Analysing the EU Data Privacy Implications Resulting from Executive Order 14086: A Legal Perspective*, 16(1) LEXONOMICA 85, 102 (2024).
99 *Intelligence Community Directive 204: National Intelligence Priorities Framework*, OFF. OF THE DIR. OF NAT'L INTEL. 1 (Jan. 7, 2021), https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf.
100 Decision 2023/1795, *supra* note 10, recital 135.
101 EO 14086 內使用 Signal 字眼，故提到其規範時使用「訊號」作為情報機構蒐集之目標。*See generally* EO 14086, *supra* note 93.
102 EO 14086, *supra* note 93, sec. 2, § (b)(i)(A).
103 *Id.* sec. 2, § (b)(i)(B).
104 *Id.* sec. 2, §§ (b)(ii)(A)(1)-(3).
105 *Id.* sec. 2, § (b)(ii)(A)(4).
106 *Id.* sec. 2, § (b)(ii)(B).
107 *Id.* sec. 2, § (b)(iii)(A).

doi:10.6342/NTU202504586

(c)小節則是規定了保障措施應評估情報活動之必要性以及比例原則，並指明了應考量之因素[108]。此外，在可以使用針對性蒐集即達成目標時，不得使用大規模蒐集，而即使使用大規模蒐集，也應使用合理之方法和技術措施，以將蒐集範圍限制於經驗證之優先情報[109]。

大規模蒐集之合法目標僅有 6 個，包括危害較大之恐怖主義、間諜活動、網路安全威脅以及大規模殺傷武器等[110]。此外其與針對性蒐集之列舉目標相同，可以由總統增加合法目標，並可選擇不公開之[111]。

另外本小節亦對個人訊息之處理進行規範，包括最小化訊息之保留時間以及傳播範圍、限制可以存取資料之範圍以及防止未授權人士存取資料、確保資料之客觀性以及準確性、查詢大規模蒐集之資料時應確保未經最小化之大規模蒐集之訊息之保護、以及保持情報活動之文件紀錄以對情報活動之各方面進行合理評估[112]。

(d)小節規定了對訊號情報活動進行之監督，其要求要有美國監察長（Inspector General，下稱「監察長」）、CLPO 以及其他監督合規之官員之監督，以確保遵守美國法律[113]。監督之官員得獲取與其職責相關之所有資訊，以確保其能採取適當行動，並履行其監督職責[114]。CLPO 之決定對情報機構有拘束力，並可以要求情報機構提供其所需之資訊[115]，並不受到情報機構之阻礙，且有獨立性保障，除非有不當行

[108] *Id.* sec. 2, § (c)(i).
[109] *Id.* sec. 2, § (c)(ii)(A).
[110] *Id.* sec. 2, § (c)(ii)(B).
[111] *Id.* sec. 2, § (c)(ii)(C).
[112] *Id.* sec. 2, §§ (c)(iii)(A)-(E).
[113] *Id.* sec. 2, §§ (d)(i)(A), (d)(iii).
[114] *Id.* sec. 2, § (d)(i)(B).
[115] *Id.* sec. 2, §§ (d)(ii)-(iii).

doi:10.6342/NTU202504586

為或失能等情況外，CLPO 不得因其依據 EO 14086 所為之行動受到解職[116]，故擁有一定之獨立性保障。

第三節設計了爭端解決機制，規範如何審查由合格國家之適當機構移送之合格投訴，以審查是否有違反美國法規之相關行為並在必要時採取適當之補救措施[117]。所謂「合格國家」，係指由司法部長經與國務卿、美國商務部部長和情報總監協商後指定之特定國家或一體化之區域經濟組織。合格國家應對美國人之個人資料提供適當保障，並且其與美國之間之資料傳輸得以促進美國之國家利益[118]。合格國家之人民得向合格國家之公共機構投訴美國情報機構之違規行為並由其傳輸至美國以開啟程序[119]。此等投訴採取「信念測試[120]（Belief Test)」，即投訴人僅需合理相信其個人資訊已經被傳輸至美國，並發生了涉及投訴人個人資訊之違規行為所提出之投訴，即可被認定為合格投訴[121]。

爭端解決程序之開始係由情報總監與司法部長協商，以建立一個由 CLPO 審查之程序[122]，而其結論係由合格國家之相關機構[123]——也就是資料主體最初投訴之對象——通知資料主體以下兩種結果之一——「審查未發現任何涵蓋之違規行為」或是「CLPO 發出了採取適當補救措施之決定」[124]，並通知其可以對資料保護

116 *Id.* sec. 2, §§ (d)(i)(C), (d)(iv)
117 *Id.* sec. 3, § (a).
118 *Id.* sec. 3, § (f)(i).
119 *Id.* sec. 3, § (b).
120 EDPB Opinion, *supra* note 11, at 51.
121 EO 14086, *supra* note 93, sec. 4, § (k)(i).
122 *Id.* sec. 3, § (c).
123 *Id.* sec. 3, § (c)(i)(E).
124 *Id.* sec. 3, § (c)(i)(E)(1).

doi:10.6342/NTU202504586

審查法院（Data Protection Review Court，下稱「DPRC」）提出上訴，並會指派一位特別辯護者（Special Advocate）保護其利益以進行程序[125]。特別辯護者於程序中應為投訴人之利益進行辯護，並可獲得機密之國家安全資訊並應確保該資訊安全[126]。

DPRC 法官由司法部長、美國商務部部長、情報總監與隱私與公民自由監督委員會（Privacy and Civil Liberties Oversight Board，下稱「PCLOB」）共同協商以任命[127]，並以三人組成小組審查自 CLPO 上訴之案件[128]。DPRC 之決定對情報機構亦有拘束力，並且情報機構不得影響其決定，同時 DPRC 之法官與 CLPO 相同，不得被隨意解職，也不得被影響[129]。同時，DPRC 也只會作出「沒有發現任何違規行為」，或是「DPRC 已經發布了要求適當補救之決定」之回應[130]。

PCLOB 被鼓勵針對 CLPO 以及 DPRC 所處理之投訴案件進行年度審查，包括(1)其是否及時處理投訴、(2)是否能完整存取必要之資訊、(3)是否按照 EO 14086 運作以及(4) CLPO、DPRC 以及情報機構是否能有效貫徹 EO 14086 之保障措施[131]。

第二款 小結

本文認為，EO 14086 進行了諸多改革。首先，其具體的指出了情報行動的目標，應能有效限縮情報機構的監控範圍。其次，其建立了具備一定獨立性的事後救

[125] *Id.* sec. 3, §§ (c)(i)(E)(2)-(3).
[126] *Id.* sec. 3, § (d)(i)(C).
[127] *Id.* sec. 3, § (d)(i)(A).
[128] *Id.* sec. 3, § (d)(i)(B).
[129] *Id.* sec. 3, §§ (d)(ii)-(iv).
[130] *Id.* sec. 3, § (d)(i)(H).
[131] *Id.* sec. 3, § (e)(i).

doi:10.6342/NTU202504586

濟機制，為美國情報法規的首例，可說是一項大幅度的制度改革。此外，亦有許多監督機構，特別是 PCLOB 發布之報告應能提高情報行動的透明性，以強化監督效果。惟行政命令的本質即不約束總統的權力，可以被總統隨意變更，此亦反映在總統得以增加合法蒐集目標的規定上，故留下了隱憂。

第二節 歐盟資料保護法律

第一項 憲法層面

歐盟將資料隱私納為基本權利之一環，在憲法層面由兩個系統所組成[132]，包括歐洲人權公約（Convention for the Protection of Human Rights and Fundamental Freedoms，下稱「ECHR」），以及歐洲聯盟基本權利憲章[133]（Charter of Fundamental Rights of the European Union，下稱「EUCFR」）。ECHR 第 8 條反映了具體之隱私權，規定：「每個人都有權要求尊重其私人和家庭生活、住所和通信[134]」，而 EUCFR 更進一步保障了個人資料保護權利，EUCFR 第 8 條規定：「每個人都有權保護與

[132] Perumal, *supra* note 5, at 104.

[133] 歐盟之資料隱私相關規範相當多元，為避免重複，以下將以歐盟隱私相關規範、歐盟標準以及歐盟法之保護水準等涵蓋性詞語，表示歐盟整體之隱私規範。其中相關之重要規範包括：歐洲聯盟基本權利憲章第 7 條之對私人和家庭生活之尊重、第 8 條之個人資料保護，以上二者係個人資料被傳輸至外國時被認為受到不正當之存取時所涉及之條文。第 47 條之獲得有效救濟以及公平審判之權利係 CJEU 於審查美國所建立之救濟機制是否能夠有效於歐盟人民之權利不受到保障而需要救濟時給予保護時之法源基礎。另外第 52 條第 1 項則規定對基本權利之限制應有之必要性及比例原則，在審查美國情報機構之監控行為之程度是否為對基本權利為最小程度之限制時作為法源基礎。另外歐洲人權公約雖然並非歐盟法之一部分，但其解釋對歐盟相關規範產生重要影響。Charter of Fundamental Rights of the European Union, arts. 7-8, 47, 2000 O.J. (C 361) 1 [hereinafter EUCFR]; Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR].

[134] ECHR, *supra* note 133, art. 7.

doi:10.6342/NTU202504586

其相關的個人資料。此類資料必須公平的為特定目的處理，並基於相關人員的同意或法律規定的其他合法基礎。每個人都有權存取與其相關之已被蒐集之資料，並有權要求更正。這些規則的遵守應由獨立機構監管[135]」。

第二項 Directive 95/46/EC

隱私指令是歐洲聯盟執行委員會（European Commission，下稱「歐盟執委會」）發布的關於個人資料保護的歐盟層級的指令，其具體反映歐盟對於將個人隱私作為基本人權的做法，強調人民對於資料所擁有的資訊自決權，得以掌控個人資訊的取得、存儲、使用、揭露、以及對已儲存資料的存取與更正[136]。隱私指令的存在確保歐盟成員國皆提供充足的隱私權保護，並使個人資訊可以在成員國間自由流通並同時得到保護[137]。

隱私指令雖作為歐盟等級的文件，但其是一個指令，故其並不具備可直接被適用的法律地位，本質上係加諸歐盟成員國自行立法實踐隱私指令之標準[138]。在隱私指令下，各國透過各自立法，使境內的相關事務適用該國的法律[139]，各國並應設置獨立的主管機關以監管相關活動[140]。

隱私指令的規範相當廣泛且嚴格，涵蓋所有個人資料（Personal Data）[141]。個

---

135 EUCFR, *supra* note 133, art. 8.
136 Reidenberg, *supra* note 13, at 732.
137 *Id.* at 732.
138 *Id.* at 718-19; 戴豪君、林其樺 (2018)，〈政府與產業因應 GDPR 之調適措施〉，《台灣經濟論衡》，16 卷 3 期，頁 15。
139 *Id.* at 733.
140 *Id.*
141 Directive 95/46/EC, *supra* note 6, art. 8.1.

doi:10.6342/NTU202504586

人資料包含已識別或可識別者（Identified or Identifiable），特別是種族或族裔、政治意見、宗教或哲學信仰、工會會員身分、健康、以及與性生活相關等的敏感資訊[142]。若欲處理（Process）涵蓋的個人資料，原則上應得到該資料主體（Data Subject）的明確同意[143]。

隱私指令跨境資料傳輸規定在第 25 條，該條規定僅在資料傳輸不會對遵守其他規定產生負面影響時始得為之，也就是對傳輸資料必須提供「適當的保護水準（Adequate Level of Protection）」才可以進行[144]。被歐盟執委會認定具備充分保護水準的國家，即獲得「適足性認定」，此為隱私指令的基石[145]。若資料的接收者所在的國家並不具有充分保護水準，該接收者可以透過隱私指令第 26 條的例外規定，包括資料主體的明確同意[146]、為履行資料主體以及資料掌控者間契約或先契約義務所必要[147]、為締結或履行資料掌控者及第三者之間對資料主體有利者[148]、為公共利益或法律主張上所必要[149]、為保護資料主體重大利益所必要[150]、依法律應作為可查詢之公開資訊[151]、以及適當的保障措施，例如適當的契約條款[152]與歐盟執委會發布的 SCCs[153]。

---

142 *Id.* art. 1(a).
143 *Id*. art. 7(a).
144 *Id.* art. 25.1; 戴豪君、林其樺，前揭註 138，頁 18。
145 Jung, *supra* note 14, at 8.
146 Directive 95/46/EC, *supra* note 6, art. 26.1(a).
147 *Id.* art. 26.1(b).
148 *Id.* art. 26.1(c).
149 *Id.* art. 26.1(d).
150 *Id.* art. 26.1(e).
151 *Id.* art. 26.1(f).
152 *Id.* art. 26.2.
153 *Id.* art. 26.4.

doi:10.6342/NTU202504586

隱私指令對美國資料相關權利、實踐以及政策帶來相當大的壓力。鑑於美國缺乏資料隱私相關的法律保護，適足性之評估本質上極為困難。除了歐盟等級的規範需要配合外，各國各自獨立的主管機關亦在個案上擁有些微的決定權力[154]，這使得將歐洲內蒐集的資訊傳輸至美國的業務受到威脅[155]。而相對的在透過隱私指令的協調後，儘管仍存在些微差異，歐盟國之間的資料傳輸受到的阻礙則較為輕微，給予了歐洲公司競爭優勢[156]。

第三項 General Data Protection Regulation

第一款 基本規範

GDPR 是歐盟於 2018 年 5 月 25 日正式施行，用以取代並完善隱私指令的規則，以應對更加數據化的現今社會[157]。在施行的約莫兩年之前，其最終版本於 2016 年 4 月 14 日公布，給予適用的機構 2 年的時間調整並適應新的規則，受到了機構的重視[158]。

GDPR 作為規則（Regulation），得以直接產生法律效力，毋需經由各國國內立法程序進行轉換[159]。當時被論者稱為最嚴格的資料相關法律[160]，為美國從事有關歐盟人民資料的機構帶來巨大的挑戰。GDPR 有著更多的合規要求以及嚴厲的經濟

154 Reidenberg, *supra* note 13, at 736.
155 *Id.* at 735.
156 *Id.*
157 Jung, *supra* note 14, at 10.
158 *See id.* at 10-11.
159 張志偉（2018），〈歐盟資料保護基本規則導論〉，《月旦司律評》，創刊號，頁 166。
160 *Id.* at 12.

doi:10.6342/NTU202504586

處罰機制[161]，亦已發生數起大型美國公司遭到開罰的紀錄，例如法國資訊自由委員會（Commission nationale de l'informatique et des libertés，下稱「CNIL」）於 2019 年因為 Google 公司缺乏 GDPR 要求的透明性、不適當的資訊以及缺乏適當的廣告個人化的同意機制而處罰其 5,000 萬歐元的罰鍰[162]；隨後 2023 年 CNIL 再次因為 Google 公司在 Cookies 的同意與否的選擇上，拒絕的選項不如同意的選項容易選取，而再次對 Google 開出 1 億 5 千萬歐元罰鍰的處罰[163]。此外愛爾蘭資料保護委員會（Irish Data Protection Commission，下稱「DPC」）針對 Meta 系列公司亦有處罰，例如於 2023 年針對 Facebook 和 Instagram 違反跨大西洋資料傳輸規定處罰 Meta Platforms Ireland Limited（下稱「Meta Ireland」）3 億 9 千萬歐元的罰鍰[164]等等。此罰鍰數額對此類大型公司來說並不是可以忽視的數字，可見 GDPR 在執行以及規範上對歐盟人民的隱私有更實質的保護，大型公司也不得不更加認真對待 GDPR 的規範要求，與過去隱私指令以及安全港協議時期時常被隨意違反的情況有所不同[165]。

第二款 跨境資料傳輸之限制

---

161 *Id.*

162 *The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against GOOGLE LLC*, EDPB (Jan. 21, 2019), https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en.

163 *Closure of the injunction issued against GOOGLE*, CNIL (Aug. 1, 2023), https://www.cnil.fr/en/closure-injunction-issued-against-google#:~:text=On%2031%20December%202021%2C%20in,to%20accept%20them%2C%20within%20three.

164 *Facebook and Instagram fined €390m over GDPR breaches*, ILN (Jan. 5, 2023), https://www.irishlegal.com/articles/facebook-and-instagram-fined-eur390m-over-gdpr-breaches.

165 Jung, *supra* note 14, at 12.

doi:10.6342/NTU202504586

GDPR 關於跨境資料傳輸之限制以及授權主要規定在第五章中。GDPR 對跨境資料傳輸採取「原則禁止，例外允許」之規範方式[166]。GDPR 第 44 條原則上禁止將資料主體[167]的資料傳輸至第三國及其他國際組織，或是在第三國及其他國際組織間傳輸。而例外規定則規定於 45 條以下[168]。

首先，GDPR 第 45 條第 3 項係適足性認定之基本規定，即歐盟執委會在評估第三國有充分保護水準並透過通過法案認定該國有與歐盟實質相當之資料隱私保護水準後，得授予該國適足性認定[169]。得到適足性認定之國家收受資料則不需要再獲得個別授權[170]。在認定是否授予適足性認定時，歐盟執委會應考量法治、對人權之尊重以及自由，包括關於公共安全、國防、國家安全、刑事法律，也包括上述法律之施行與立法、是否有獨立之救濟手段、以及相關國際承諾等[171]。截至 2025 年 7 月止，世界上有十二個國家獲得適足性認定，另外有三個國家，包括本文討論之美國，獲得有限之適足性認定[172]，足見其有一定之嚴格程度。

GDPR 第 46 條另外允許在有適當保護措施（Appropriate Safeguard）之情況下傳輸資料。適當保護措施包括歐盟執委會制定之 SCCs、歐盟資料保護機構核准的

---

166 廖淑君，前揭註 18，頁 119。

167 GDPR 將個人資料定義為可以連結到已識別或可識別之自然人，也就是資料主體。GDPR, *supra* note 8, art. 4(1).

168 *Id.* art. 44.

169 *Id.* art. 45(3).

170 *Id.* art. 45(1).

171 *Id.* art. 45(2); 戴豪君、林其樺，前揭註 138，頁 20-21。

172 *Adequacy Decisions*, EUR. COMM'N, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Mar. 9, 2025).

doi:10.6342/NTU202504586

資料保護契約條款、行為守則、以及有拘束力的承諾等[173]；此外第 49 條亦有七種例外規範，包括資料主體之明確同意，以及為保護其他重要利益所必要等等[174]。

GDPR 將 SCCs 與拘束性的公司規則（Binding Corporate Rules）視為合法將資料傳輸出歐盟的架構，創造更廣的合法傳輸管道，對美國公司來說，選擇違反規則變得成本更高；相反的，使歐盟人民的隱私更能得到符合歐盟標準的保障為更合理的選擇[175]。

[173] GDPR, *supra* note 8, arts. 46-47.

[174] *Id.* art. 49(1); 例外得進行資料傳輸之條件包括：

> 「(a)資料主體在已被告知欠缺適足性認定與適當保障措施所可能產生之風險後，已明確同意該項傳輸；
> (b)該傳輸為履行資料主體與資料控制者間契約或應資料當事人之要求所彩取之前契約措施所必要；
> (c)為締結或履行資料控制者與其他自然人或法人之間，基於資料主體利益所締結之契約所必要之傳輸；
> (d)為重大公共利益所必要之傳輸；
> (e)為建立、行使或抗辯法律主張所必要之傳輸；
> (f)資料主體因生理或法律因素無法給予同意時，資料主體或第三人之重要利益需收保護時；
> (g)根據歐盟法或成員國國內所規範之具體情況下，為提供一般大眾或可證明之利害關係人查詢所為之登記所需之傳輸。」

[175] Jung, *supra* note 14, at 15.

doi:10.6342/NTU202504586

第三節 小結

本章介紹了美國情報法規的演變，並說明了其所面臨的批評，包括情報行動的廣泛授權、缺乏監督與救濟機制。EO 14086 則是帶來了顯著的改革，對多數問題作出了回應，但是其是否能有效的改善情報機構權力過大的問題仍有疑問。

此外，本章亦介紹了歐盟的資料隱私保護法規，並聚焦於跨境資料傳輸的規範。欲將資料自歐盟傳輸至歐盟以外的國家或地區時，需要滿足特定的例外條件，其中美國透過建立資料傳輸架構以獲得適足性認定，並在合作過程中，面臨了 CJEU 設下對基本權利保護的高標準所帶來的阻礙。本章將於第三章詳細說明歷來的三個資料傳輸架構面臨的問題，以及 CJEU 在過程中透過先行裁決建立的適足性認定標準。

doi:10.6342/NTU202504586

第參章 歐美跨境資料傳輸協議之演變

本章將先依次介紹安全港協議與隱私盾協議的背景和內容，並詳細說明兩者與相應時代背景下的美國情報法規在 CJEU 的先行裁決中所受到的評價，以及兩者之間有何異同。在 Schrems I 與 Schrems II 案中，亦分析 CJEU 要求的資料保護水準，以便後續對現行法規進行分析。

隨後，本章將介紹現行的資料傳輸架構——DPF，並分析其與前兩者之間的異同。透過分析其在談判與審議過程中所收到的意見，以辨明 DPF 在各項議題上與前二者之不同，以及其所為之改革與 CJEU 之標準之間是否仍存在差異，進而分析其前景與可能尚待改革之議題。

第一節 Safe Harbor Agreement

第一項 安全港協議架構

在貿易層面，歐盟執委會基於隱私指令第 26 條給予的適足性認定，對一國服務提供者在歐盟境內提供服務會帶來相當的競爭優勢[176]。為了避免隱私指令導致美國機構無法再合法將蒐集的歐盟人民資料傳輸至美國，從而損失競爭優勢，美國商務部開始與歐盟執委會談判，在 2000 年 7 月建立名為安全港協議[177]的一套關於傳輸資料之隱私保護規則，並由歐盟執委會給予其適足性認定（下稱「Decision

[176] Tsai-fang Chen, *Non-Discrimination Under the Most-Favoured-Nation Obligation and Adequacy Decisions in the General Data Protection Regulation*, ASIAN J. WTO & INT'L HEALTH L. & POL'Y 309, 328-29 (2023).
[177] Reidenberg, *supra* note 13, at 738.

doi:10.6342/NTU202504586

2000/520」）[178]。

依安全港協議，美國機構每年將自我認證其符合安全港協議之要求，以取得直接從事跨大西洋資料傳輸之資格。美國機構違反安全港原則時由美國聯邦交易委員會（Federal Trade Commission，下稱「FTC」）以其從事不公平競爭為由進行執法[179]，以使歐盟得以在保護個人資料，以及跨境資料傳輸的現實需求間取得平衡[180]。此協議並非使美國整體獲得適足性認定，而是透過授予安全港協議適足性認定，使自我認證之機構得以直接傳輸資料[181]。

安全港協議有七個主要的原則[182]：

1. 告知——蒐集資料的組織應明確且顯眼的給予資料主體關於蒐集資料的目的、機構的聯絡方式、可能得到資訊的機構，包括可能得到揭露的第三方的類型等等資訊。

2. 選擇權——蒐集資料的組織應提供資料主體在資料將被提供給第三方，或是資料將被用在不符合最初蒐集時的目的時，享有退出權，亦即可不再授與資料使用權，並且資料主體此一選擇機制應明確且顯眼。於個案資料屬於敏感資訊時，蒐集資料的組織應提供資料主體事前的主動同意權。

---

[178] Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 O.J. (L 215) 7.
[179] Tzanou, *supra* note 12, at 5; Gregory Shaffer, *Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance Through Mutual Recognition and Safe Harbor Agreements*, 9 COLUMBIA J. EUR. L. 29, 64 (2022).
[180] Shaffer, *supra* note 179, at 57-58.
[181] *Id.* at 61-62.
[182] *Id.* at 62-63; Jung, *supra* note 14, at 24-26.

doi:10.6342/NTU202504586

3. 持續傳輸——資料蒐集者在將資料傳輸給第三方時，應向資料主體提供相關資訊以及給予選擇權，並且確認該第三方有相等的隱私保障地位。唯有滿足此等要求，該最初的資料蒐集者始得在第三方違反隱私相關規定時免責。

4. 安全保障——資料蒐集者應確保資料不被曝光、不當使用、未授權存取、更改、喪失或損壞。

5. 資料完整性——資料蒐集者應確保資料不受到不合於目的的使用與處理，並盡力確保資料的準確、完整以及維持更新。

6. 可存取性——資料蒐集者應使資料主體得以合理存取以及更正資料，除非提供此等存取機制的成本與其所能保障的個人隱私不成比例，或是可能會侵害其他第三人的權利。

7. 執行——應存在一個機制可以確保資料蒐集者遵循安全港協議的規定，包括隨時可供使用並可負擔的追索機制，以及足夠嚴格的懲罰機制。此包括一個隨時可供資料主體使用的索償機制、核實系爭機構是否確實遵守應有的隱私規範的程序，以及補正系爭機構未能遵守隱私相關原則而產生的後果等。相關懲罰應足以確保資料蒐集者會遵守規則。

第二項 安全港協議之影響

安全港協議起初成功的作為政治上的調和劑，緩和了歐美雙方在此議題上可

doi:10.6342/NTU202504586

能產生的衝突與困難。此外當時歐盟內部仍有國家尚未完全完成立法轉換[183]，倘若其於進行隱私指令的必要轉換時強硬對待美國，可能會影響歐盟內部的討論[184]。美國內部也受到不希望直接適用隱私指令約束的壓力，而安全港協議可作為緩和壓力的暫緩機制[185]。

儘管安全港協議取得了政治上的成功，但也因此作出了許多妥協。有論者即在施行初期提出了諸多質疑。首先，其適用範圍相當狹窄，僅包含 FTC 以及美國交通部（United States Department of Transportation）管轄下的機構[186]，所以很多機構都不能適用。

其次，在歐盟境內設立設備以蒐集資料的機構也不能適用安全港協議。蓋隱私指令規定即使公司位於歐盟外，但只要使用在歐盟境內的設備蒐集資料，就會直接適用歐盟法律[187]。這會大幅影響以網站作為主體的公司，因為網站使用者均會以本地設備上網蒐集資料[188]，導致其必須直接適用歐盟法。

再者，基於安全港協議，歐盟主管機關可更加容易地辨識出未透過安全港協議自我認證的公司，此時就能更小範圍的調查並判斷其是否提供其他的保障機制，如此一來，美國公司將更容易暴露在被禁止從事跨大西洋的資料傳輸的風險下[189]。

---

183 隱私指令提供的轉換期僅到 1998 年 10 月，惟仍有若干國家直至安全港協議生效，因為未完成轉換而產生的訴訟仍在進行。Reidenberg, *supra* note 13, at 733.
184 *Id.* at 739.
185 *Id.*
186 *Id.* at 743.
187 *Id.*; Directive 95/46/EC, *supra* note 6, art. 4.1(c)
188 Reidenberg, *supra* note 13, at 743.
189 *Id.* at 743-44.

doi:10.6342/NTU202504586

除了上述缺點外，安全港協議本身對歐盟人民給予的保護也低於隱私指令的要求，例如不保護公開資料，以及美國在協調過程中宣稱存在但實際上無法實質發揮功能的救濟及求償機制[190]。

安全港協議的自我認證機制也不無問題，因為欠缺主管機關或是第三方認證機構等管控機制的緣故，適用機構有自行解釋的空間[191]；歐盟發行的法律文件亦表示安全港協議下的自我認證機制的驗證可以自行驗證或是由外部機構驗證[192]，如此恐無法完全滿足歐盟所欲達到的隱私保護水準。最終安全港協議在 2015 年 10 月 6 日被歐盟法院於著名的 *Maximillian Schrems v Data Protection Commissioner*（下稱「Schrems I」）案中宣告無效。其中即提及安全港協議在其運作期間的自我認證機制是否得以有效保護歐盟人民的隱私權利，此亦為安全港協議最終被宣告無效的主要理由之一[193]。

安全港協議因為缺乏實質有效的監控手段，其實效備受質疑。實際上美國機構的遵循情形也並不理想，自我認證過的機構並未完全實踐安全港協議的標準，未自我認證卻冒充受認證機構身分運作也時有發生[194]。隨著科技的飛速發展，跨大西洋的資料流動也指數性的攀升[195]，再加上 2013 年被揭發的斯諾登事件[196]更加凸顯了資料隱私的重要性及風險，故歐盟於 2013 年推動了安全港協議的修正，提出 13 項

190 *Id.* at 744-46.
191 Jung, *supra* note 14, at 27.
192 2000 O.J. (L 215) 16.
193 Jung, *supra* note 14, at 28.
194 *Id.* at 29-30.
195 *Id.* at 30.
196 *Edward Snowden: Leaks that Exposed US Spy Programme*, BBC (Jan. 17, 2014), https://www.bbc.com/news/world-us-canada-23123964.

doi:10.6342/NTU202504586

修正建議以利安全港協議可以持續妥善運作[197]。

雖然歐盟執委會與美國商務部有意談判修正版的安全港協議，以對歐盟資料主體提供更完善的資料保護[198]，但最終未能在 Maximilian Schrems（下稱「Schrems」）提起之訴訟完結前完成，安全港協議的適足性認定也在 2015 年 10 月 6 日被歐盟法院宣告無效。

第三項 Safe Harbor Agreement 的消亡——Schrems I 案

Schrems I 案的原告是一位來自奧地利的資料隱私推動者 Schrems[199]，其最初的訴求源自於斯諾登曝光美國用以大規模蒐集資料並監視人民的稜鏡計劃[200]（Planning Tool for Resource Integration, Synchronization, and Management，下稱「PRISM」）[201]，一個允許 NSA 取得美國大型科技公司的中央伺服器內資料的計劃[202]。其於 2013 年 6 月向 DPC 提出申訴，控訴 Facebook Ireland Ltd（下稱「Facebook Ireland」）違反隱私相關規定讓 NSA 監控其自歐盟境內蒐集之資料，故要求 DPC 禁止 Facebook Ireland 將其資料傳輸至美國[203]。隨後 DPC 認定沒有證據顯示 Facebook 允許 NSA 存取其資料，且美國與歐盟之安全港協議具備適足性認定而不需要進行進一步之調查，故將其駁回[204]。

---

197 Jung, *supra* note 14, at 22.
198 Terpan, *supra* note 3, at 1056.
199 Jung, *supra* note 14, at 31.
200 Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶ 28 (Oct. 6, 2015).
201 Tzanou, *supra* note 12, at 2-3.
202 *Id.*
203 *Id.* at 3.
204 Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶ 29 (Oct. 6, 2015).

doi:10.6342/NTU202504586

敗訴的 Schrems 以 DPC 作為被告在愛爾蘭高等法院（下稱「高等法院」）進行控訴。高等法院認為美國情報機構的監視是單方面且秘密的，歐盟人民的權利無法得到保障，需要證實此等限制在國家安全問題上是具備必要性且符合比例原則的。此外，美國是否提供適足的保護仍存疑，故以愛爾蘭法律的觀點，DPC 應該要繼續進行調查[205]。高等法院隨後認為雖然 Schrems 並未提出爭執，但此案件觸碰到安全港協議之適足性認定是否有效，故應停止訴訟程序並送至 CJEU，就系爭案件中調查的獨立機構是否受到該適足性認定決定的拘束進行先行裁決[206]。

CJEU 在其先行裁決中認定，依隱私指令的制度設計，儘管歐盟執委會已經授予適足性認定，但並不防止會員國內的獨立監管機構審查系爭資料傳輸的合法性[207]，否則將阻止資料主體向獨立資料保護機構提出申訴的權利[208]。

CJEU 在先行裁決中亦進一步釐清，授予適足性認定並不以具有與歐盟完全相同的法律規範為必要，僅是需要有「實質相當」的保護水準[209]。但即使如此，法院也表示其他國家之隱私規範應該以歐盟的高標準作為目標[210]。惟對於何謂具備適足性，CJEU 在 Schrems I 案中並未給出明確的認定標準，僅透過隱私指令第 25 條第 6 項說明跨境資料傳輸的接收國應「確保」有適足性之保護，且適足性之判斷應基於「保護個人的私人生活以及基本自由及權利」[211]。

---

[205] *Id.* ¶¶ 30-33.
[206] *Id.* ¶¶ 34-36.
[207] *Id.* ¶ 57.
[208] *Id.* ¶¶ 58, 66.
[209] *Id.* ¶ 73.
[210] *Id.*
[211] *Id.* ¶ 71.

doi:10.6342/NTU202504586

至於在給予適足性認定的審查上，CJEU 認為個人資料保護在尊重私人生活基本權利方面有其重要角色，且當個人資料被傳輸到不能確保充分保護水準的第三國時，其基本權利可能受到侵害的人數眾多，故歐盟執委會在判斷是否給予適足性認定時，其裁量權應收縮，應該要以嚴格的標準審視之[212]。

至於自我認證機制之合法性問題，CJEU 認為自我認證機制本身並不違反隱私指令第 26 條第 6 項的要求，但是一個有效的管理機制對於保護基本權利是必要的[213]。CJEU 指出，在安全港協議的制度設計上，其設下之資料保護原則是可以在與「國家安全、公共利益或執法要求」相衝突下退讓的[214]，且 CJEU 一再強調此等對資料的存取是一般性、無差別的，此種對基本權利的限制本身很難滿足 EUCFR 第 7 條之要求[215]。CJEU 同時也指出，歐盟執委會在隨後也強調美國並無法提供安全港協議所要求的保護以及有效的申訴管道[216]。此等缺陷皆無法確實保障歐盟人民的基本權利，故 CJEU 最終認定安全港協議之適足性認定決定無效。

隨後 CJEU 又針對 Decision 2000/520 第三條表示意見。其認為該條第一項規定，歐盟國會員的主管機關對於適足性認定是否足以保護資料主體權利的認定權限設下過多限制，構成不當限制資料保護機構之權力，相當於剝奪資料主體之權利[217]，違反隱私指令的要求，故此 Decision 2000/520 之第三條亦應為無效[218]。最後

---

212 *Id.* ¶ 78.
213 *Id.* ¶ 81.
214 *Id.* ¶¶ 84-86.
215 *See id.* ¶¶ 84-94.
216 *Id.* ¶¶ 90, 95.
217 *Id.* ¶¶ 99-103.
218 *Id.* ¶ 104.

doi:10.6342/NTU202504586

因為 Decision 2000/520 之第 1，3 條應與第 2，4 條不可分割，故 Decision 2000/520 至此全部無效[219]。

第四項 小結

事後以觀，安全港協議之設計並沒有針對美國情報機構廣泛監視且無節制之大規模蒐集計劃、以及外國人對於受到監視基本上毫無救濟管道的問題提出回應，其設計基礎基本上只是形式上回應並建構得以直接跨境傳輸資料的橋樑。換言之，歐盟執委會作出適足性認定主要還是基於政治與經濟考量，可見強大經濟實力帶來之影響力，但安全港協議最後還是在司法審查中下敗下陣來。

Schrems I 案判決指出了本案的根本爭議，也就是美國一方面在保護國家安全上較為激進之做法，另方面缺乏有效的中央監管與求償機制。惟有學者提出，Schrems I 判決通篇除了要求授予適足性認定應建立在與歐盟有實質相當的資料保護水準之外，並未針對美國的資料保護規範進行實質性的分析及認定，僅係以其規範侵害了歐盟隱私規範之本質（Essence）[220]而認定不能給予適足性認定，論證似有不足。只是因為安全港協議本身之缺陷較為重大，對於國家安全等目的之蒐集資料範圍基本不受限制，救濟手段也趨近於不存在[221]，故本文認為，CJEU 或許不需要詳細分析歐盟標準之保護水準及安全港協議之差異，即可作出安全港協議以及

[219] *Id.* ¶¶ 105-06.
[220] *See generally* Tzanou, *supra* note 12; Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, ¶¶ 94-95 (Oct. 6, 2015).
[221] Sara Gerke & Delaram Rezaeikhonakda, *Privacy Shield 2.0- A New Trans-Atlantic Data Privacy Framework Between the European Union and the United States*, 45(2) CARDOZO L. REV. 351, 361 (2023).

doi:10.6342/NTU202504586

美國法規不具備適足性之結論。

本文認為，本案中 CJEU 之著力點在於安全港協議本質的制度設計。在美國情報法規授權情報機構得以大規模、無差別的蒐集資料的背景下，安全港協議又以美國法為優先，其將國家安全、公共利益以及執法要求置於優先地位的設計本身，即無法滿足歐盟法的要求，也就沒有詳細審視其它具體的資料保護規範，或是實務的必要。

Schrems I 案聚焦在美國對於其國家安全、公共利益以及執法等目的所為之監視行為、司法救濟管道之缺失。其同時確認歐盟境內應有資料保護機構，並且有保護資料主體權利之義務。整體而言，就歐美之間對於資料隱私保護之爭議而言，Schrems I 案仍為較為早期之階段，但其觀點仍為日後之討論奠定一定基礎，並指明了發展的主要方向。

第二節 Privacy Shield

第一項 隱私盾協議架構

隱私盾協議是在安全港協議被宣告無效後，美國與歐盟執委會在 2016 年 2 月達成用以取代安全港協議的資料傳輸協議[222]，歐盟執委會並在 2016 年 7 月 12 日授予其適足性認定（下稱「Decision 2016/1250」）[223]。

[222] Terpan, *supra* note 3, at 1046.
[223] Commission Implementing Decision (EU) 2016/1250 Of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 281) 31 [hereinafter Decision 2016/1250].

doi:10.6342/NTU202504586

隱私盾協議的架構相對複雜，包括歐盟執委會的適足性認定[224]、美國商務部增強隱私保護以及與歐盟方面合作之承諾[225]、美國商務部的隱私盾原則[226]、美國國務卿對於會確實執行監察專員機制之信件[227]、FTC 對於(1)優先處理和調查轉介之案件；(2)處理虛假或欺騙性的隱私盾協議資格聲明；(3)持續的命令監督；以及(4)與確實執行與歐盟資料保護機構加強執法合作等的承諾[228]、美國交通部對於(1)優先調查涉嫌違反隱私盾協議的行為；(2)對作出虛假或欺騙性隱私盾認證聲明的實體採取適當執法行動；以及(3)監督並公開有關隱私盾協議違規的執法命令之承諾[229]、情報總監辦公室法務長對情報活動之說明[230]、美國司法部國際事務助理總檢察長兼顧問對於自企業獲取商業資料和其他紀錄資訊，以供刑事執法或公共利益目的的主要調查工具的簡要概述[231]。

作為安全港協議的替代品，在經歷 Schrems I 案後，隱私盾協議在規範層面上有些許改善。首先與先前的安全港協議相同，隱私盾協議採取自我認證的方式，蓋此方式在 Schrems I 案中未被認定為不妥，只是其監管不足成為問題，故在隱私盾協議中，欲自我認證之機構須作出更多承諾並受到美國商務部的監督。其次，情報總監承諾國家安全機構存取來自歐盟資料時，會有明確的限制與控制，且歐盟執委會、美國商務部、以及歐美雙方各自的資料保護機構會每年進行審查。再者，歐盟

[224] *Id.* art. 1.
[225] *Id.* annex I.
[226] *Id.* annex II.
[227] *Id.* annex III.
[228] *Id.* annex IV.
[229] *Id.* annex V.
[230] *Id.* annex VI.
[231] *Id.* annex VII.

doi:10.6342/NTU202504586

人民有更好的救濟機制可以進行有效的控訴[232]。

此外，在隱私盾協議下，美國政府設立了新的監督機制——申訴專員（Ombudsperson）[233]，以作為獨立的審查機關。另外，歐巴馬政府在 2016 年 2 月 24 日制定司法救濟法（Judicial Redress Act），以賦予歐盟人民在美國受到與美國人民同等的美國隱私法（Privacy Act of 1974）保護[234]。

雖然有上述之改進，但隱私盾協議仍有缺失。首先，Schrems I 案下，國家安全例外議題是導致安全港協議的適足性認定無效的的導火索。與安全港協議所採取的一般例外規定不同，新的隱私盾協議有較為清楚的規範，包括國家安全例外適用的要件，以及相關的監督與問責機制等等[235]，但事實上美國並未實質承諾其會遵從歐盟基本的隱私權要求[236]。再者，關於自動蒐集資料的限制不足，以及並未刪除無用資料等缺陷，依舊存在[237]。另外，在 Schrems I 案中相當重要的實質有效監控與救濟機制有效性等問題，也懸而未決[238]。

另一個 Schrems I 案中凸顯的重大問題為情報機構的無限制蒐集資料問題，雖然主管機關承諾會對大規模蒐集資料有所限制，但就法律層面而言，美國相關法規並無實質限制[239]，故本文認為，可以預期司法審查時此承諾很難被視為是有效的限制手段。

---

232 Terpan, *supra* note 3, at 1051.
233 Decision 2016/1250, *supra* note 223, recital 116.
234 Terpan, *supra* note 3, at 1051.
235 *See* Tzanou, *supra* note 12, at 12.
236 *Id.* at 12-13.
237 Terpan, *supra* note 3, at 1051.
238 *Id*.
239 *Id*.

doi:10.6342/NTU202504586

最後，關於隱私盾協議新設的獨立監督機構——申訴專員，歐盟執委會在 Decision 2016/1250 中直接提及對其獨立性的疑慮[240]。另外，歐盟執委會在給予安全港協議時並未實質審查美國的資料保護規定，也被 CJEU 指出並予以批評，但在處理隱私盾協議時，歐盟執委會仍無此等實質審查[241]，故隱私盾協議仍處於較大的法律風險之中。

隱私盾協議的本質並非一個具備法律性質的協議或是承諾，而是一個美國主管機關提出的文件[242]，其中國務卿（Annex 3）、FTC 主席（Annex 4）、美國交通部部長的信件或許至多可以被稱為是行政協議（Executive Agreement），但情報總監與助理司法部長（Assistant Attorney General）的信件因為並未被送至歐盟機構，故無法構成行政協議[243]。

實際上，隱私盾協議被認為只是安全港協議的重新包裝，並無實質改變[244]。多數觀點認為隱私盾協議對 Schrems I 的回應並不完整[245]，若再次受到 CJEU 的司法審查，很可能再次面臨被宣告無效的下場。但事實上，考量到美國與歐盟對於隱私保護的巨大差異，短期內要求美國大幅修正其整體法制，恐仍難以期待[246]；另一方面，歐盟仍有相當程度的經濟上需求，而歐盟執委會將經濟需求放在相當高的順位[247]，故隱私盾協議仍有其存在的理由。基此，隱私盾協議的適足性認定在 2020 年

[240] Decision 2016/1250, *supra* note 223, art. 1(124).
[241] Terpan, *supra* note 3, at 1052.
[242] *Id*.
[243] *Id*.
[244] Connolly, *supra* note 61, at 100.
[245] *See id.*; Terpan, *supra* note 3, at 1053.
[246] Terpan, *supra* note 3, at 1057.
[247] *Id.* at 1058.

doi:10.6342/NTU202504586

7月16日最終被CJEU宣告無效[248]，也就是*Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*（下稱「Schrems II」）案。

第二項 再次失敗——Schrems II 案

Schrems I 案後，該案被撤銷發回 DPC 調查，而 Facebook Ireland 表示其將歐盟內蒐集之資料傳輸至美國的 Facebook Inc.是基於 SCCs[249]，即一套歐盟執委會[250]批准之合約條款（下稱「Decision 2010/87」）[251]，並要求 Schrems 重新提出其主張[252]。Schrems 嗣後主張即使是依據 SCCs，亦不改變美國情報機構蒐集其資料的事實，故要求 DPC 禁止 Facebook Ireland 將其資料傳輸至 Facebook Inc.[253]。

由於本次 Schrems 的主張會涉及批准 SCCs 之 Decision 2010/87 之有效性，故 DPC 在 2016 年 5 月 31 日將此爭議起訴至高等法院，以使高等法院將其送至 CJEU 進行先行裁決[254]，而後高等法院於 2018 年 5 月 4 日將案件送至 CJEU[255]。

第一款 愛爾蘭高等法院之認定

---

[248] PRIVACY SHIELD, https://www.ftc.gov/business-guidance/privacy-security/privacy-shield (last visited Feb. 25, 2025).

[249] Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd & Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 54 (July 7, 2020).

[250] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, 2010 O.J. (L 39) 5. [hereinafter Decision 2010/87]

[251] 此為第二版本，第一版本為 Commission Decision of 15 June 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, Under Directive 95/46/EC (Notified Under Document Number C(2001) 1539), 2001 O.J. (L 181) 9 所批准。

[252] Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd & Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 54 (July 7, 2020).

[253] *Id.* ¶ 55.

[254] *Id.* ¶ 57.

[255] *Id.*

doi:10.6342/NTU202504586

高等法院在移送文件中附上其調查結果，其中提及美國的情報活動的授權基礎來自於 FISA 第 702 條以及 EO 12333。FISA 第 702 條授權司法部長以及情報總監在經過 FISC 的同意下許可監視外國人的行動，此為 PRISM——透過大型網路服務商獲取用戶之私人通訊[256]——與上游監控計劃[257]（UPSTREAM）————透過直接獲取海底電纜等基礎設施，以直接獲得原始傳輸的資料[258]——的授權基礎[259]。本文主要係討論資料可能因被情報機構要求提供而傳輸至美國機構，故與 PRISM 之關聯性較高。CJEU 認為，PPD 28 僅係要求情報行動應「盡可能量身定制」[260]，故高等法院認為此等限制並無法滿足必要性與比例原則的要求[261]。

針對司法保障問題，美國最主要用以規範違法監視的法源基礎係來自美國憲法第四修正案[262]，然而此等權利並不適用於歐盟人民，故可能對歐盟人民的訴訟權保障造成巨大障礙[263]。另外，申訴專員本質上亦非 EUCFR 第 47 條所要求之法院，故歐盟人民在「司法」上仍難以獲得保障[264]。

高等法院提出了兩個主要問題：其一是當資料被傳輸至第三國並可能被該國的政府機構——在本案尤其是國家安全機構——處理時，歐盟的相關法律是否適

256 Gemar, *supra* note 23, at 500-01.

257 UPSTREAM 計劃係指 NSA 透過電信企業複製和過濾網路流量已取得資訊之計劃。Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd & Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 62.

258 Gemar, *supra* note 23, at 499-500.

259 *Id.* ¶ 61.

260 Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd & Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 64 (July 7, 2020); PPD 28, *supra* note 66.

261 Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd & Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 64 (July 7, 2020).

262 U.S. CONST. amend. IV.

263 Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd & Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 65 (July 7, 2020).

264 *Id.*

doi:10.6342/NTU202504586

用？其二是歐盟執委會的適足性認定，在基於 SCCs 的跨境資料傳輸下，是否拘束歐盟成員國的主管機關[265]？高等法院進一步認為，Decision 2010/87 所定的 SCCs 並不能拘束該第三國，故難以保障資料主體之權利[266]；另外高等法院指出，Decision 2010/87 賦予歐盟成員國主管機關即使在使用 SCCs 的情況下依舊可以認定第三國之保護不足而禁止傳輸資料[267]，故使用 SCCs 亦不能保證資料受到充分的保障[268]。

高等法院基於上述認定，裁定停止訴訟程序，並將以下問題移送至 CJEU 進行先行裁決：

1. 當個人資料由歐盟成員國的私人公司基於商業目的，而根據 SCCs 傳輸給第三國私人公司，且該資料在第三國可能被其政府機構進一步處理，以用於國家安全目的，同時也可能用於執法和與第三國之外交事務時，在考量歐盟法規中與國家安全相關之規定後，歐盟法規是否適用於此資料傳輸[269]？

2. 當基於 SCCs 傳輸之資料可能被用於國家安全目的時，其是否侵害個人隱私權？根據隱私指令，應適用之標準應是歐盟層級之法律，或是成員國之法律？若為後者，是否也應包含其對牽涉到國家安全之情況之實踐[270]？

3. 在判斷第三國之個人資料保護水準是否符合隱私指令之要求時，應參考何等因素[271]？

---

265 *Id.* ¶ 66.
266 *Id.* ¶ 67.
267 Decision 2010/87, *supra* note 250, art. 4.
268 Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd & Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 67 (July 7, 2020).
269 *Id.* ¶ 68(1).
270 *Id.* ¶ 68(2).
271 *Id.* ¶ 68(3).

doi:10.6342/NTU202504586

4. 基於高等法院針對美國相關法律之事實認定，依據 SCCs 將個人資料自歐盟傳輸至美國是否侵害 EUCFR 第 7 條及第 8 條所賦予之權利[272]？

5. 基於高等法院針對美國相關法律之事實認定，美國提供之救濟途徑是否滿足 EUCFR 第 47 條之要求？如為肯定，美國在國家安全背景下對司法救濟施加之限制是否滿足 EUCFR 第 52 條的比例原則、並且不逾越民主社會中國家安全目的的必要範圍？

6. 依據 SCCs 傳輸至第三國之資料，在考量到隱私指令以及 EUCFR 第 25 條及第 26 條，應該考慮何等因素[273]？

7. SCCs 僅適用於締約雙方而不拘束第三國之政府機構，此一事實是否影響隱私指令第 26 條第 2 項所要求之充分保障[274]。

8. 當資料保護機構認為監控相關法律違反隱私指令第 25 條和第 26 條以及 EUCFR 時，資料保護機構是否必須暫停資料傳輸？或是考慮到 Decision 2010/87 序言第 11 條，僅在特殊情況下暫停之[275]？亦或是資料保護機構有自由裁量權[276]？

9. 基於隱私指令第 25 條第 6 項，認定隱私盾協議具備適足性之 Decision 2016/1250 是否拘束成員國之資料保護機構和法院，從而導出美國法規具有一般性的適足性認定？如果答案為否，它與依據 SCCs 傳輸到美國的資料是否受到充分保

[272] *Id.* ¶ 68(5).
[273] *Id.* ¶ 68(6).
[274] *Id.* ¶ 68(7).
[275] Decision 2010/87, *supra* note 250, recital 11.
[276] Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd & Maximillian Schrems, ECLI:EU:C:2020:559, ¶ 68(8) (July 7, 2020).

doi:10.6342/NTU202504586

障的評估有何關聯性[277]？

10. 根據高等法院對美國法律的事實認定，隱私盾協議中的申訴專員機制，結合美國現有制度，是否足以確保美國提供依 SCCs 傳輸到美國的個人資料的資料主體與 EUCFR 第 47 條所要求的救濟[278]？

11. Decision 2010/87 批准 SCCs 之決定是否違反 EUCFR 第 7 條、第 8 條以及第 47 條[279]？

第二款 CJEU 之裁決

第一目 程序問題

由於在程序進行中，GDPR 正式施行並取代先前之隱私指令，而 DPC 在移交先行裁決時引用者卻為隱私指令，故可能產生爭議。CJEU 在此問題上認為，因 GDPR 完整延續隱私指令之內容，且歐盟判例法要求 CJEU 應解釋所有與裁決事件相關之法律條款，故此規範之變更不會使系爭裁決案件得出不受理之結果[280]，且其將依 GDPR 作為法律基礎進行裁決[281]。

關於應否受理之問題，德國和英國政府亦提出了問題。首先是德國政府認為 DPC 僅係對 SCCs 的有效性表達疑慮，而非認定其無效，其並無完整的立場[282]，另

[277] *Id.* ¶ 68(9).
[278] *Id.* ¶ 68(10).
[279] *Id.* ¶ 68(11).
[280] *Id.* ¶ 71.
[281] *Id.* ¶¶ 77-79.
[282] *Id.* ¶ 72.

doi:10.6342/NTU202504586

外，高等法院並未確認 Schrems 是否同意此等傳輸，蓋倘若其同意，將使其他問題在本案沒有討論的必要[283]。英國政府則認為，高等法院並未確認系爭傳輸是否是基於 SCCs 傳輸的[284]，蓋高等法院上述提出的問題係使用假設性用語。

但 CJEU 對這些問題的回應則是，其僅在法律問題與主要訴訟之實際事實或目的無關，且問題是假設性的，以及其沒有足夠之事實或法律來給出有效之答覆時，始得拒絕裁決，否則其有責任對法律問題進行裁決[285]，最終 CJEU 認為在此案其有義務做出先行裁決[286]。

第二目 GDPR 適用問題

對於問題 1 的回應，CJEU 認為在資料被傳輸至第三國，且可能被第三國之政府機構以公共安全、國防、以及國家安全目的存取的情況下，並不適用歐洲聯盟條約第 4 條第 2 項以及 GDPR 第 2 條第 1 項、第 2 項之(a)、(b)、(d)款所稱在國家安全領域不適用之結論，蓋此等規範係適用於歐盟國之間，故與本案無關[287]。此外，GDPR 第 45 條第 2 項 a 款亦規定在評估保護水準是否適足時應考量公共安全、國防、國家安全及公共機構存取資料的途徑等等，換言之第三國在上述目的下存取及處理資料應在 GDPR 的規範範圍內，故 GDPR 第 2 條第 1 項和第 2 項應解釋為一國的商業機構將資料傳輸到第三國之商業機構，並且在傳輸時或之後會被第三國

283 *Id.*
284 *Id.*
285 *Id.* ¶ 73.
286 *Id.* ¶¶ 74-76.
287 *Id.* ¶¶ 80-86.

doi:10.6342/NTU202504586

政府機構因公共安全、國防或是國家安全目的存取時，應落入 GDPR 之適用範圍內[288]。

第三目 適足性之判斷依據

關於問題 2、問題 3 與問題 6 中提出，判斷保護是否具備適足性之標準，CJEU 認為 GDPR 第 46 條雖然沒有具體說明適當保障措施、可執行之權利、以及有效的法律救濟的性質，但依據 GDPR 第 44 條之解釋，該條之解釋方式應係確保歐盟人民之資料隱私保護水準不被削弱[289]。故與 Schrems I 案之解釋方式相同，GDPR 第 45 條第 1 項之充分保護之水準應係指有與歐盟內實質相當之保護水準[290]。當第三國未有適足性認定之適當保護措施下，GDPR 的第 107 條以及第 108 條序言指出，依第 46 條第 1 項提供之適當保護措施應彌補第三國資料保護之不足，以確保對資料主體在歐盟法所受到之保護[291]。而所謂實質相當，CJEU 認為應係指歐盟層級之法律，包括 EUCFR 以及相關歐盟法律，但不包括尚未成為歐盟法律體系之 ECHR 以及成員國之國內法[292]。

第四目 資料保護機構暫停或禁止資料傳輸的義務

關於問題 8，CJEU 表示，國家監管機構的責任即是監督對歐盟內關於個人資

288 *Id.* ¶¶ 82-89.
289 *Id.* ¶¶ 91-92.
290 *Id.* ¶ 94.
291 *Id.* ¶ 95.
292 *Id.* ¶¶ 97-100.

doi:10.6342/NTU202504586

料的保護，並且確保其執行，在資料被傳輸至第三國時，此等責任特別重要[293]。雖然監管機構有權力考量哪些行動是適當和必要的，但其仍必須盡其審慎義務，以確保落實 GDPR 的要求[294]。在考量所有情況後，倘若資料保護的要求無法被遵守，除非傳輸或接收之公司自行暫停或終止傳輸，否則監管機構有義務暫停或禁止傳輸[295]。此問題應係源自於 SCCs 修訂前之 Decision 2010/87 之版本中之第 11 條序言，該序言提及監管機構僅在特殊情況中始有暫停或禁止傳輸之權力[296]，但 CJEU 提及嗣後修訂之 Decision 2016/2297 中已將 Decision 2010/87 第四條文字修正為直接規定監管機構暫停或禁止傳輸之權力[297]，故未來應不再限制於特殊情況[298]。

CJEU 隨後指出，歐盟執委會根據 GDPR 第 45 條第 1 項授予之適足性認定對歐盟監管機構具有約束性[299]，但這不妨礙權利主體於其權利受到侵害時提出救濟。受理救濟之機關以及法院亦應進行審查，在遇到適足性認定之有效性存疑時，則應移送至 CJEU 進行先行裁決[300]。

第五目 SCCs 之資料保護水準與有效性

---

293 *Id.* ¶¶ 107-08.
294 *Id.* ¶ 112.
295 *Id.* ¶ 113.
296 本序言中使用「特殊情況（Exceptional Cases）」的字眼。Decision 2010/87, *supra* note 250, recital 11.
297 Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 Amending Decisions 2001/497/EC and 2010/87/EU on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries and to Processors Established in such Countries, Under Directive 95/46/EC of the European Parliament and of the Council, art. 2, 2016 O.J. (L 344) 100.
298 Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd & Maximillian Schrems, ECLI:EU:C:2020:559, ¶¶ 114-15 (July 7, 2020).
299 *Id.* ¶¶ 116-18.
300 *Id.* ¶¶ 119-20.

doi:10.6342/NTU202504586

問題 7 與問題 11 係在討論，SCCs 既然不能拘束第三國的政府機構，是否代表其不能提供足夠之保護，從而無效。CJEU 認為，SCCs 與適足性認定不同，Decision 2010/87 並不涉及第三國的國家機關，無法要求歐盟執委會在作出決定前先行評估第三國的保護水準[301]，而第三國資料保護的不足，應由使用 SCCs 的機構提供額外保障，以保障資料主體之權利[302]，倘若保障不足，監管機構應暫停或禁止傳輸[303]。

Decision 2010/87 以及 Decision 2016/2297 共同構築 SCCs 之決定是否有效？CJEU 分析了 SCCs 中的條款，其認定 SCCs 中有要求傳輸資料之雙方遵守歐盟相關之規則，特別是依 SCCs 第 5 條第 a 款，當第三國的資料接收者無法履行合約義務時，其應儘速通知歐盟內的傳輸者[304]。另外 CJEU 也指出 SCCs 第 4 條(a)款及第 5 條(a)、(b)款要求資料接收者應確認該第三國之資料保護水準，倘若遵守當地法律會使其無法透過 SCCs 保障資料主體之權利，則應依 SCCs 第 4(f)通知資料傳輸者該情況，資料傳輸者則應暫停或終止傳輸[305]，同時也使資料主體得以提起訴訟以獲得救濟[306]。另外 SCCs 第 4 條(g)款也規定資料傳輸者在收到上述通知時也應轉發予監管機構，以使監管機構得以確定是否應暫停或禁止傳輸[307]。

綜合上述，CJEU 認為 SCCs 已提供足夠的保護以及救濟機制，使資料主體得

301 *Id.* ¶¶ 129-30.
302 *Id.* ¶¶ 131-33.
303 *Id.* ¶¶ 134-35.
304 Decision 2010/87, *supra* note 250, Annex, clause 5(a).
305 Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd & Maximillian Schrems, ECLI:EU:C:2020:559, ¶¶ 141-42 (July 7, 2020).
306 *Id.* ¶ 144.
307 *Id.* ¶ 145.

doi:10.6342/NTU202504586

於其權益不受到保障時可暫停或停止資料的傳輸，故其不認為有宣告 Decision 2010/87 批准 SCCs 之決定無效之必要[308]。

第六目 適足性認定之拘束性

關於問題 4、問題 5、問題 9 與問題 10，CJEU 認為此四問題主要係詢問(1)歐盟執委會之適足性認定是否拘束歐盟成員國之主管機關？(2)透過 SCCs 將資料傳輸至美國是否違反 EUCFR 第 7 條、第 8 條以及第 47 條，特別是申訴專員制度是否能滿足 EUCFR 第 47 條之要求[309]？

首先，CJEU 認為適足性認定拘束歐盟成員國之主管機關，惟投訴人提出申訴時，該機關仍應審查該資料傳輸是否符合 GDPR 所定下之要求，如其認為投訴人之主張有理由，則應促使國內法院移送至 CJEU 進行先行裁決[310]。

其次，CJEU 認為 Schrems 係認為美國未能提供適當之保護水準，而此主張本質上是對 Decision 2016/1250 之有效性的挑戰；此外雖然本案係針對 SCCs 提出，但 CJEU 認為隱私盾協議帶來之變化及影響亦不可忽視，尤其是高等法院針對其中之申訴專員制度提出疑問，應一同審查，故 CJEU 認為有必要審查隱私盾協議之有效性[311]。

第七目 隱私盾協議之適足性認定之有效性

[308] *Id.* ¶¶ 148-49.
[309] *Id.* ¶ 150.
[310] *Id.* ¶¶ 155-57.
[311] *Id.* ¶¶ 151, 158-61.

doi:10.6342/NTU202504586

關於隱私盾協議之適足性認定之有效性，首先如同 Schrems I 案中 CJEU 中所提出之觀點，CJEU 認為歐盟執委會應在其決定中認定美國是否能提供與歐盟法相同之保護水準[312]。隱私盾協議附件 II 之段落 1.5 亦指出，在滿足國家安全、公共利益或執法要求所必要之範圍內，歐盟法之要求應退讓[313]，此一特點與安全港協議並無二致[314]。歐盟執委會在考量到相關規範包括 FISA 第 702 條、EO 12333 以及 PPD 28 後，認定美國針對此等國家行為嚴格的限制，係落於實現相關合法目標之必要範圍內，並提供足夠之保障[315]，確保了個人資料得到充分之保障[316]。

CJEU 指出，在歐盟法之解釋下，基本權利並非不可限制，僅係其限制應有明確之規則，並在嚴格且必要之範圍下實施，且必須指明可以對資料進行處理之情況和條件，也就是應符合比例原則之要求[317]。但 FISA 第 702 條以及 EO 12333 中並無法明確的看到比例原則之拘束，故應從實施層面來觀察此等限制是否存在。

FISC 授權如 PRISM 與 UPSTREAM 等監控計劃，但其授權與否之判斷，實質上係基於此等監控計劃是否與獲取外國情報之目標相關，但不涉及外國之個人是否適當地被獲取資料[318]，另外 FISA 第 702 條也未對監視行為之權力施加限制，故這並不符合比例原則之要求[319]。就司法救濟層面而言，PPD 28 以及 EO 12333 之內

312 *Id.* ¶ 162.
313 Decision 2016/1250, *supra* note 223, Annex II, ¶ 1.5.
314 Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd & Maximillian Schrems, ECLI:EU:C:2020:559, ¶¶ 164-65 (July 7, 2020).
315 Decision 2016/1250, *supra* note 223, recital 140.
316 *Id.* recital 136; Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd & Maximillian Schrems, ECLI:EU:C:2020:559, ¶¶ 166-67 (July 7, 2020).
317 Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd & Maximillian Schrems, ECLI:EU:C:2020:559, ¶¶ 174-77 (July 7, 2020).
318 *Id.* ¶ 179.
319 *Id.* ¶ 180.

doi:10.6342/NTU202504586

容均規範監控行為，而未提供可執行之司法權利以及救濟管道[320]，但有效之司法審查之存在係 EUCFR 第 47 條所保障權利之必要組成[321]。

至於新設之申訴專員制度是否可以彌補此一缺失，包括是否滿足 EUCFR 第 47 條之要求？CJEU 表示，申訴專員係由國務卿指派，而其並無任期保障，可能對其獨立性造成影響[322]。另外，雖然 Decision 2016/1250 規定美國情報機構應改正被申訴專員指出之不當行為，但是並未賦予申訴專員針對改正不當行為之拘束力，或是對資料主體之其他保障措施[323]。

第三款 小結

於 Schrems II 案中，CJEU 作出比 Schrems I 案中更細緻的分析[324]。首先是保護標準，其根據 EUCFR 解讀 GDPR 之要求，自行進行了比例原則之審查，並使用了相當嚴格之審查標準[325]。其次，針對 Schrems I 案中對於隱私權的本質以及有效的司法保障，本案有更完整的論述，特別是說明美國的國家安全需求不得完全凌駕於資料隱私保護的原則之上。

再者，於審查其他國家針對 EUCFR 第 52 條第 1 項基本權的限制時，CJEU 建立了更具體的審查標準，包括：(1) 此等限制必須是以法律規定、(2) 授權限制基本權利之法律基礎應清楚界定限制基本權利之範圍、(3) 為滿足比例原則之要求，

320 *Id.* ¶¶ 181-82, 192.
321 *Id.* ¶¶ 186-89.
322 *Id.* ¶ 195.
323 *Id.* ¶ 196.
324 Tzanou, *supra* note 12, at 15.
325 Pedersen, *supra* note 19, at 218.

doi:10.6342/NTU202504586

相關法律應制定「清楚精確的規則以管理適用範圍」，以及「實施最低限度的保障，以使資料主體獲得足夠的保障，以有效的防範其資料受到濫用」以及（4）資料被傳輸至之第三國應提供資料主體有效且可執行的權利。上述四項審查標準提供了一個明確的審查機制，也提升了法律明確性[326]。

綜上所述，隱私盾協議仍然無法解決在 Schrems I 案中美國情報機構監視行為不受拘束之問題，雖然美國政府試圖透過 PPD 28 限制情報機構之監視行為，但依 CJEU 之見解，此等限制並未達到歐盟法所設下之標準。且上述提到之法令當中，經國會通過而具備法律位階之法律僅為 FISA 第 702 條，但其僅為廣泛之授權，故 CJEU 認定其無法有效限制情報機構之行為。

另外對於缺乏有效司法救濟之問題，美國雖然試圖透過申訴專員進行彌補，但申訴專員的權限依舊過小，並非有效之獨立司法救濟手段。事實上，CJEU 相當重視資料主體之權利無法受到保障時，是否有暫停或禁止傳輸的外部機制以控制使用隱私盾協議之公司，由此判決以觀，建立一個符合 CJEU 要求之獨立救濟機構，或許可大幅改善歐美間在資料傳輸議題上的差異。

繼安全港協議後，隱私盾協議再次失敗，對歐美間跨境資料傳輸的實踐造成莫大之影響，短期內連續變動也可能造成法律上高度的不確定性。但 CJEU 也在判決中提到，GDPR 中仍有由第 45 條第 3 項、第 46 條以及第 49 條等建立的合法進行資料傳輸之管道，不至於造成法律真空[327]。另外，CJEU 在本判決中認定 SCCs 之

[326] Tzanou, *supra* note 12, at 16.
[327] Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd & Maximillian Schrems,

doi:10.6342/NTU202504586

使用係合於歐盟法要求，故並未阻斷機構使用 SCCs 辦理資料傳輸，也提供了高度的法律確定性。但在此之外，法院也在對 SCCs 之分析中再次強調完整保護資料主體權利之重要性，要求使用 SCCs 之機構並不能僅因使用 SCCs 即可無限制的自由傳輸資料，而仍需要實施額外的保障，包括加強調查第三國保護水準之義務、未合規時之通知、以及自主暫停或停止傳輸等保障措施，以確保資料主體之權利可以受到保護。也因為 SCCs 不僅限於歐美之間之資料傳輸，故也為其他國家提供了穩定之管道，也成為了從歐盟向外傳輸個人資料之最被廣泛使用的方式[328]，在 2019 年的調查中即指出，有百分之 88 的機構將 SCCs 作為首選的資料傳輸管道[329]，而在 2021 年又提升至百分之 94[330]。

歐盟執委會在 2021 年 6 月 4 日批准新的 SCCs 條款[331]，並要求其作為 2021 年 9 月 27 之後簽訂之資料傳輸相關合約之基礎[332]。此等變更固然為使用機構帶來成本[333]，但其或可維持其在歐盟法下之合法地位，並進一步降低法律之不確定性。

ECLI:EU:C:2020:559, ¶ 202 (July 7, 2020).
328 Gerke & Rezaeikhonakda, *supra* note 221, at 369-70.
329 J. Trevor Hughes & Angela Saverice-Rohan, *IAPP-EY Annual Privacy Governance Report 2019*, EY xix (2019), https://f.hubspotusercontent20.net/hubfs/525875/IAPP_EY_Governance_Report_2019.pdf.
330 Müge Fazlioglu, *IAPP-EY Annual Privacy Governance Report 2021*, EY 4 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4227244.
331 Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance), 2021 O.J. (L 199) 31.
332 *Id.* art. 4.
333 Gerke & Rezaeikhonakda, *supra* note 221, at 371.

doi:10.6342/NTU202504586

第三節 Data Privacy Framework

第一項 EO 14086 之影響

在考量是否給予 DPF 適足性認定之決定草案中，歐盟執委會表示，其認為 EO 14086 的保障和救濟機制是其評估美國整體法律框架之基本要素，是否給予適足性認定取決於 EO 14086 之實施、美國情報機構相應之變革、以及是否將歐盟指定為合格的組織[334]。本文認為，EO 14086 的改革與制度對 DPF 有至關重要的影響，故在說明 DPF 之前，應先行說明 EO 14086 對歐美跨境資料傳輸議題帶來的影響。

EO 14086 對情報活動施加了更多限制，並針對 CJEU 所提出之重大缺陷進行針對性修正，使其相關規範朝歐盟標準更加靠近，但有論者認為其可能仍然無法完全滿足 GDPR 以及 EUCFR 之要求[335]，以下分述之。

首先，EO 14086 列舉了為了國家安全開展情報活動之目標。雖然不論是在針對性蒐集或是大規模蒐集時，均可以由總統以公開或在一定條件下不公開之方式增加國家安全事由，以面對未來可能之新興威脅，但在歐盟之判例法下，國家安全本身即構成得限制人民基本權利之理由，並且無法詳盡定義或列舉，故無需有更詳細之區分以設立法律界限，EO 14086 之規定實際上已經高過歐盟法之標準[336]。惟

---

[334] *Id.* at 385.
[335] *Id.* at 394.
[336] Alex Joel, *Necessity, Proportionality, and Executive Order 14086*, AM. U. WASH. COLL. L. 1, 8-12 (May 2023), https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1101&&context=research&&sei-redir=1&referer=https%253A%252F%252Fscholar.google.com%252Fscholar%253Fhl%253Dzh-TW%2526as_sdt%253D0%25252C5%2526q%253Deo%252B14086%2526btnG%253D#search=%22eo%2014086%22.

doi:10.6342/NTU202504586

亦有觀點認為美國在侵害資料主體權利更嚴重的大規模蒐集的情況下，賦予總統得更新並且得以不公開之權力，並不符合歐盟之要求[337]。

CJEU 在判斷資料主體是否受到充分保護時，除了考量相關法規規範外，也認為應考量實施之情況，而 EO 14086 雖然使用了與歐盟相近之必要性以及比例原則等字眼，但美國國內之解釋與歐盟的解釋方式仍有出入，而傳統上美國會給出更寬泛的解釋[338]，可能會導致難以符合歐盟標準之要求。在分析 EO 14086 中之必要性以及比例原則條款之要求上，必要性被定義為無可行之其他手段，而比例原則則是要求應考量經驗證之優先情報與對隱私和公民自由之影響之間取得平衡，再加之美國法實務上之解釋，與歐盟法實際上相當接近[339]，故仍有待觀察其實施情況，歐盟個人資料保護委員會（European Data Protection Board，下稱「EDPB」）亦同意此等觀點[340]。但亦有觀點分析，必要性與比例原則實際上是模糊之用語，另外 EO 14086 中規定訊號情報不必是推進經驗證之優先情報事項方面的唯一可用或使用手段，此等解釋與 CJEU 之比例原則適用方式不相容。此外，美國總統意圖使比例原則之解釋貼合 CJEU 之解釋的可能性不大，美國司法部（United States Department of Justice）曾表示會使用美國法來進行解釋，而大規模蒐集的掃蕩式之蒐集方法更會侵害到 EUCFR 中之其他基本權利，美國至少應考慮在 NSA 獲得資訊前先移除相關之敏感資訊[341]。

337 Gerke & Rezaeikhonakda, *supra* note 221, at 385.
338 *Id* at 394-95.
339 Joel, *supra* note 336, at 12-18.
340 EDPB Opinion, *supra* note 11, at 31.
341 Pedersen, *supra* note 19, at 227-29.

doi:10.6342/NTU202504586

如前所述，有意見認為實際上歐盟在國家安全例外之原則上並無列出具體目標之要求，但亦有認為外國之資料主體會因此無法確定自己何時、是否正在受到監控，其不確定性以及缺乏透明性無法符合歐洲人權法院（European Court of Human Rights）所要求的「法律應足夠清晰，以便公民充分理解公共機構有權採取任何監控措施的情況和條件」，以及「法律必須以足夠清晰的方式指名授予主管機構的任何裁量權的範圍及其行使方式」的要求，另外，其合法目標之用語較為廣泛，故應額外判斷是否與國家安全利益相關，而缺乏事前司法審查亦可能導致其監控行為不限於 CJEU 所認定之國家安全目的[342]。

再者是 DPRC 與 CLPO 相同，只會回覆投訴人「審查沒有發現任何涵蓋的違規行為」或是「DPRC 發布了要求採取適當補救措施」的決定[343]，也就是指投訴人無法獲知 DPRC 的判斷基礎，從而難以進行其他救濟。同時針對 DPRC 之決定也無法再向聯邦法院進行上訴[344]，CJEU 已經在 Schrems I 案中表示這是不能滿足 EUCFR 第 47 條的要求的[345]。

除了歐盟內部在給予適足性認定前程序之意見之外，另有觀點對新的獨立申訴與救濟機制是持較樂觀的態度的，認為其相較於先前隱私盾協議時期的申訴專員制度有相當大的改進[346]。EO 14086 中規定 DPRC 之法官不得同時兼任美國政府

342 *Id.* at 225-27.
343 EO 14086, *supra* note 93, sec. 3, § (d)(i)(H).
344 Gerke & Rezaeikhonakda, *supra* note 221, at 399.
345 *Id.*
346 *Id.* at 397.

doi:10.6342/NTU202504586

內的任何其他職務[347]，並且在獨立性小節中規定司法部長不得干預決定，亦不得罷免法官，除非存在不當行為以及身體健康問題[348]，帶來了足夠之獨立性需求，但其任命後四年得連任之特性亦可能會帶來對其獨立性之影響，EO 14086 亦未約束美國總統將之解職之權力，加之 DPRC 之授權基礎來自 EO 14086，可能被總統隨時修改，故實際上美國總統對其獨立性之影響不可忽視[349]。

有論者也提出 EO 14086 之設計可能無法滿足 EUCFR 第 47 條要求之問題點。首先，DPRC 雖名為法院但實質上是行政部門，雖然 EO 14086 引入了獨立性保障措施，但對 CJEU 而言可能並不夠彌補其本身是行政部門之問題，Schrems 也表示此等法院並非法院[350]。其次是特別辯護者沒有足夠之獨立性要求，僅是在其被任命之前之兩年內不得是行政部門的僱員，此等獨立性保障較低，可能無法足以真正獨立的代表投訴人利益[351]，而其是在救濟程序中投訴人唯一可以倚仗之對象。另外，特別辯護者並不參與 CLPO 之程序，係在 DPRC 階段開始參與，而事實認定係在 CLPO 程序時進行，在此方面應有改進之空間，使其能夠有更全面的監督功能[352]。

本文認為，EO 14086 首次對美國的情報行動進行了大幅度的改革，展現了持續與歐盟合作之決心。在多數議題上，其改革幅度均受到了部分質疑，但亦有部分改革得到了認可，例如必要性與比例原則之加入，以及部分意見認為列舉國家安全

347 EO 14086, *supra* note 93, sec. 2, § (d)(i)(A).
348 *Id.* sec. 2, § (d)(iv).
349 Pedersen, *supra* note 19, at 229-30.
350 Gerke & Rezaeikhonakda, *supra* note 221, at 398.
351 *Id.*; Connolly, *supra* note 61, at 112-13.
352 Pedersen, *supra* note 19, at 236.

doi:10.6342/NTU202504586

目標本質上已高過歐盟法的標準。

在 EO 14086 的改革仍不被完全認可之情況下，歐盟執委會與美國仍持續合作，並協議出 DPF 的草案，開啟了是否授予 DPF 適足性認定的程序，以下將詳細說明 EDPB 以及歐洲議會對其之意見。

第二項 決議程序與意見

第一款 協議背景

2023 年 5 月 12 日，Meta Ireland 因為未提供適當保護措施而違反 GDPR 第 46 條第 1 項，被 DPC 處以十二億歐元罰鍰[353]，並被要求在六個月內暫停傳輸與處理歐盟人民之資料，以及改善其資料處理以符合 GDPR 之規定[354]。此一事件顯示失去隱私盾協議對從事跨大西洋資料傳輸所帶來之法律不確定性[355]。普遍而言，隱私盾協議之適足性認定被宣告無效後，美國公司倘若欲將歐盟資料傳輸至美國，需要基於 GDPR 內之其它規範進行，進而造成了較高的成本以及法律上之不確定性[356]，此等缺點驅使美國再次與歐盟協調出新的協議，並改善先前安全港協議與隱私盾協議之不足。

歐盟與美國在 2022 年 3 月 25 日宣布其談判之結果——一個新的跨大西洋資料隱私架構。針對 CJEU 在 Schrems II 案中提出的問題提出解決方式，包括建立一

353 Meta Ireland 的前身為前述之 Facebook Ireland。Gerke & Rezaeikhonakda, *supra* note 221, at 372.
354 *Id.*
355 *Id* at 373.
356 *Id.*

doi:10.6342/NTU202504586

套新的規則與有約束力的保障措施以限制美國情報機構之行為、一個新的二級救濟系統，包括一個資料隱私審查法院——DPRC，以及加強自我認證機制管理以及整體的監控和審查機制等[357]。

DPF 之通過程序包括送至 EDPB 並參考其意見、送至第 93 條委員會[358]並得到其同意投票，此外歐洲議會得以隨時行使對適足性之審查權，最後歐盟執委會始得給予適足性認定[359]。目前 DPF 之適足性認定尚未被宣布無效，但其正面臨合法性之挑戰，其未來尚存在法律上之不確定性，故在程序中各部門之意見對於分析其前景應有重要之參考價值，以下將說明並分析之。

第二款 EDPB 之意見

EDPB 依據 GDPR 第 70 條第 1 項(s)款，有權在歐盟執委會給予適足性認定前分析該國之保護水準，並給予歐盟執委會是否授予適足性認定之意見[360]。EDPB 給予了相當多具體且細節之意見[361]。

整體而言，EDPB 認為 DPF 的原則與隱私盾協議基本上相同[362]，惟在過去 CJEU 所重視之情報機構監控行為授權過廣以及缺乏有效救濟機制的問題下，DPF 時期

---

357 *Id.* at 374-75; *Trans-Atlantic Data Privacy Framework*, EUR. COMM'N (2022), https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/Trans-Atlantic%20Data%20Privacy%20Framework.pdf.

358 透過 GDPR 第 93 條建立的負責控制歐盟執委會之委員會。GDPR, *supra* note 8, art. 93.1; *see generally* Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, 2011 O.J. (L 55) 13.

359 Gerke & Rezaeikhonakda, *supra* note 221, at 386.

360 GDPR, *supra* note 8, art. 70(1)(s).

361 *See generally* EDPB Opinion, *supra* note 11.

362 *Id.* at 11.

doi:10.6342/NTU202504586

有 EO 14086 帶來之改革，故可能帶來不同之結果。

第一目 DPF 之優點

首先是限縮情報行動授權範圍。EDPB 認為出於執法目的以獲取資料通常可被視為係正當目的，惟在歐盟法下仍需受到必要性與比例原則之約束[363]，至於美國法下，EO14086 某程度也已將此明文化。EDPB 並認為在美國法下，搜索令、傳票等強制獲取資訊之措施的獲取及使用受到高度且全面之規範，故其認為美國之執法調查系統在此方面足以有效保護資料主體之權利，並符合相關之必要性及比例原則要求。在非刑事執法之過程中，例如發出民事傳票等情況就沒有事前司法審查之要求，惟此等行為在後續訴訟也可能受到挑戰並受到法院審查，加上 PCLO、監察長等之外部控制，故整體而言，EDPB 認為美國執法機構獲取美國公司持有資料所受到之監督相當健全且獨立[364]。

其次是建立救濟機制。EDPB 表示，當資料主體認為權利被侵害時，依據 Schrems I 案之解釋以及 EUCFR 第 47 條，應有有效之救濟手段，以保護其權利。美國法下對於此等救濟機制已以數部法律中之相關規範保護之。故 EDPB 僅表示歐盟執委會應澄清此等救濟途徑為何，並且應進一步闡明這些救濟是否提供 CJEU 所要求之更正與刪除資料之相關權利[365]。

在評估資料保護規範是否能有效保護資料主體權利時，有效執行的申訴以及

[363] *Id.* at 23.
[364] *Id.* at 23-25.
[365] *Id.*

doi:10.6342/NTU202504586

救濟機制是最重要的因素[366]。首先，資料主體必須在合格國家之監管機構進行投訴，而適足性認定草案之生效條件係將歐盟指定為合格實體。至於所謂合格投訴，應基於涵蓋之違法行為，即對於隱私和公民自由利益受到不利影響[367]。而歐盟執委會表示所謂不利影響之定義並非是要限縮可投訴之範圍，應包含所有違反 EO 14086 第 4(d)(iii)節[368]中提到之規定，故只要有所違反即應能獲得救濟，而非額外要求有一定程度之損失[369]。

在美國法院獲得救濟，通常需要原告提出主張表明其(1)已遭受實質上的損害、(2)損害可以合理地追溯到被告的受質疑的行為、以及(3)該損害很可能（Likely）存在，而不僅僅是推測性的，並可通過有利決定得到救濟[370]。美國國內實務針對具備一定程度保密性之國家監控行為之爭議，例如源自 FISA 第 702 條之爭議，通常認為其主張難以建立，以及基於國家機密原則，導致民事案件難以進入實質審理而被駁回[371]。而 DPRC 救濟系統之信念測試並不要求投訴人證明資料已經被情報機構存取，此舉降低了提起救濟之門檻[372]。DPRC 的空泛回應則係為保護敏感資訊不被隨意外流，故有其正當基礎，但仍應能有衡平措施，例如賦予投訴人陳述意見權或是揭露判決摘要。儘管如此，EDPB 仍對於 DPRC 之空泛回應以及其不允許投訴

366 *Id.* at 11.
367 *Id.* at 50-51.
368 其中提到美國憲法、FISA 或 FISC 批准之程序、EO 12333 以及其相關程序、EO 14086 本身及相關程序、以及各種相關法規、命令、政策或程序等等。EO 14086, *supra* note 93, sec. 4, § (d)(iii).
369 EDPB Opinion, *supra* note 11, at 50-51.
370 Connolly, *supra* note 61, at 113-14.
371 Chauvin, *supra* note 33, manuscript at 12-19.
372 EDPB Opinion, *supra* note 11, at 51.

doi:10.6342/NTU202504586

人再行上訴之設計表達擔憂[373]。

第二目 DPF 遺留之問題

DPF 延續了很多隱私盾協議的實質內容，問題也仍然存在[374]。首先是一如既往之自我認證機制。EDPB 對於 DPF 繼續使用之自我認證系統表達疑慮，並且指出過去隱私盾協議內之監督及審查機制流於形式，並無法發揮實質功能。就此美國商務部以及美國交通部承諾會採取實質之執法行動，並與歐盟之資料保護機構合作，EDPB 也將會密切關注[375]。

其次是可以不遵守 DPF 原則的例外規定。在 DPF 中，經 DPF 認證的組織在三種情況下可以不遵守 DPF 原則之要求，包括(a)遵守法院命令、促進公共利益、法律執行或國家安全需求與遵守 DPF 之義務所衝突者、(b)為執行法律、法院命令或政府處分，而有必要違反 DPF 之原則者、(c)GDPR 所允許之例外情況，且其違反情況有可類比之情況者[376]。EDPB 表示依此文義恐難以判斷例外情況之具體範圍，故建議歐盟執委會可以進行釐清[377]。

再者是情報行動的事前授權。由於 FISC 之任務僅係授權監控計劃而非個別監控行動，故 EDPB 認為其未能提供外國人有效之保障，且 EO 14086 無法解決此一

---

373 *Id.* at 51-53.
374 *Id.* at 3.
375 *Id.* at 20-21.
376 *Commission Implementing Decision of XXX Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data Under the EU-US Data Privacy Framework*, EUR. COMM'N (Dec. 13, 2022), https://commission.europa.eu/document/download/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en?filename=Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf
377 EDPB Opinion, *supra* note 11, at 15.

doi:10.6342/NTU202504586

問題，也無法對其產生約束力[378]。至於大規模蒐集，EDPB 表示大規模蒐集對於基本權利之侵害較為嚴重，並指出歐洲人權法院認為大規模蒐集之事前獨立審查以及事後監督與審查同等重要，並且所謂的獨立，係指由獨立於行政部門之外之機構進行，惟此等設計不管在 FISA、EO 12333 及 EO 14086 中均不存在[379]。此外，EO 14086 仍然允許暫時性大規模蒐集，雖然其縮小了適用範圍，並提供額外保障措施，但所謂「暫時」是否表示目標尚未明確即可持續進行大規模蒐集和傳播？此外蒐集後之資料存取以及是否有更加嚴格之保障措施，仍不夠明確，故 EDPB 再次強調應有獨立之監管機構進行全面監督[380]。

再者是訊號情報（Signals Intelligence）之定義，EO 14086 並沒有相關定義，但參考 EO 12333 之定義則會過於廣泛。而 EO 14086 具體列出了進行訊號情報蒐集時被允許之 12 個目標、5 個禁止之目標、以及 6 個大規模蒐集之合法目標，惟有些目標相當籠統，且美國總統有權增加目標項目[381]，故 EDPB 認為情報機構不能僅因符合上述目標即被認為係合理蒐集情報，而應有更具體之規則[382]。

另外在情報活動範圍最小化之議題上，EO 14086 要求情報蒐集活動應盡可能具針對性，並要求其應使用侵入性較低的之方式，並符合必要性及比例原則之要求[383]。在實施層面，EO 14086 給予美國情報機構自發佈起最多一年的時間更新其政

[378] *Id.*
[379] *Id.* at 33-34.
[380] *Id.* at 36-37.
[381] *Id.* at 29-30.
[382] *Id.* at 30.
[383] *Id.*

doi:10.6342/NTU202504586

策與程序更新[384]，但 EDPB 建議歐盟執委會基於更新後的程序作為是否給予適足性認定之判斷基礎[385]。

關於事後救濟機制，EDPB 認為 CLPO 不能符合 EUCFR 第 47 條之要求，並已被歐盟執委會多次確認[386]。而 DPRC 是否能夠符合該要求，EDPB 認為依據歐盟判例法，EUCFR 第 47 條之要求並不以真正之法院為必要，但必須能夠提供獨立且公正之救濟管道，而 DPRC 之起訴門檻較美國法院低，使資料主體可以更容易的使用救濟管道，故 EDPB 認為就制度設計而言 DPRC 能提供充足的保護，只是實踐上 DPRC 是否能夠維持其獨立性，有待觀察及分析[387]。

依照 EDPB 之理解，雖然 DPRC 係屬於美國司法部之行政機關，但其任命程序以及獨立性保障是參考聯邦法官[388]，故應能符合 EUCFR 第 47 條之要求，但其與聯邦法官仍有以下差異。首先，決議草案並未定明總統是否有權解職或罷免 DPRC 之法官；其次，其與聯邦法官不同，DPRC 法官得參與司法外活動，只要該活動不干擾他們公正、有效以及獨立的履行其職責，並且也受到 PCLOB 和監察長之審查及監督，應不會影響其職責之運行[389]，只是此方面仍待實務觀察[390]。

EDPB 另外指出，DPRC 法官對機密資訊存取需要特別之安全許可，並且需要透過 CLPO 取得，但是 CLPO 並不具備獨立性，這與歐盟法官以及美國聯邦法官

384 EO 14086, *supra* note 93, sec. 2, §§ (c)(iv)(B)-(C).
385 EDPB Opinion, *supra* note 11, at 31.
386 *Id.* at 45.
387 *Id.* at 46-47.
388 *Id.* at 47.
389 28 C.F.R. § 201.7(c) (2022).
390 EDPB Opinion, *supra* note 11, at 48.

doi:10.6342/NTU202504586

之權限不相同，此差異可能會影響 DPRC 的獨立性，應在日後之聯合審查中評估其在實務上之影響[391]。

第三目 EDPB 之其它建議

EDPB 亦提出了能有所改進之議題。在外部監督上，EDPB 認為 PCLOB 可以對 EO 14086 之規範發揮全面監督的作用，雖然 PCLOB 之建議不具形式上之拘束力，但情報機構負責人有義務仔細考慮並解決其提出之問題，只是其實施情況仍有待觀察[392]。另外，過去在 PPD 28 以及 FISA 第 702 條之審查上，PCLOB 對隱私盾協議之聯合審查中所給予 EDPB 之資訊與其公開予公眾者一致，並承諾在審查 EO 14086 之報告後會將其報告內容公開，但實際上 PCLOB 公開非機密報告必須與情報機構協調，不能自主決定。故 EDPB 希望未來 PCLOB 可以有更高之獨立性，發揮對情報機構之監督，並對其有拘束力[393]，考量到歐洲人權法院對公眾監督之要求標準，EDPB 認為 PCLOB 每半年向總統及國會提交之報告已經足夠[394]。

關於救濟機制，EDPB 注意到 DPF 中之七種救濟機制與隱私盾協議大致相同[395]，EDPB 認為救濟機制應重質不重量，而隱私盾協議之救濟機制均以在美國進行救濟為主，這會削弱歐盟內資料保護機構之監控權力，並且複雜化救濟機制[396]，應

391 *Id* at 48-49.
392 *Id.* at 42-43.
393 *Id.*
394 *Id.* at 44.
395 *Id.* at 21.
396 *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, EUR. COMM'N 1, 26 (Nov. 23, 2016), https://ec.europa.eu/newsroom/article29/items/640157.

doi:10.6342/NTU202504586

由一個獨立的爭議解決機構來調查與解決個人投訴[397]。另外，在美國機構並未在歐盟法下運做而僅適用 DPF 之情況下，如果歐盟資料主管機關在此情況下可以在程序上提供協助，將對爭議解決機制之有效性帶來正面影響，例如作為資料主體之代表或中介機構，或是授權資料主體得直接在歐盟行使其權利[398]。

第四目 小結

EDPB 之意見整體著重於分析 EO 14086 帶來之改革。綜合而言，EDPB 對 EO 14086 之改進保持正面態度，但也同時認為還存有需要修正之問題，歐盟執委會也需要更明確的指引以及有效的監督[399]。

EDPB 表示是否給予 DPF 適足性認定應基於 EO 14086 之相關政策以及實施情況，並認為 EO 14086 針對美國情報機構之行動提出相當程度的改善，特別是引入了必要性以及比例原則之概念，並且在歐盟可被認定是合格組織之前提下設計一個全新，且相較於過去監察專員制度大幅度進步的救濟途徑[400]。

EDPB 雖然整體而言採取正面態度，但其也指出了 EO 14086 中的問題。EO 14086 關於大規模蒐集的規範仍存有疑慮，特別是對於資料的保存以及傳播[401]，此外在其他的議題上，EDPB 雖然對其制度設計大體表示滿意，但也對未來實際施行情況持保留態度，亦即其認為 DPF 之成功與否與受美國日後之實務執行左右，但

397 *Id.*
398 EDPB Opinion, *supra* note 11, at 48.
399 *Id.* at 6.
400 *Id.* at 4-5.
401 *Id.* at 5.

doi:10.6342/NTU202504586

與過去相比已有長足之進步。

總體而言，EDPB 認為未來美國商務部、其他美國機構、歐盟執委會以及相關歐盟監管機構進行審查時，應特別注意相關州法律、暫時性大規模蒐集之例外情況、必要性和比例原則之實踐以及相關之政策和程序，以及相關保障措施以及補償措施在 FISC 領導之監管背景下如何運作[402]。至於 EO 14086 對 FISA 第 702 條以及 EO 12333 之監控權力之實際限縮之效果，仍有待觀察及分析，在相關資訊無法被公布之情況下，PCLOB 之評估報告或許可以做為參考[403]。

第三款 歐洲議會之意見

在送予 EDPB 並得到意見後，適足性認定草案被送至歐洲議會並聽取意見。歐洲議會整體反對就當前之適足性認定草案以及美國之整體法制給予 DPF 適足性認定，但也給出了應調整之方向。

第一目 授權監控問題

歐洲議會認為大規模監控係對個人隱私的侵擾且不加區分地蒐集資料，有損歐洲公民和企業對數位服務之信任，對數位經濟產生不良影響。且美國國內亦禁止大規模蒐集，但卻並未禁止對歐盟人民為相同之行為[404]。

---

402 *Id.* at 53-54.
403 *Id.* at 37-40.
404 *Adequacy of the protection afforded by the EU-U.S. Data Privacy: Framework European Parliament Resolution of 11 May 2023 on the Adequacy of the Protection Afforded by the EU-US Data Privacy Framework (2023/2501(RSP))*, EUR. PARLIAMENT, ¶ H (May 11, 2023), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.pdf [hereinafter EP Opinion].

doi:10.6342/NTU202504586

歐洲議會認為美國沒有聯邦級的隱私和資料保護法規，但認同 EO 14086 引入之保護措施，例如必要性及比例原則之要求，只是需要密切監控並評估其運作。惟 DPRC 之程序缺乏透明度，可能會難以評估[405]。歐洲議會亦注意到 EO 14086 中之資料保護原則有長足進步，但其實質解釋上可能與歐盟法以及 CJEU 不一致，而係以美國法之解釋方式來詮釋，例如經驗證之優先情報以及授予美國總統增加合法目的權限之規定[406]。

針對大規模蒐集，雖然 EO 14086 認為原則應優先採取針對性蒐集，並且有多項保障措施，但缺乏獨立之事前授權，包括 EO 12333 也沒有如此規定。同時美國缺乏嚴格之資料保存與傳播規則，以及暫時性大規模蒐集等問題。故在資料傳播之議題上，歐洲議會參考 EDPB 之建議，認為資料傳播會帶來額外風險，應分析與確定第三國是否提供足夠之保障水準[407]。

此外 FISA 授權之訊號情報範圍過於廣泛，故歐洲議會呼籲歐盟執委會在未來之談判中澄清 EO 14086 中之訊號情報之定義和範圍[408]。另外歐洲議會亦認為 EO 14086 之涵蓋範圍不夠廣泛，例如不適用於透過愛國者法案以及雲法案（CLOUD Act）等其他方式取得之資料[409]。

最後，美國缺乏聯邦層級之隱私保護法律，最重要用以規範情報機構監控行為之 EO 14086 僅係行政命令，可以不經過國會即由總統隨意修改，對歐盟來說難以

405 *Id.* ¶ J.
406 *Id.* ¶ 2.
407 *Id.* ¶¶ 3-4.
408 *Id.* ¶ 7.
409 *Id.* ¶ 5.

doi:10.6342/NTU202504586

預見未來之發展，故除了定期審查外，亦應加入落日條款，以規範並應對美國未來之行為[410]。

第二目 救濟機制問題

歐洲議會認為根本問題是歐洲資料主體在受到美國人監控時尋求司法救濟能力之不足，故其要求歐盟人民應能享有與美國人民相同之權利[411]。DPRC 之空泛回應、無法向聯邦法院上訴、沒有損害賠償之規定等問題，都應該要由歐盟執委會與美國談判以改善[412]。

針對 DPRC 法官獨立性之問題，歐洲議會表示其雖然有一定之獨立性保障，但美國總統可以推翻 DPRC 之決定或是罷免法官，甚至可以秘密進行，將使 DPRC 法官之獨立性得不到保障[413]。另外代表投訴人利益之特別辯護者亦欠缺足夠之獨立性要求[414]，此等設計無法滿足 EUCFR 第 47 條之要求[415]。

另外歐洲議會提出，雖然美國在政府存取資料之議題上做出諸多限制，但在商業組織的相關問題上卻沒有作出改變，仍然只能依靠爭端解決機制或是商業組織的隱私計劃，故歐洲議會呼籲歐盟執委會密切分析這些機制的有效性[416]。

綜上，歐洲議會與 EDPB 皆認為應有更具體之規則將相關規範明確化，並且

410 *Id.* ¶ 12.
411 *Id.* ¶ 6.
412 *Id.* ¶ 8.
413 *Id.* ¶ 9.
414 獨立辯護者限於初次任命前兩年未曾擔任行政部門僱員者。28 C.F.R. § 201.4 (2022).
415 EP Opinion, *supra* note 404, ¶ 9.
416 *Id.* ¶ 10.

doi:10.6342/NTU202504586

持續關注並審查具體之實施狀況[417]。歐洲議會強調 GDPR 下的之適足性認定是法律問題而非政治問題，且政治及商業利益也無法與隱私權利平衡[418]。基此，歐洲議會作出決議，認為 DPF 框架以及美國之具體法規措施，並無法有效保護歐盟人民之權利並符合歐盟法之規範，故歐盟應更進一步評估美國具體之實施情況。在歐盟並未被指定為合格實體之情況下，歐盟並無法有效的評估救濟機制之運作情況，故歐盟應持續與美國談判，並不要授予適足性認定[419]。

第三目 小結

歐洲議會提出不要授予適足性認定之結論，而其事實認定與 EDPB 之意見書並無太大之出入，惟其針對欠缺明確性之部分，例如實施情況、DPRC 獨立性問題等，相對均採取較負面之看法，認為倘若無法確認符合歐盟標準即不應給予適足性認定，此與 EDPB 較傾向先微調後追蹤之看法有所不同。歐洲議會另外提醒，不斷授予被 CJEU 宣告無效之適足性認定之資料傳輸協議，會對歐洲企業帶來沈重的合規成本，其擔心 DPF 會再次步入後塵[420]。

第二項 現行架構——Data Privacy Framework

歐盟執委會在 2023 年 7 月 10 日通過了授予 DPF 適足性認定之決定[421]（下稱「DPF 決定」），賦予歐美間新的資料傳輸框架 DPF 適足性認定，使自我認證符合

417 *Id.* ¶¶ 13-14.
418 *Id.* ¶ 1.
419 *Id.* ¶¶ 15-20.
420 *Id.* ¶ 11.
421 *See generally* Decision 2023/1795, *supra* note 10.

doi:10.6342/NTU202504586

其原則之機構可以直接進行跨大西洋的資料傳輸而不需額外的保障措施[422]，補足了隱私盾協議適足性認定被宣告無效後之空缺。在通知歐盟成員國適足性認定之授予後，歐盟執委會將與相關機構與美國再次評估其適足性[423]，其後至少每四年重新評估[424]。

DPF 決定係由數個部分組成，包括最前面之背景介紹，介紹了有關跨大西洋資料傳輸相關之情報機構行動限制、流程與監督、相關的美國國內法與爭端解決機制、為 DPF 特別設計之爭端解決機制等，其本文則是說明美國法律以及 DPF 框架結合能提供歐盟資料主體與歐盟實質相當之保護水準。隨後之附件係來自美國各部門之信件，闡釋其各自之職權以及積極配合執法之意願[425]。

第一款 DPF 架構

DPF 亦採用向美國商務部自我認證之方式，惟美國商務部僅進行管理，對於違反 DPF 原則之執法則是由 FTC 以及美國交通部負責[426]，且因 DPF 認證之組織並不直接適用歐盟法而僅受美國法約束[427]，故應適用聯邦交易委員會法[428] (Federal Trade Commission Act)、美國運輸部不正當商業行為之規範[429]等相關禁止不正當商業行為之相關規範來執法[430]。

---

422 Gerke & Rezaeikhonakda, *supra* note 221, at 355.
423 Decision 2023/1795, *supra* note 10, art. 3(4).
424 GDPR, *supra* note 8, art. 45(3).
425 *See* Decision 2023/1795, *supra* note 10.
426 Gerke & Rezaeikhonakda, *supra* note 221, at 392.
427 EDPB Opinion, *supra* note 11, at 11.
428 Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (1914).
429 49 U.S.C. § 41712 (1978).
430 *Id.*

doi:10.6342/NTU202504586

美國商務部建立並公開所有加入 DPF 架構之名單，並會在每年重新認證後更新之[431]。認證後 DPF 之原則即會立即開始適用，即使在日後退出 DPF，其在加入 DPF 期間透過 DPF 傳輸之資料亦應持續受到 DPF 原則之保護[432]。

DPF 機構應提供後續程序以驗證其對 DPF 原則之實踐，可透過自我評估或外部審查，至少每年一次。為使獨立爭端解決機制之調查順利，DPF 機構亦應留存其對隱私保護之實踐紀錄，並提供予獨立爭端解決機構以利調查[433]。

第一目 監督機制

經 DPF 認證之機構應公開宣佈遵守 DPF 原則並公開其隱私政策並全面實施之，並同時向美國商務部提交相關訊，包括機構名稱、處理個人資料之目的、涵蓋之個人資料、驗證之方法、相關獨立救濟機制、以及對之有管轄權之執法機構[434]。DPF 機構應每年重新認證，並由美國商務部驗證之，並公開其認證之機構名單以及執法機構管轄之名單，在該機構無法遵守 DPF 原則時，該機構及美國商務部亦應刪除任何明示或暗示其仍為 DPF 認證機構之聲明[435]。美國商務部會主動或根據投訴調查虛假的聲明，並採取相關法律行動[436]。

如果有證據顯示 DPF 機構不遵守 DPF 下之承諾，美國商務部將要求其提交詳細之問卷，仍不能滿足要求時，該機構即會被轉介至 FTC 或美國交通部以進行執

---

431 Decision 2023/1795, *supra* note 10, annex I, art. III(6)(d).
432 *Id.* annex I, art. III(6)(f).
433 *Id.* annex I, arts. III(7)(a)-(e).
434 *Id.* recital 48.
435 *Id.* recitals 49-52.
436 *Id.* recitals 56-57.

doi:10.6342/NTU202504586

法行動，持續不遵守之機構會自 DPF 名單移除並被要求返還或刪除根據 DPF 獲取之個人資料。另外自願退出或未能重新認證之機構，亦須返還資料或是在確保資料受到保護之情況下保留資料[437]。

為確保充分之資料保護水準，美國應設立一個獨立之監督機構以監督和執行資料保護規則，由 FTC 以及美國交通部進行調查和執法。其職責係調查機構遵守 DPF 原則之情況以及調查虛假聲明，透過臨時或永久禁令、民事懲罰等措施索求補償並進行懲罰以進行補救，並建立 DPF 案件中受到 FTC 命令約束之機構列表[438]。航空公司則由美國交通部進行專屬管轄，優先以和解之方式解決，若無法達成則會依行政法官之管道進行管理及爭端解決[439]。

第二目 DPF 機構之義務

一旦機構自願認證為 DPF 組織，即會立即產生對於 DPF 原則遵守之義務，並且具有強制性和可執行性，應採取適當之技術和組織措施以確保合規，並留存紀錄以利後續爭端解決[440]。

DPF 機構有詳盡之告知義務，應告知個人其參與 DPF 之情況、蒐集之個人資料類型以及目的、其在美國並遵守 DPF 原則之實體之資訊、投訴途徑，包括獨立爭端解決機構、可能向其揭露資料之第三方以及揭露目的、資料主體存取個人資料

437 *Id.* recitals 54-55.
438 *Id.* recitals 61-63.
439 *Id.* recital 64.
440 *Id.* recitals 44-46.

doi:10.6342/NTU202504586

之權利以及限制使用和揭露其個人資料之選擇權等資訊[441]。

DPF 規定資料僅應為特定之目的而蒐集並在與目的相容之範圍內使用，並以合法且公平之方式處理[442]。當其基於不相同但仍相容之目的處理資料或是向第三方揭露之前，必須透過清晰、明顯且容易獲得之機制給予資料主體退出之機會[443]。

DPF 機構在向第三方傳輸個人資料時，應遵守通知義務以及給予資料主體選擇權，並與第三方簽訂契約，確保第三方維持相同之資料保護水準，並僅能於有限和特地之目的內使用資料。此外在確定無法滿足契約義務時通知 DPF 機構、停止處理、以及採取適當之補救措施[444]。

DPF 要求機構確保資料之準確性、最小化和安全性，應確保資料保持更新及正確、僅在目的範圍內存取、以及確保其安全[445]，並告知資料主體該機構參與 DPF 之情況、蒐集之資料類型、處理目的、可能得到資料之第三方之類型、身分及目的、個人權利、如何聯繫該機構、以及可用之救濟途徑等等資訊[446]。

第三目 資料主體在 DPF 下之權利

資料主體之權利包括選擇權、資料存取權、反對處理權以及糾正與刪除權。選擇權係指資料主體得選擇是否將其資料揭露予第三方，或是是否用於與蒐集時不

441 *Id.* annex I, art. II.
442 *Id.* recitals 13-14.
443 *Id.* recital 15.
444 *Id.* annex I, art. II(3).
445 *Id.* recitals 20-24, annex I, art. II(4).
446 *Id.* recitals 25-26.

doi:10.6342/NTU202504586

同之目的，而在不同意時得選擇退出[447]；此外敏感資料則應獲得事前之同意權[448]。

資料存取權之部分，資料主體有權在不需任何理由之情況下向機構請求確認其是否正在處理其個人資料以及其處理目的、機構揭露資料對象等資訊，並僅能受到與歐盟法類似之合理限制，例如可能侵害他人權利、成本與消除之隱私風險不成比例、干擾公共利益等情況，或是重複或無理之請求、詐欺性之請求等[449]。此等得拒絕提供之情況應由機構負責證明[450]。

糾正與刪除權係指資料主體得對不準確之資料進行糾正或修改，以及對違反 DPF 原則處理之資料請求刪除；例外情況為，DPF 機構提供存取資料之成本與個人隱私面臨之風險不成比例，或者會侵害第三人之權利[451]。在自動化決策之問題上，鑑於自動化處理通常在歐盟境內進行，將直接適用 GDPR 之規定，即使需要在美國進行自動化決策，美國法律亦對不利決定提供了特定之保護機制，故無需進行額外規定[452]。

第四目 救濟機制

DPF 要求機構透過有效且容易獲得之獨立救濟管道為受違規影響之個人提供救濟。機構可選擇透過歐盟或美國之獨立救濟機制來達成此一要求，包括與歐盟之

447 *Id.* annex I, art. II(2)(a).
448 *Id.* annex I, art. II(2)(c).
449 *Id.* annex I, arts. III(8)(g)-(h).
450 *Id.* recitals 29-31.
451 *Id.* annex I, art. II(6).
452 *Id.* recitals 32-36.

doi:10.6342/NTU202504586

資料保護機構合作、直接向資料保護機構進行投訴[453]、獨立替代性爭議解決機制，或是將 DPF 原則納入機構之隱私計劃並包含有效的求償以及執行機制，並由自律機構回應申訴。

當上述途徑以及美國商務部、FTC 均無法解決爭議時，資料主體可以訴諸具有約束力之仲裁。仲裁條款係規定於附件 I 之 DPF 原則之附件 I，資料主體可以通過仲裁來尋求剩餘救濟，並得到歐盟資料保護機構之協助[454]。仲裁小組由美國商務部以及歐盟執委會根據獨立性、誠信以及在歐美資料保護方面之專業指定之十名仲裁人組成。而其救濟內容係特定、非金錢性之救濟，當事雙方須承擔自身之一切費用[455]。所謂「剩餘救濟」係指在提出仲裁前應先窮盡向 DPF 機構尋求救濟、使用獨立之救濟機制，以及通過歐盟資料保護機構向美國商務部提供之所有免費救濟途徑後，始得提出仲裁，並且有一事不再理之要求[456]。仲裁之結果具有拘束力，並得依美國法尋求強制執行[457]。

資料主體亦應能直接向 DPF 機構投訴，並在 45 日內得到回覆或獲得救濟。其亦可向指定之獨立爭議解決機構提出投訴。獨立爭議解決機構應施加足夠嚴格之制裁和補救措施，以確保機構遵守 DPF 原則、要求組織撤銷或糾正不合規之影響、以及停止進一步處理資料並刪除之，最後公開調查結果，且每年應發布其調查之

453 *Id.* recitals 72, 77-79.
454 *Id.* recitals 83-85.
455 *Id.* annex I, annex I, ¶¶ A-B.
456 *Id.* annex I, annex I, ¶ C.
457 *Id.* annex I, annex I, ¶ E.

doi:10.6342/NTU202504586

年度報告，並受到美國商務部之驗證[458]。私營部門之獨立爭端解決機構和自律機構必須將 DPF 機構未能確實遵守其裁決之情況，通知具有管轄權之政府機構或法院以及商務部[459]。

DPF 機構亦得與歐盟資料保護機構合作，並在向美國商務部提出之認證聲明中承諾將在調查和解決根據 DPF 原則產生之問題與資料保護機構合作，並會遵循其提供之任何建議[460]。資料保護機構發出建議後，機構若無法在 25 天內配合或對於其延遲提出合理之解釋即會被認為嚴重違反承諾，而被送至 FTC 或美國交通部等對詐欺或虛假陳述案件中具有執法權力之美國機關進行執法[461]，最終可能會受到美國法之懲罰或是被移出 DPF 名單；反之若資料保護機構未採取行動，資料主體則可以向歐盟成員國之法院提起救濟[462]。

在刑事執法情況下，資料主體若認為權利受侵害，得向刑事執法機關或是向 PCLO 進行投訴，包括請求存取和更正資料，另外也有多數法律可以請求民事或刑事之司法救濟[463]。

FTC 則承諾會優先審查自律機構或獨立爭端解決機構、歐盟成員國以及美國商務部收到不遵守 DPF 原則之指控以適用聯邦交易委員會法第 5 條[464]之禁止商業中之不公平或欺騙性行為之規定，並透過禁制令來禁止受質疑之行為，或者在聯邦

458 *Id.* recitals 69-71.
459 *Id.* annex I, art. III(11)(e).
460 *Id.* annex I, art. III(5)(b).
461 *Id.* annex I, art. III(5)(c)(ii).
462 *Id.* recitals 75-76.
463 *Id.* recitals 112-18.
464 15 U.S.C. § 45.

doi:10.6342/NTU202504586

法院透過訴訟解決[465]。

倘若機構無法遵守爭端解決之決定，爭端解決機構應通知美國商務部和 FTC 或主管之法院，並被要求提出報告回應，未能配合者會被移出 DPF 名單[466]。除上述救濟機制外，資料主體亦可以透過美國法既有之規範，在普通法院提起訴訟[467]，另外亦有前述 EO 14086 建立之 CLPO 以及 DPRC 之二級救濟，共同建構了多元的爭端解決體系。

第五目 政府機關存取資料之限制

DPF 亦規定法律對資料隱私權之限制係限於必要性以及比例性原則之下，並制定有拘束力之明確規則以及施加最低保障措施，並可由獨立且公正之法庭進行爭端解決，並進行可強制執行之救濟[468]。

關於刑事執法目的，美國法下有搜索令或傳票之要求，並在其簽發、範圍均有嚴格限制，其行為態樣包括調取商業紀錄、電子儲存之資訊、通訊資訊紀錄等等，並應採取最不侵入性之調查方法[469]。而在民事或為監管目的發出之傳票，則適用類似之程序，由負責之機構依法律在確保調查係根據合法目的進行、手段與目的相關、發出機構尚未擁有傳票所欲尋求之資訊並已遵循必要之行政程序。雖然未有事前司法程序，但在事後之司法程序會受到司法審查[470]。

---

[465] Decision 2023/1795, *supra* note 10, art. III(11)(f).
[466] *Id.* recitals 72-73.
[467] *Id.* recitals 195-99.
[468] *Id.* recital 89.
[469] *Id.* recitals 92-93, 95-100.
[470] *Id.* recital 94.

doi:10.6342/NTU202504586

蒐集資料之後，聯邦機構應建立全面之隱私計劃，以確保隱私標準能夠貫徹。行政管理預算局（Office of Management and Budget）依法發布 A-130 通函，要求所有聯邦機構對於個人資料之創建、蒐集、使用、處理、儲存、維護、傳播和揭露，僅限於法律授權、或相關且合理認為對於適當執行授權機構職能所必需之範圍內。另外，聯邦機構必須確保個人可識別資料之準確、相關、即時和完整，並且僅儲存發揮其職能所需之最低限度之資料[471]。

電子政務法（E-Government Act）另外要求所有聯邦機構建立防止未經授權接觸資料之安全保護措施，類似的聯邦紀錄法（Federal Records Act）和其補充規定要求聯邦機構持有的資訊受到保障措施的約束，確保完整性並避免未經授權的存取[472]。除其他外，聯邦資訊安全管理法（Federal Information Security Modernisation Act of 2014）則授權行政管理預算局和國家標準與技術研究所（National Institute of Standards and Technology）制定對聯邦機構具有拘束力之標準，規定了資訊安全之最低標準，另外聯邦機構亦必須根據行政管理預算局之指導方針維護和實施資料洩漏之處理計劃[473]。

第六目 對政府機關之監督

刑事執法部門內均設有 PCLO，雖然不同部門之 PCLO 之間之具體權力可能略有不同，但通常都包括監督相關部門關於隱私和公民自由之問題，確保各部門建立

471 *Id.* recitals 101-02, 106.
472 *Id.* recitals 104-05.
473 *Id.* recital 104.

doi:10.6342/NTU202504586

適當程序處理個人之投訴。PCLO 應確保能獲得足夠的資源以履行其義務，並定期向國會報告[474]。

每個情報機構都設有監察長[475]，負責監督美國司法部之行動，其在定位上是獨立的，並有權獲得所有相關資訊。監察長針對非法行為或濫用權力之投訴進行調查[476]，雖然其發布之糾正行動建議不具拘束力，但其發布之報告通常會公開並會送交國會，並協助國會發揮其監督職能[477]。

在反恐活動之範圍內，具有刑事執法責任之部門受 PCLOB 之監督。PCLOB 亦可獲得相關資訊，可以向政府和執法機關發布建議，並定期向國會委員和總統報告，且其報告應在最大範圍內公開。另外刑事執法活動亦受美國國會特定委員會之監督[478]。

總統情報顧問委員會（President's Intelligence Advisory Board）內之情報監督委員會（Intelligence Oversight Board）負責監督美國情報機構之守法情況，並依 EO 12333 接受所有情報機構負責人對於可能違反行政命令或總統指令之情報活動之報告，並向總統報告未被司法部長、情報總監或情報機構負責人充分處理之情報活動，並向司法部長報告可能違反刑法之行為[479]。

美國國會之特定委員會亦對外國情報活動有監督責任，其會定期收到包括來

474 *Id.* recital 108.
475 *Id.* recital 165.
476 *Id.*
477 *Id.* recital 109.
478 *Id.* recitals 110-11.
479 *Id.* recital 166.

doi:10.6342/NTU202504586

自司法部長、情報總監、情報機構以及其他監督機構之報告，特別是國家安全法規定總統應確保國會情報委員會能充分且及時的瞭解美國的情報活動、非法情報活動、以及相關之之糾正行動[480]。除此之外不同之監督機構亦有特定應向國會報告之內容，使國會能發揮其監督權能[481]。

同時如同上述，CLPO 以及 PCLOB 均應發揮其監督功能，FISC 亦可在違反相關規定，例如違反目標選定程序之情況下，命令相關情報機構採取補救行動，例如終止獲取資料、刪除非法獲取之資料、以及要求政府停止或不開始執行 FISA 第 702 條之認證等[482]。情報界採取各種努力提高透明度並減少違法之行為[483]。

第四項 Data Privacy Framework 遺留之法律風險

雖然 EDPB 在 DPF 決定通過前整體給予支持之意見，但仍提出若干疑慮值得持續觀察。情報行動授權的程序並未改變，仍由 FISC 負責授權監控計劃。而由 DPRC 負責事後救濟則是一項重大的改革，提供了歐盟人民救濟管道，但是其是否能獨立運作仍待觀察。

DPF 則是納入了大量的 GDPR 規定，在美國的國內法與 GDPR 規範架構有本質上差異的情況下，DPF 提供的資料保護規則對雙方的合作有巨大貢獻。資料傳輸協議無法解決情報法規潛藏的問題，但是在資料的跨境傳輸以及處置上已經做

480 *Id.* recital 169.
481 *Id.* recitals 170-71.
482 *Id.* recital 174.
483 *Id.* recitals 172-73.

doi:10.6342/NTU202504586

出完整的回應。

第四節 Data Privacy Framework 之後續發展

第一項 聯合審查

DPF 之適足性認定決定中要求歐盟與美國在生效後一年內進行第一次對適足性認定之聯合審查。歐盟執委會蒐集了各利害關係人之資訊，特別是資料隱私權利相關之非政府組織、DPF 下認證之組織以及美國政府相關人員，另外還蒐集了大眾的回饋以進行參考。歐盟方面則有 EDPB 之代表、資料保護機構和歐洲資料保護監督員（European Data Protection Supervisor）參與[484]。

第一款 DPF 架構

美國商務部表示，第一年的目標是完善認證程序。截至第一次聯合審查為止，尚無收到由歐盟轉介的投訴案件，故尚無法評估此方面的執法成果。雖然沒有投訴的案件，但是美國商務部的職責亦包括自動查詢違反 DPF 的自我認證聲明，以及違反 DPF 規則的調查。美國商務部在此方面有所作為，拒絕了 33 個機構的自我認證登記。此外，美國商務部亦正在建立自動化檢查機制。在 FTC 以及美國交通部的執法行動中，雖然收到些許投訴案件，但是均係針對非 DPF 機構之投訴，可見

484 *Report from the Commission to the European Parliament and the Council on the First Periodic Review of the Functioning of the Adequacy Decision on the EU-US Data Privacy Framework*, EUR. COMM'N, at 1-2 (Oct. 9, 2024), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-EU-US-Data-Privacy-Framework-report-of-the-Commission-on-how-the-framework-is-functioning_en [hereinafter First Joint Review Report].

doi:10.6342/NTU202504586

截至第一次聯合審查為止 DPF 架構得以妥善運作[485]。

除了政府方面的監督機制外，DPF 下亦有私部門提供的監督機制。DPF 機構指定之獨立救濟機制之負責機構亦在審查會議中發表了其一年之間活動之報告，包括 Better Business Bureau（下稱「BBB」）、Verasafe、JAMS 以及 TRUSTe。BBB 表示其收到了 87 起來自歐盟資料的投訴，並只有 2 起符合解決條件，兩者均因為資料主體不再回應而終結。Verasafe 則收到 26 起投訴，僅有 6 起符合解決條件，其中的兩起關於存取以及刪除請求的投訴已受到解決，兩起仍在等待處理，以及兩起被撤回或是因資料主體未回應而結束[486]。

雖然監督及救濟機制得以妥善運作，但也可以從上述救濟機制低迷的投訴數量可以發現，歐盟資料主體對於其權利及權利行使機制可能並不夠了解。為解決此問題，美國商務部表示可以與歐盟資料保護機構合作，以提高歐盟資料主體對於 DPF 之了解，並得到歐盟執委會的支持。此外，對於 DPF 中特定議題及機構類型的特別指導方案也在建立中[487]。

第二款 監控行動授權基礎

FISC 在 2023 年 7 月 1 日針對批准了三項外國情報類別：(1)外國政府及相關實體、(2)反恐、以及(3)打擊武器擴散，並經過針對性和最小化處理[488]。受到日落

[485] *Id.* at 2-5.
[486] *Id.* at 5-6.
[487] *Id.* at 7-8.
[488] *Id.* at 12.

doi:10.6342/NTU202504586

條款影響，美國國會在 2024 年 4/19 日通過了 RISAA 以重新授權 FISA 第 702 條，進行變更，包括 FISA 第 702 條允許的監控活動範圍以及機構與程序的變更[489]。

RISAA 擴大了外國情報訊息的定義，包括與反毒品相關的訊息，此與美國遇到毒品危機有關[490]。此外，RISAA 亦擴大了電子通訊服務提供商之定義（Electronic Communication Service Provider），從而擴大了可能被強制提供訊息的公司的範圍，現今之定義係「獲取正在或可能用於傳輸或儲存有線或電子通訊的設備」的其他服務提供商，同時明確排除公共居住設施、住宅、設居設施和食品服務場所。美國司法部表示這只會額外涵蓋極少數的技術公司，並承諾會縮小其範圍，但其本質上仍是擴大解釋範圍，故引來了擔憂，目前在國會中有進一步修訂之法案。另外，PCLOB 在會議中確認，即使 RISAA 進行了改革，亦不影響 EO 14086 的規範，並未限制資料主體行使權利[491]。

RISAA 將原本實踐之程序法規劃引入了新的保障措施，其中部分增加了對可能受到 FISA 第 702 條監控之非美國人士相關的保障。首先是增加了額外的問責、監督和報告要求。最後，RISAA 設立了由國會成員、PCLOB 主席、國家情報首席副總監（Principal Deputy Director of National Intelligence）、副司法部長（Deputy Attorney General）以及國會認命的其他成員組成 FISA 改革委員會（FISA Reform Commission），以對於 FISA 之改革作出建議[492]。

---

489 *Id.*
490 *Id.* at 12-13.
491 *Id.* at 13-14.
492 *Id.* at 14-15.

doi:10.6342/NTU202504586

自數據層面以觀，透過 FISA 第 702 條授權監控之目標數目仍在上升，而情報總監辦公室表示其中有多種原因介入，包括情報優先級的變化、世界的變化、技術能力、目標行為、以及電信行業的變化等。另外 DPF 機構也在許可下一定程度的公布了其收到國家安全信函請求資料之次數，近年來這些數字保持相對穩定[493]。

美國情報機構亦會透過購買的方式來獲取商業機構的資料，此等行為不在 FISA 以及 EO 14086 之規範範圍內，但是 DPF 中對於自願與第三方分享資料之行為有所約束。FTC 對於銷售敏感資料的資料經紀商 Outlogic 採取了執法行動，對於其未告知個人相關之銷售情況、未能採取措施給予個人退出的機會、允許將資料用於潛在的歧視性目的、以及並未限制第三方使用此類訊息等缺陷，FTC 禁止其向第三方銷售地理位置資料，並刪除其非法使用和分享的資料。歐盟執委會相信並認為 FTC 在 DPF 認證機構違反上述規定分享資料時會採取相同的行動[494]。

第三款 監控行動之監督及救濟機制

情報界對於其內部運作持續提出評估以及報告，並由情報總監辦公室的監察長辦公室進行全面管轄。PCLOB 則有特定的監督職能，其啟動了一個監督項目以(1)審查情報機構採納的更新政策和程序的實施情況，以確保與 EO 14086 一致，以及(2)對新的補救機制運作進行年度審查。PCLOB 亦針對 FISA 第 702 條提出報告，包含與其有關之監控計劃運作的相關事實和法律資訊，並對於情報機構提出遵守

493 *Id.* at 15-16.
494 *Id.* at 16-17.

doi:10.6342/NTU202504586

法規之建議，也向美國國會提出有關重新授權之建議。另外，PCLOB 之部分成員之任期即將到期，其新成員之選任也引來了擔憂與關注[495]。

EO 14086 向司法部長建議建立新的補救機制，以處理涉及關於傳輸到美國的個人資料受到影響隱私與公民自由之違法行為，也就是 CLPO 與 DPRC 之兩階層救濟機制。EDPB 與美國採取了多項措施以促進投訴之提交和處理，並建立了加密的通訊管道，但截至審查會議為止，此救濟機制尚未被觸發過[496]。

第四款 歐盟執委會之結論

根據審查中之資訊，歐盟執委會認為美國當局已經建立必要之結構和程序以確保 DPF 之有效運作。惟因自 DPF 生效以來僅過去一年，關於保障措施之實際應用經驗必然有限，故歐盟執委會將會持續密切關注，特別是(1)PCLOB 即將發布關於 EO 14086 的實施以及訊號情報救濟機制運作之報告、(2)FISA 第 702 條潛在的進一步修訂、以及(3)PCLOB 新成員之提名以及認命。

另外，歐盟執委會亦提出了三項確保持續有效運作之重點：(1)美國商務部充分利用 DPF 中之管道，以監督 DPF 機構遵守原則之情況，並識別虛假聲明、(2)FTC 進一步發展主動調查和執行認證機構遵守 DPF 則之方法、以及(3)美國商務部、FTC、以及歐盟資料保護機構就 DPF 原則下之關鍵要求制定共同指導之工具[497]。

---

[495] *Id.* at 17-19.
[496] *Id.* at 19-21.
[497] *Id.* at 21.

doi:10.6342/NTU202504586

第五款 小結

本次審查中美國方面展現出了執行上的積極性，在監管以及執法上積極運作，並持續開發有助於監管與執法的工具以及政策，以及積極與歐盟方面合作。但亦顯現出了部分問題。

首先是 FISA 第 702 條之監控授權仍然持續增加，雖然美國方面表示係因有各種不同之因素共同造成，言下之意即是美國並非有意持續擴大監控措施，但此一事實對於改善 CJEU 對於美國情報法規的看法是不利的。

其次是以歐盟資料主體提出之申訴中，其數量小、符合要求之申訴比例亦較低，可以顯現出資料主體對於 DPF 下之救濟機制可能並不了解及熟悉，審查會議中也提出此等問題，在未來應致力改善之。

本文認為，美國方面積極監管及執法為歐盟人民的資料隱私帶來巨大助益，也改善了過去資料傳輸架構的問題，展現了合作的誠意。除了積極管理 DPF 機構外，情報體系也大幅度的改良，建立了大量的監督機制；惟仍然欠缺事前授權，可能成為影響雙方合作前景的關鍵。

第二項 EDPB 之報告

在第一次聯合審查中，EDPB 亦派出了五名代表參加，並發布了相關報告。EDPB 之報告內容與前述第一次審查報告高度重疊，但也提出了其他的意見，為免重複，以下將僅節錄額外之具體建議。

doi:10.6342/NTU202504586

首先對於自我認證機制，EDPB 認為主動開啟合規行動之監測有其重要性，並且其認為雖然自動化檢測機制可以有效幫助監管，但只能補充，而不能取代對具體案例的個別調查和評估。另外，有大量已經退出或是被列為不活躍之機構，其是否歸還或刪除資料並未在 DPF 之網站上被公布，也不清楚其是否已經回應美國商務部其對於資料之處理方式[498]。

其次是許多 DPF 機構並不了解將來自歐盟之資料再次傳輸到未有適足性認定之第三國之要求，EDPB 建議美國商務部針對持續傳輸進行指導，並發布持續傳輸責任原則（Accountability for Onward Transfer Principle）[499]。

在人力資源資料之問題上，自隱私盾時期歐美之間即對其範圍之定義有所出入。美國商務部向來認為僅有在同一企業集團內部處理僱員資料才屬於 DPF 下之人力資源資料，但 EDPB 卻認為任何與僱傭關係相關的僱員個人資料均屬之。EDPB 支持美國商務部表示願意在聯合審查過後的數月內制定關於人力資源資料相關之指導原則，以消除此等分歧帶來的問題，並希望在發布前與美國商務部討論以使雙方能達成共識[500]。

在造成許多討論的必要性與比例原則之討論中，EDPB 希望可以在定期審查中進一步討論具體之實例，而目前仍無法評估其在實務上的實施情況，並需要持續仔

[498] *EDPB Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework*, EDPB, ¶¶ 8-9 (Nov. 4, 2024), https://www.edpb.europa.eu/system/files/2024-11/edpb_report_20241104_reportonfirstreviewofeu-u.s.dpf_en.pdf.
[499] *Id.* ¶ 16.
[500] *Id.* ¶¶ 17-18.

doi:10.6342/NTU202504586

細監控。EDPB 另外指出 PCLOB 之審查將對深入理解與探討此議題特別有幫助，故呼籲歐盟執委會可以特別關注 PCLOB 是否有發現個機構內部政策與程序中是否有任何缺失，並是否已透過 PCLOB 提出之建議而獲得妥善處理[501]。

在 FISA 第 702 條之重新授權議題上，EDPB 認為 PCLOB 建議將 EO 14086 的十二項合法蒐集目標編入法典，可以將 EO 14086 與 FISA 第 702 條之外國情報的定義統合，並賦予 FISC 明確的管轄權，在審查時適用 EO 14086 之標準，而 RISAA 並未為之[502]。

在引起眾多討論的 DPRC 法官之獨立性問題上，EDPB 表示自 EO 14086 以及司法部長發布之法規所提供之保障措施，無法消除對 DPRC 的獨立性產生的合理懷疑，應在實際運作中持續觀察，EDPB 並認為 PCLOB 若能在其針對首次聯合審查所發布之報告中，著重探討獨立性問題將特別具參考價值[503]。

本文認為，EDPB 對於審查之結論整體與聯合審查之報告差異不大，其提出多項建議，並且在因施行期間過短而無法有效觀察之議題上，如同其針對 DPF 決定之意見相同，提出了仍應密切觀察之議題。此外，報告中可以得出其對於 PCLOB 作為監督機制的重視程度，在多數議題上均期待 PCLOB 可以發布報告以仔細說明，也提高了 PCLOB 新成員選任及空缺填補之問題之重要性。

501 *Id.* ¶¶ 28-30.
502 *Id.* ¶ 39.
503 *Id.* ¶ 56.

doi:10.6342/NTU202504586

第五節 小結

本章介紹了歐美歷來的三個資料傳輸架構，以及在各自時期情報法規的變化和改革。在合作的過程中，美國持續的對 CJEU 的質疑進行回應。本文認為，在 DPF 架構的設計以及運行上已經達到了相當高的水準，基本上解決了跨境資料傳輸過去的缺陷。

惟在情報法規的議題上，是否已經達到了 CJEU 的要求？多數意見認為仍有改良的空間。情報機構事前授權的問題在合作過程中幾乎未受更動。雖然 EO 14086 加入了必要性與比例原則要求，並列舉了得進行情報行動的國家安全目標，但是 FISC 仍僅寬泛的授權監控計畫，而不具體授權監控目標，美國並未在此問題上進行回應。

其餘的問題大多均有一定程度之改善，在救濟機制上，DPRC 的獨立性是否足夠意見分歧，本文認為，其日後的運行成果將大幅度左右論者對其之看法。而其制度設計本身是否能滿足 EUCFR 第 47 條之要求？仍有模糊之處，論者也對其提出能改進之空間，但事實上 DPRC 法官已有高度之獨立性保障，為歐盟人民的資料保護水準給予高度貢獻。

在瞭解資料傳輸架構之議題，以及 DPF 所受之評價後，本文將於第伍章聚焦重要之核心議題，並提出現存美國規範與 CJEU 的高標準之間的差距，並分析如欲確保 DPF 決定的有效性，美國所應進行之改革。

doi:10.6342/NTU202504586

第肆章 Data Privacy Framework 存續所需之改革

noyb[504]是 Schrems 創立的一個非政府組織，致力於執行資料隱私保護的法律[505]。noyb 認為 DPF 基本上只是過去失敗的隱私盾協議的複製品而已[506]，故其在 2023 年 7 月 10 日表達了對 DPF 之批評並宣稱即將會有針對 DPF 之訴訟[507]。此舉顯示出 DPF 仍有可能需要再次面臨 CJEU 的檢視。

CJEU 在 Schrems II 案中闡釋了與歐盟實質相當的資料保護水準所需的要求。如欲以判決中 CJEU 所提出之要求為基準，美國現行的法規以及 DPF 所提供的資料保護水準是否足以滿足 CJEU 的要求？以及美國如欲達成 CJEU 的要求，應為如何之改革？本章將逐一分析。

第一節 關鍵議題

DPF 很大程度弭平了歐美在資料隱私保護領域的差異，惟其無法影響情報體制的問題。在 Schrems II 案中 CJEU 對美國情報法規提出的質疑在 EO 14086 下得到了舒緩，但是其亦並未完全的作出回應，加上行政命令之法律地位，仍然被認為無法完整的達到 CJEU 的要求。本節將逐一分析現行美國法規與 DPF 的運行狀況，並與 CJEU 之標準進行比較，以確認其對 CJEU 的質疑是否完整回應，以及分析

---

504 名稱來自於「none of your business」。*FAQs*, NOYB, https://noyb.eu/en/faqs (last visited Mar. 12, 2025).

505 *About us*, NOYB, https://noyb.eu/en/about-us (last visited Mar. 12, 2025).

506 *New Trans-Atlantic Data Privacy Framework largely a copy of "Privacy Shield"*. noyb *Will Challenge the Decision.*, NOYB, https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu (last visited Mar. 12, 2025).

507 *European Commission Gives EU-US Data Transfers Third Round at CJEU*, NOYB (July 10, 2023), https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

doi:10.6342/NTU202504586

其中的爭議。

第一項 情報機構監控行為之授權

第一款 情報行動之定義問題

如前所述，EO 14086 仍未對情報行動進行精確定義，不同情報機構可能產生不同之解釋結果，進而影響法律監督之統一性和可預測性。故 CJEU 在 Schrems II 案中即曾強調清晰、精確和透明的資料處理實踐的必要性，並指出此處之模糊定義可能對 DPF 帶來法律風險[508]。

第二款 FISA 第 702 條改革建議

PCLOB 在 2023 年 9 月發布了關於 FISA 第 702 條之運作報告，並在其中提出建議。FISA 第 702 條之爭議在美國很大程度聚焦在如何避免無意或有意的監視到美國人從而違反美國憲法第四修正案的要求[509]，而本文主要聚焦於對歐盟資料主體之資料保護議題。惟此等討論關乎如何提高情報機構之監管，以及如何確保如最小化程序等原則適用於所有情報機構之資料蒐集行為，故仍有參考價值。

PCLOB 建議將 EO 14086 之 12 項合法蒐集目標編入法典，可以使其與 FISA 中對於外國情報的定義保持一致，進而提供對隱私和公民自由的保護，並縮小 FISA

[508] Dimović, *supra* note 98, at 101.
[509] *See generally* Gemar, *supra* note 23; Chauvin, *supra* note 33; *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, THE PRIV. & C.L. OVERSIGHT BD. 1 (Sept. 28, 2023), https://documents.pclob.gov/prod/Documents/OversightReport/054417e4-9d20-427a-9850-862a6f29ac42/2023%20PCLOB%20702%20Report%20(002).pdf [hereinafter PCLOB Report on FISA 702].

doi:10.6342/NTU202504586

第 702 條之蒐集範圍。另外，EO 14086 雖具有法律效力，但 FISC 目前並無法定管轄權執行行政命令，因此無法在評估 FISA 第 702 條之蒐集計劃的合法性時將其納入考量，PCLOB 認為法典化將可以提供必要的明確性並確保 EO 14086 在司法體系中得到適當之執行[510]。此外，PCLOB 亦有提出諸多聚焦於改善情報機構的內部流程以及內部的審計，以及加強培訓情報機構的內部人員之建議[511]。

整體而言，PCLOB 之建議並未對 FISA 第 702 條提出重大變更，主要係聚焦於監管措施及具體之作為。其較為重大之建議主要係將 EO 14086 之合法蒐集目的法典化。如前所述，在歐盟法的規定下，國家安全事由並不需要被細分，但文獻普遍提出美國總統有權增加國家安全目的係一問題，倘若採取 PCLOB 認為應法典化之看法，或可解讀為其亦認為不應賦予總統該權力。另外 PCLOB 亦認為法典化後可以成為 FISC 認證監控計劃時之依據，應可有效限制監控計劃在目的上之範圍。本文認為，將 EO 14086 的 12 項目標法典化雖然可能不必要，但是可以提供顯著的幫助。

除了監控目標是否法典化的討論以外，FISC 是否進行個別化授權，也是其是否可以滿足 CJEU 所定義的「事前獨立授權」的重要審查因素之一，CJEU、EDPB 以及歐洲議會均曾對此議題提出意見[512]，為重要之關鍵議題之一。

第二項 必要性與比例原則解釋問題

[510] *Id.* at 202-03.
[511] *See id.* at 214-25.
[512] *See supra* text accompanying note 342, 378, 379, 407.

doi:10.6342/NTU202504586

EO 14086 要求訊號情報工作限於在與經驗證之優先情報成比例之範圍和方式下進行，強化了比例原則之概念。在美國法的解釋下，必要性被定義為無可行之其他手段，比例原則要求政府證明沒有限制性較小的方法可以用以實現相同之目標，進而將基本權利之侵害最小化，並由壓倒性的公共利益證明是合理的。有觀點認為其與歐盟法實際上非常接近[513]，但亦有觀點認為其無法滿足歐盟法之要求[514]。

歐盟與美國之間必要性與比例原則之差異亦體現在大規模蒐集之議題上[515]，鑑於大規模蒐集對基本權利之侵害較針對性蒐集高出許多，要能夠通過比例原則之審查之難度亦高出許多。

必要性與比例原則在歐洲人權法院之解釋下已確定必要一詞包含比例原則的概念，亦即除非與所追求之目標成比例，否則不能被視為在民主社會中所必要，而 EO 14086 始終將之進行區分，並以與美國法傳統之解釋表達之[516]。至於在美國法下，必要性與比例原則之用語雖始於 EO 14086，但其法律概念在美國法下亦原已存在。至於其是否能達到歐盟之標準，應在具體案例中分析，歐洲議會與 EDPB 即支持此觀點[517]。

綜上，本文認為必要性以及比例原則之引入，提供美國實務解釋的基礎，可用以調整其情報行動之授權，並進一步貼近歐盟之標準，進而可透過雙方之談判、持續之聯合審查以及採納 PCLOB 之相關意見，提供解決雙方解釋差異的空間。雖然

513 Joel, *supra* note 336, at 12-18.
514 Dimović, *supra* note 98, at 100.
515 *Id.* at 101.
516 *Id.* at 98.
517 *See* EDPB Opinion, *supra* note 11, at 31; EP Opinion, *supra* note 404, ¶ J.

doi:10.6342/NTU202504586

美國法與歐盟法在解釋上有差異，但是 CJEU 已表示授予適足性認定不以有相同之法規範圍必要，僅需能達到實質相當之保護水準，故不應僅因解釋方式不同而直接認定美國法保護水準較低。

第三項 救濟機制

是否建構獨立並且有效之救濟機制，係 CJEU、歐盟執委會以及學術文獻中共同關注之議題。CJEU 並不要求救濟機制必須設於司法機構，而應就其運作方式進行判斷，但直至首次對 DPF 適足性認定之聯合審查為止，DPRC 並無運作之紀錄[518]，故僅能透過其規範設計進行判斷。DPRC 有保障其獨立性之機制，惟其與美國聯邦法官之獨立性要求亦有差距。如同歐洲議會所指出，DPRC 由司法部長任命，而總統對法官的罷免權力沒有限制，總統也有權推翻 DPRC 的決定，故法官之續任也依賴於行政部門，這些均會對其獨立性造成影響[519]，對於 CJEU 可能無法滿足 EUCFR 第 47 條之要求。

其次是其決定之透明度問題。不論是 CLPO 或 DPRC 均只會認定是否有違規行為存在，而不給予資料主體參與程序之機會，亦不提供理由。雖然其設有特別辯護者代表資料主體之利益參與程序，但特別辯護者之獨立性亦不完整，在得到不利之決定時亦無法繼續救濟。考量到情報行動本質上具有機密性，使資料主體無法參與程序或許有其正當性，但仍可透過例外情況之設計，例如資料解密後之通知或是

[518] First Joint Review Report, *supra* note 484, at 19-21.
[519] Dimović, *supra* note 98, at 97.

doi:10.6342/NTU202504586

在必要之情況下提供陳述意見之機會，以改善透明度問題。

綜合而言，DPRC 救濟機制之保護水準仰賴美國總統、DPRC 法官、以及特別辯護者之公正性以及妥善運作，並未在法規上提供最低之保護底線，同樣可能會使此救濟機制無法滿足 CJEU 之要求。

此外，在第一次聯合審查中顯現出了歐盟資料主體對自身權利或是救濟機制之使用上可能不了解之問題，提出投訴之數量較低，其中合格投訴之比例亦較低，美國商務部因此認為應提高歐盟資料主體之權利意識，以及對救濟機制之熟悉程度，並希望積極與歐盟資料保護機構合作。實際上，資料主體對於救濟機制及自身權利之不熟悉恐非美國方之責任，但美國願意積極促進資料主體之權利實現，仍值得肯定。

第四項 DPF 機構管理

在第一次聯合審查中，美國商務部就其自身執行層面展現其積極性，例如拒絕了部分不合格之認證登記，亦持續發展自動化檢查程序。另外，FTC 收到之投訴亦均係針對非活躍機構、未參與 DPF 框架或是未涉及自歐盟傳輸資料之機構，也就是未有針對虛假聲明之機構之投訴，可見 DPF 框架之審查機制得以良好運作並初具成效。另外，FTC 亦有主動調查中之案件，在歐盟資料主體對於其權利之認知以及行使可能還有待加強之背景下，美國機構之主動調查對於其權利保護之重要性大幅提升，在此方面也提供了良好的助益。

doi:10.6342/NTU202504586

第二節 美國立法及修法建議

經過前述分析，本文認為美國現行的資料隱私保護法規無法完全滿足 CJEU 立下之高標準，故本節將分析美國如欲完整滿足 CJEU 之要求，並且確保 DPF 可以長期存續所需進行之修法以及改革。本節主要分為兩部分，首先分析 FISA 第 702 條之修正建議，其次係美國聯邦層級資料隱私保護法律之討論。

第一項 FISA 第 702 條修正

即使 EO 14086 有相關限制，美國之情報機構監控法規亦無法滿足 CJEU 之要求，且行政命令之法律位階本身即有其風險。在 EO 14086 制定之初，即有民間倡議認為美國之監控制度問題不能單靠行政命令解決，而應由國會制定有意義之監控改革，否則跨大西洋資料傳輸之爭議將會為美國企業帶來巨大的代價[520]。

第一款 情報行動授權

在所有應調整之問題上，本文認為 FISA 第 702 條、EO 12333 以及 EO 14086 共同構築之情報行動授權體系之修正最爲重要。首先，FISC 以及 FISCR 作為既存之授權法院，應使其事前審查中。除進行適當性之審查外，亦包含必要性及比例原則之審查，並於法規中劃分其範圍以及審查標準。而 EDPB 已指明美國自身已有高標準，故將其明文化並納入 FISA 第 702 條，亦能達到與歐盟實質相當之保護水

[520] *New Biden Executive Order On EU–US Data Transfers Fails to Adequately Protect Privacy*, ACLU (Oct. 7, 2022), https://www.aclu.org/press-releases/new-biden-executive-order-eu-us-data-transfers-fails-adequately-protect-privacy.

doi:10.6342/NTU202504586

準。此外，傳統 FISC 在進行個別化決定時，需確認有理由相信目標是外國勢力或外國勢力的代理人，並且目標正在使用或即將使用特定設施後才能發出[521]，惟個別化授權並未出現在 FISA 第 702 條之授權內，2023 年授權之三項目標均非常廣泛[522]，即使使情報機構在執行目標選定時可選擇之目標數量相當大，即使確實透過最小化程序嚴格選定，該選定程序亦非事前之司法審查，若得以透過 FISC 進行選定，始能成為 CJEU 所認定之事前司法審查。

在大規模蒐集之問題下，CJEU 並不認為其本身違法，且歐盟成員國亦有大規模蒐集資料之行動，本文亦認為要求美國完全停止大規模蒐集對其主權之影響過大，實際上並不可行，故問題應聚焦在執行層面。在執行層面，美國大規模蒐集之監控對象之數量過於巨大，並且在近年有逐年上升之趨勢（截至 2023 年）[523]，自表面上來看即有授權寬泛之外觀，故本文認為美國應考量如何進一步限制大規模蒐集之範圍以期達到 CJEU 所要求之標準[524]。

在合規之問題上，PCLOB 指出根據 FISA 第 702 條之監視措施蒐集了過多資料，同時，即使情報規範相當寬鬆，情報機構在遵守規範上顯得並不配合[525]，導致資料隱私被高度侵害。故除了法律之修正外，持續加強情報機構之合規也是應努力

---

521 George W. Croner, *FISA Section 702's Challenging Passage to Reauthorization in 2023*, 14 J. NAT'L SEC. L. & POL'Y 55, 64-65 (2023).
522 *See supra* text accompanying note 488.
523 PCLOB Report on FISA 702, *supra* note 509, at 58; *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities*, OFF. OF THE DIR. OF NAT'L INTEL. 1, 19 (Apr., 2024), https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf. Calendar Year 2023at 19
524 Pedersen, *supra* note 19, at 233-34.
525 Connolly, *supra* note 61, at 118-19.

doi:10.6342/NTU202504586

之目標。

此外，合法之授權監控目標之法規化亦係多方向來之倡議，包括 PCLOB 之建議。在目標增加之問題上，亦應有國會之同意程序，以免除總統濫權以及不透明之疑慮。

第二款 救濟機制

本文認為，將 DPRC 之二級救濟體系一同納入 FISA 第 702 條之範疇，亦可解決其由行政命令建立帶來之不穩定性。此外，由國會通過法律亦可排除總統干預其獨立性之權力。雖然歐盟資料主體自始均可以在聯邦法院依美國法提起訴訟，但由於多層保密，以及原告需要證明自己因為隱私侵犯而導致實際損害，使得法庭上確立地位之要求相當嚴格，歐盟資料主體實際上難以在民事訴訟中挑戰 FISA 第 702 條或是 EO 12333 所授權之監控活動[526]。DPRC 體系所帶來之較低之開啟救濟之門檻，在面對高度不透明之情報機構行動有其必要性，故此體系之留存，或能確保歐盟人民得以行使其救濟權利。

本文建議美國國會應透過立法將 DPRC 建立為真正之法院以免去爭議，並考慮增加其上訴機制，例如 FISCR 之於 FISC 之關係，或是使 DPRC 之決定可以被上訴至上訴法院，如此一來始有真正之二級司法救濟體系。另外。DPRC 不進行事實認定之問題也可藉由修法改善，以完善救濟體系之完整性，特別辯護者無法參與

[526] Dimović, *supra* note 98, at 96-97.

doi:10.6342/NTU202504586

CLPO 程序之問題也可以一同解決。

第四款 小結

FISA 第 702 條之修正建議大體上係將 EO 14086 之內容法規化，並將其未完成之改革予以完善。除情報行動授權以及救濟機制等大方向之改良外，EO 14086 內關於資料之保存以及傳輸之規範之法規化，亦得以提高資料隱私保護水準，並使其更加貼近歐盟之法規。最終對於 CJEU 而言，美國之資料保護水準是否足以獲得適足性認定高度仰賴 FISA 第 702 條之改革。

第三項 美國聯邦資料隱私保護法律倡議

對於美國來說，以國家為單位獲得適足性認定必定較以 DPF 框架獲得適足性認定在商業上更佳[527]，而目前之努力方向均為透過 DPF 架構之額外要求，諸如獨立之申訴機制以及對 DPF 機構之資料處理要求，以試圖達到歐盟之標準。

有論者針對美國聯邦隱私法規的建立提出意見。首先，美國已經有數州已經通過了受 GDPR 高度啟發的隱私法律，並且預期未來會有更多州跟進[528]。雖然多數州法律之間有相似性，但仍有不同，而要遵守所有不同的法律會帶來高成本，故制定聯邦等級的法律，有助降低法律遵循成本，並且也可以直接使所有州的人民甚至外國人都同時受到保護[529]。

---

527 Shaun G. Jamison, *Creating a National Data Privacy Law for the United States*, 10(1) Cybaris® 1, 23-24 (2019).
528 Gerke & Rezaeikhonakda, *supra* note 221, at 400.
529 *Id.*

doi:10.6342/NTU202504586

其次，聯邦層級之隱私法律有助於證明其與 GDPR 第 45 條之要求更進一步靠近，蓋美國是所有獲得適足性認定之國家內唯一沒有涵蓋全國的隱私法令的國家，雖然 EO 14086 有全國效力、並且針對相關行為進行規範，但行政命令本質並非國會所通過之法律，其變更不需國會之同意，也與歐盟無關，而不需要與歐盟溝通，亦可以被總統變更或廢除[530]，與聯邦法律之地位無法相比，對歐美跨境資料傳輸議題之影響並不顯著。基此，聯邦層級之隱私法律的存在對於美國與歐盟之間資料保護協議之存續有正向的影響，且可能有必要。

再者是訴訟權的問題。資料主體在遭遇情報機構不法侵害時，因為國家機密特權，難以證明其所受之損害，甚至是其正在受到監控之事實，此困難已被美國最高法院確認[531]。另外即使經過 DPRC 之程序，欲得到救濟之資料主體依然無法確認真實情況為何。有見解認為，資料主體若係基於 SCCs 之契約義務對美國機構提出訴訟，會比對美國政府提起訴訟更加容易[532]。

第一款 聯邦隱私法律立法倡議及分析

第一目 建立類似歐盟標準

與歐盟有 GDPR 作為保護隱私的基本法律不同，FTC 透過監管不公平和欺騙性交易行為保護消費者個人資訊，但其權力僅限於其被授權之特定法律，並未有完

530 *Id.* at 400-01.
531 Connolly, *supra* note 61, at 114-16.
532 *Id.* at 116.

doi:10.6342/NTU202504586

整監管所有資料隱私事務之權限。另外，科技之持續發展可能導致原有之法規並不能包含新型態之權利侵害行為，鑑於此缺陷，美國各州正在制定自己之法規，並效仿 GDPR 模式賦予消費者對自身資料隱私之權利[533]。

加州透過實施加州消費者隱私法案（California Consumer Privacy Act，CCPA）開創了州等級之資料隱私立法之趨勢，其後又有加州隱私權法（California Privacy Rights Act，CPRA），並採用了類似於 GDPR 之模式，相較於部分州對於行業較為優惠，加州採用了與 GDPR 相同之選擇加入模式以及要求企業揭露資料蒐集並根據消費者請求刪除資料等[534]。

本文認為，在部分州已經有 GDPR 模式之立法背景下，可以看出其模式在美國是可行的。透過此種立法可以大幅消除美國與歐盟之間之法規差異，在未來之合作及互動上可以帶來效益。另外，透過聯邦級之立法改革，配合 FISA 第 702 條之修法也可能促使美國得以獲得完整之適足性認定，也可以降低美國商務部等行政機關在驗證上之成本，以及降低複雜性。

第二目 統一國內標準

首先，統一標準對產業發展有利，可以提供更簡化的做法以降低法遵成本，並可以提高明確性以及透明度。此種作法可以提高在全球經濟中的競爭力，許多大型企業已表達支持並積極促進聯邦資料隱私法律之立法，但此立法也可能對不具備

[533] Lydia Rudden, *Fragmented Data Privacy Laws: Time for Federal Legislation*, 2025 B.C. INTELL. PROP. & TECH. F. (forthcoming 2025) (manuscript at 4-5).
[534] *Id.* manuscript at 3-10.

doi:10.6342/NTU202504586

處理最基本要求能力的小型企業產生不成比例之影響，其成本可能超出其負荷能力。隨著各州調整其資料隱私法規，若聯邦資料隱私法律採用此些州法律之共同特點可能可以降低負擔，例如對現行州法律進行認可等[535]。

聯邦資料隱私法律也可以消除管轄權模糊之問題。因各州規範密度不一，消費者若在不同州之間移動而使用不同州內之法律，對各服務提供者而言難以辨別各消費者所受之保護程度，故導致了較高之法律風險，此外不同之規範密度亦可能阻礙企業擴展至保護密度較高之州，亦可能使企業僅在保護密度較低之州開展業務，而使保護密度較高之州無法獲得特定產品或服務，亦或是失去工作機會[536]。

較高之資料保護水準會帶來更高之合規成本，企業可能會試圖遊說各州，試圖使保護密度較低之資料保護法規成為多數，進而影響未來可能出現之聯邦資料隱私保護法。儘管此遊說力量可能導致聯邦層級的立法失敗，企業仍可能自行採取 GDPR 等級之高標準。另外，企業也可能會移往保護密度較低或是較為一致之國家，從而導致資本移出美國[537]。本文認為，建立聯邦資料隱私保護法律可以統一標準，為美國的資料相關產業帶來助益。

第三目 提高美國的資料保護水準

隨著 GDPR 的出台，美國消費者對於其個人資料之隱私之重視也隨之提高，聯邦的資料隱私保護法律可以提供消費者統一的資料保護法規。亦有反對資料隱

535 Jamision, *supra* note 527, at 119-21.
536 Rudden, *supra* note 533, manuscript at 9-11.
537 *Id.* manuscript at 12.

doi:10.6342/NTU202504586

私法規的企業認為消費者接受提供資料以換取更加個性化的服務，但此問題可以透過選擇權解決；反而，若未提供此種選擇會剝奪美國人之基本隱私權。此外，聯邦資料隱私立法亦可以給予資料安全保護，避免受到洩漏導致被分享給不良之第三方[538]。

聯邦資料隱私保護法律應包含一套強而有力，並且可以適用所有消費者之消費者權利。目前機構需要根據消費者居住地提供不同之權利，包括存取、刪除個人資料，以及對於敏感和非敏感資料的同意權、退出權等。而在執法方面，在沒有特定政府機構執行聯邦法律之情況下，國會應考慮建立私人的民事訴訟權以直接起訴侵犯其隱私權的機構[539]。

惟如前所述，在面對情報機構之行為時可能會需要面對國家機密特權之問題，故本文認為，立法設計上應能參考 DPRC 之信念測試以降低起訴門檻。另外，鑑於資料傳輸之全球性，在考量量聯邦層級之資料隱私保護法律時，亦應將外國人民之救濟權利一併納入考慮，以達到給予及時且有效救濟之目的。

第二款 現行發展

在 2024 年，美國隱私權法案（American Privacy Rights Act，下稱「APRA」）被提出，延續了過去聯邦隱私立法提案的特質[540]。APRA 由不同黨派的議員提出，

538 Jamision, *supra* note 527, at 119, 121.
539 Perumal, *supra* note 5, at 122-23.
540 Lothar Determann et al., *American Privacy Rights Act - A First Glance at the US Congress's Newest Comprehensive Privacy Bill*, 6(4) J. DATA PROT. & PRIV. 1, 8 (2024).

doi:10.6342/NTU202504586

並受到支持，有論者對其前景表達樂觀的態度[541]。

APRA 採用了許多 GDPR 的概念，但是保護水準與 GDPR 仍有差異，例如 APRA 主要採用消費者選擇退出（Opt-out）機制，為事後選擇的權利，但是 GDPR 系採取事前選擇的加入（Opt-in）機制[542]。此外，APRA 不包含美國國內所有的機構，僅包含受 FTC 所管轄的企業、運輸業者與非營利組織，並且同時排除小型企業[543]。

根據美國憲法第十修正案，所有未明確授予聯邦政府的權力會保留予各州[544]，故各州擁有監管資料隱私之權力，但聯邦亦有權力監管各州之間的商業行為[545]。APRA 採取原則排除州法的規範方式，但是在部分情況仍允許適用州法，例如有關員工隱私，或是有關健康資訊隱私的法律。此設計可能會對特定州內的機構帶來挑戰，例如在特定州內的賠償金額過高，或是帶來法律不確定性[546]。

本文認為，APRA 對美國的資料保護水準有正向的幫助，但是並未能完整帶來本文前述所提及之效益。首先，雖然 APRA 採取了聯邦法規優先的設計，但是允

---

[541] APRA 由民主黨參議員，同時為商務、科學和交通委員會主席的 Maria Cantwell，以及共和黨眾議員，同時為能源和商業委員會主席的 Cathy McMorris Rodgers 共同提出。*Id.* at 19; *The American Privacy Rights Act*, CONGRESS.GOV (May 31, 2024), https://www.congress.gov/crs-product/LSB11161; *Senators*, UNITED STATES SENATE, https://www.senate.gov/senators/index.htm (last visited Aug. 8, 2025); *Representative Cathy McMorris Rodgers*, CONGRESS.GOV, https://www.congress.gov/member/cathy-rodgers/M001159 (last visited Aug. 8, 2025); Satwik Dutta & John H.L. Hansen, *Navigating the United States Legislative Landscape on Voice Privacy: Existing Laws, Proposed Bills, Protection for Children, and Synthetic Data for AI*, ARXIV 1, 1 (July 29, 2024), https://arxiv.org/abs/2407.19677.

[542] GDPR, *supra* note 8, art. 6(1)(a).

[543] 小型企業係指年營收低於 4000 萬美元且消費者人數低於二十萬人的機構。*See* Dutta & Hansen, *supra* note 541, at 1-2.

[544] U.S. CONST. amend. X.

[545] U.S. CONST. art. I, § 8, cl. 3.

[546] *See* Determann et al., *supra* note 540, at 15-16.

doi:10.6342/NTU202504586

許例外適用州法的設計仍然保留的法律適用上的複雜性。其次，CJEU 在過去判決中並未詳細審視美國國內資料保護水準，而 APRA 提供 CJEU 良好的比較基礎，若採取與 GDPR 相似的設計，CJEU 將可以輕易的識別 APRA 保護較 GDPR 低的部分，可能會導致 APRA 無法幫助美國獲得完整的適足性認定。儘管如此，在保持 DPF 存續的議題上，APRA 仍能提供正向的助益。

第三節 小結

本章梳理了美國法規與 CJEU 所設下的標準的差異與改善方向，以及聯邦資料隱私保護法律所能帶來的益處。首先是情報法規的改革，本文認為，主要待改進的部分為(1)將 EO 14086 之內容納入法典，包括合法蒐集目標、必要性與比例原則之要求，和 DPRC 的規範，以及(2)改善 DPRC 法官的獨立性問題，以及 DPRC 決定的透明度問題。

其次，聯邦資料隱私法規的立法也能為美國的資料隱私保護帶來助益，甚至有機會使美國獲得完整的適足性認定，APRA 的後續發展也應持續關注。

上述改革均能對歐美的合作帶來幫助，但是美國與徹底改革仍有一大段距離。自斯諾登事件至 DPF 獲得適足性認定的近十年間，美國已經進行了數次改革，但是在多數議題上均無法達到 CJEU 所立下之高標準，未來能否進行大規模改革仍有疑義，特別是關乎國家安全的情報機構法規。本文將於第伍章透過對現實層面的觀察來分析歐美之間合作的可能走向。

doi:10.6342/NTU202504586

第伍章 歐美合作前景分析——對美國與 CJEU 未來走向的建議

美國情報法規最大之改革——EO 14086 係於拜登執政時發布，而隨著 2024 年川普當選美國總統並執政後[547]，其政策及立場將會如何？以及是否得以緩和跨大西洋資料傳輸的衝突？值得進一步討論。

此外，針對 TikTok 所引發之國家安全擔憂，美國近期亦針對資料傳輸祭出限制。國內層面以行政命令 14117（下稱「EO 14117」）針對特定國家（Country of Concern）可能獲取美國人敏感個人資料所帶來之極端威脅進行限制，並特別關注 AI 技術所帶來之威脅，從而增加國家緊急狀態之範圍[548]；另外美國司法部發布 Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons 以限制美國人大量敏感個人資料以及政府相關資料之傳輸[549]；國際上美國亦放棄了在世界貿易組織（World Trade Organization，WTO）談判中支持資料無障礙流動和反對資料本地化之立場[550]。由此可見，美國自身對於資料傳輸之基本立場亦有轉變，而此是否代表其對與歐盟間的跨境資料傳輸議題的立場亦會有所改變？值得後續觀察。

---

[547] Maureen Chowdhury et al., *Congress Certifies Trump's 2024 Election Win*, CNN (Jan. 7, 2025), https://edition.cnn.com/politics/live-news/election-certification-trump-01-06-25.

[548] *See generally* Exec. Order No. 14,117, 89 Fed. Reg. 15421 (Feb. 28, 2024) [hereinafter EO 14117].

[549] 此規則為執行 EO 14117 的一項最終規則，禁止和限制與特定國家或個人進行特定資料交易。特定國家例如中國、俄羅斯、伊朗、北韓，以及古巴等國家；特定人士則是受特定國家管轄，或是主要在特定國家營運的人等，包括法人。Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636 (Jan. 8, 2025) (to be codified at 28 C.F.R. pt. 202).

[550] Wanxiu Xu et al., *Global Data Governance at a Turning Point? Rethinking China-U.S. Cross-Border Data Flow Regulatory Models*, 55(106061) COMPUT. L. & SEC. REV.: INT'L J. TECH. L. & PRAC. 1, 6 (2024).

doi:10.6342/NTU202504586

第一節 美國政府的立場

欲了解美國相關法規發展的前景，應先行分析美國當前的立場。在 EO 14086 的大幅度改革後，美國是否會再進一步改革？本節將分析川普對跨境資料傳輸與情報機構監控權力的立場。

第一項 情報機構監控權力

為了實現其政治目標，川普表示其願意利用行政部門的巨大權力對人民進行監控，包括 FISA 第 702 條以及 EO 12333 等法規之執行來干預人民之權力[551]。雖然文獻在此議題之討論上較為聚焦其在國內議題上可能對美國國內事務之權力濫用，但實際上可以顯現出其對於此等權力之重視，並且並未表現出有限縮執行之意象。川普在此議題的立場上可能並不會按照 CJEU 之期待，進行完整的改革。

第二項 川普政府的國內政策

基於 DPF 對於美國之商業利益，以及歐盟作為合作夥伴所帶來之利益，川普政府對於 DPF 架構曾表示採取支持態度，並希望得以與歐盟持續進行合作[552]，但是川普的作為並非朝此方向進行。首先是川普在 2025 年 2 月 18 日發布了行政命令 14215，提高了總統對獨立監管機構的控制權力[553]，此等行為可能會影響 FTC 根

[551] Ben Wizner et al., *Trump on Surveillance, Protest, & Free Speech*, ACLU 1, 1-2, https://www.aclumaine.org/sites/default/files/trump_memo_surveillance_protest_and_free_speech.pdf.

[552] Brian Hengesbaugh & Lukas Feiler, *How Could Trump Administration Actions Affect the EU-US Data Privacy Framework?*, IAPP (Feb. 26, 2025), https://iapp.org/news/a/how-could-trump-administration-actions-affect-the-eu-u-s-data-privacy-framework-.

[553] 此行政命令名為「Ensuring Accountability of All Agencies」。Exec. Order No. 14,215, 90 Fed. Reg.

doi:10.6342/NTU202504586

據 GDPR 第 45 條第 2 款 b 項保持充分獨立，以執行 DPF 原則之能力[554]，也展現了川普試圖提高其對行政機關控制力的意圖。

其次對於 PCLOB 之成員，川普首先了三名具有民主黨傾向之成員之職務。因為 PCLOB 成員任期限制，造成其解職有法律爭議，並引發了訴訟。直到 2025 年 8 月，加上先前之空缺，PCLOB 僅剩下一名成員，此對其行使職能造成限制[555]。EDPB 及歐盟執委會均曾經強調 PCLOB 的監督功能[556]，故此解職爭議可能對歐美雙方的合作帶來不利影響。

在面對 DPF 的議題上，川普政府可能會對其進行大幅修訂。例如美國傳統基金會[557]（The Heritage Foundation）即認為歐盟對於美國資料保護之檢視可謂虛偽地提高對美國的要求，並且僅針對美國，對於歐盟國家以及俄羅斯、中國等國家反而更加友善[558]。此種會為美國帶來不利競爭條件之針對性，可能違反川普總體採取之

10447 (Feb. 24, 2025).

554 Hengesbaugh & Feiler, *supra* note 552.

555 *Id.*; *D.C. Federal Court Rules Termination of Democrat PCLOB Members Is Unlawful*, HUNTON (May 22, 2025), https://www.hunton.com/privacy-and-information-security-law/d-c-federal-court-rules-termination-of-democrat-pclob-members-is-unlawful; BOARD MEMBERS, https://www.pclob.gov/Board/Index (last visited Aug. 21, 2025).

556 *See supra* text accompanying note 392, 393, 403, 495, 501, 503.

557 美國國傳統基金會（The Heritage Foundation）為美國一對於公共政策提出建議之組織，而川普政府在其任職中大量接受其政策建議，可見其對於美國政府之實際政策具有一定之影響力。ABOUT HERITAGE, https://www.heritage.org/about-heritage/mission (last visited June 17, 2025); *Trump Administration Embraces Heritage Foundation Policy Recommendations*, THE HERITAGE FOUND. (Jan. 23, 2018), https://www.heritage.org/impact/trump-administration-embraces-heritage-foundation-policy-recommendations?utm_source=chatgpt.com.

558 Ted Bromund, *The U.S. Must Draw a Line on the EU's Data-Protection Imperialism*, THE HERITAGE FOUND. (Jan. 9, 2018), https://www.heritage.org/government-regulation/report/the-us-must-draw-line-the-eus-data-protection-imperialism.

doi:10.6342/NTU202504586

「美國優先[559]」之基本立場，進而激化川普之態度而對雙方合作之前景帶來負面影響。

第三項 川普政府的對外政策

川普政府的對外政策也展現了其強硬的一面。在 EO 14117 中，美國首次建立對美國國家安全構成不可接受風險之標準，並建立了針對大量敏感個人資料以及政府相關資料向特定國家傳輸之限制機制[560]。然而，此等限制實際上並不一定象徵美國整體政策之完全轉變，更可能係為針對中國跨國企業或中國科技公司所帶來之技術和資源威脅[561]。

自 2025 年初川普政府之部分政策行動以觀，美國短期內可能正在動搖跨大西洋經濟與貿易關係之穩定性[562]。針對歐盟向來之隱私法規要求，以及潛在的數位市場法案（Digital Markets Act，DMA）所帶來之監管要求，川普政府近期曾採取報復性關稅威脅，但歐盟方面認為對於不公平競爭和濫用行為之抑制亦能使消費者和美國企業，特別是規模較小的美國機構獲利[563]。

---

559 *President Trump's America First Priorities*, THE WHITE HOUSE (Jan. 20, 2025), https://www.whitehouse.gov/briefings-statements/2025/01/president-trumps-america-first-priorities/.
560 Xu et al., *supra* note 550, at 6.
561 *Id.* at 9; Wanxiu Xu et al., *Whose Victory? A Perspective on Shifts in US-China Cross-Border Data Flow Rules in the AI Era*, THE PACIFIC REV. 1, 17-18 (Feb. 5, 2025), https://www.tandfonline.com/doi/full/10.1080/09512748.2025.2462239#abstract.
562 Divya Sridhar, *Trump Administration Playing Truth or Dare with EU-US Data Privacy Framework*, INFOSECURITY MAGAZINE (May 5, 2025), https://www.infosecurity-magazine.com/opinions/trump-eu-us-data-privacy-framework/?utm_source=chatgpt.com.
563 Will Oremus & Andrea Jiménez, *Trump's Push Against Foreign Tech Rules Could Backfire, Critics Say*, THE WASH. POST (Feb. 27, 2025), https://www.washingtonpost.com/politics/2025/02/27/trump-data-eu-tech-regulations/?utm_source=chatgpt.com.

doi:10.6342/NTU202504586

此外，隨著人工智慧的發展，除了帶來地緣政治和商業權力競爭之挑戰外，傳統的國家安全問題以及資料隱私保護之問題亦有進一步加劇的風險[564]。EO 14117 亦表明，特定國家可能可以直接、無節制的取得美國人的大量個人資料，以進行勒索或間諜活動等行為，此會對美國國家安全帶來重大風險，而人工智慧之發展可能會對資料的濫用帶來更加劇烈之風險[565]。可見在人工智慧高速發展之時代，美國正在重新思考是否因特定之風險以及政策目標，故放棄資料應得自由傳輸之立場，而此立場與歐盟對於美國情報機構監控風險所採取之針對性措施又是否有異曲同工之妙？

第四項 小結

川普政府雖然展現與希望歐盟合作的態度，但是其國內之施政方針係提高其對於國內行政機關之掌控，以及弱化其它的監督功能，同時川普也相當重視情報機構的功能。以此立場以觀，川普並未採取措施以維持 DPF 的穩定，無法期待其完全接受 CJEU 標準並進一步作出完整的改革。

在對外政策上，川普也因為特定之國家安全威脅，而提高了對跨境資料傳輸限制，在此方面川普展現出了與歐盟類似的限制邏輯，顯現出雙方在限制資料出口的議題上有一定的共識。同時，在面對歐盟立下更多具限制性的法規時，川普也展現了強硬的態度，試圖維繫原有之貿易利益。

---

564 Xu et al., *supra* note 561, at 5.
565 EO 14117, *supra* note 548, sec. 1.

doi:10.6342/NTU202504586

本文認為，雖然川普展現出強硬的態度，也難以期待其進行完整的改革，惟為尋求雙方可能持續合作的前景，本文將透過與其他國家進行比較，以分析美國情報法規與其它國家相比較為不足的部分，並給予修法建議，以期雙方在尋求更進一步穩固合作時能有方向。

第二節 美國可能的調整方向——以英國情報法規為比較對象

受到情報監控行動過於寬泛的指責並非美國獨有，而其中一即為英國。此外，英國在 2021 年正式退出歐盟[566]之後，開始需要適用 GDPR 第五章的例外規定，始得將資料自歐盟傳輸至英國境內，隨後英國也獲得了適足性認定[567]，並且同時額外獲得了執法層面的適足性認定[568]，顯現出英國與歐盟之間的緊密合作關係。英國在脫歐之後之背景與美國相當類似，同樣曾經受到情報機構監控權力過廣的指控、同樣透過適足性認定與歐盟進行跨境資料傳輸，也同樣有改革情報法規。本章將透過比較美國與英國的情報法規在前述的關鍵議題上有何異同，以分析美國與其它使

[566] Council Decision (EU) 2020/135 of 30 January 2020 on the Conclusion of the Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (Text with EEA Relevance), 2020 O.J. (L 29) 1; Council Decision (EU) 2020/2252 of 29 December 2020 on the Signing, on Behalf of the Union, and on Provisional Application of the Trade and Cooperation Agreement Between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part, and of the Agreement Between the European Union and the United Kingdom of Great Britain and Northern Ireland Concerning Security Procedures for Exchanging and Protecting Classified Information, 2020 O.J. (L 444) 2.

[567] Commission Implementing Regulation (EU) 2021/1772 of 28 June 2021 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by the United Kingdom (Notified Under Document C(2021)4800) (Text with EEA Relevance), 2021 O.J. (L 360) 1.

[568] Commission Implementing Decision (EU) 2021/1773 of 28 June 2021 Pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the Adequate Protection of Personal Data by the United Kingdom (Notified Under Document C(2021) 4801), 2021 O.J. (L 360) 69.

doi:10.6342/NTU202504586

用適足性認定之國家在情報法規上之差異，進而分析美國是否需要調整其情報法規。

第一項 英國情報法規

英國主要監控授權立法為調查權力法案（Investigatory Powers Act 2016，下稱「IPA」）[569]。IPA 被視為對於過往情報監控體系的改善，為監控行動立下法律基礎、提高透明度、以及降低不同監控法律體系間的落差[570]。

第一款 監控授權

IPA 有稱為「雙重鎖定（Double Lock）」的保護機制，需要由英國內閣大臣[571]（Secretary of State）簽發令狀[572]（Warrant），並由司法專員（Judicial Commissioner）批准[573]。

IPA 針對通訊內容、設備資料以及大量原始資料的「取得（Acquisition）」、「保留（Retention）」與「查閱（Examination）」均有雙重鎖定的授權要求，並且兩階段均有必要性以及比例原則之審查[574]。此外，在有緊急情況時，內閣大臣亦可不經由司法專員批准而簽發令狀，惟須由司法專員事後審查，並得以使令狀無效並採取補

---

[569] Investigatory Powers Act 2016, c. 25 (UK) [hereinafter IPA].

[570] Lorna Woods, *The Investigatory Powers Act 2016*, 2017(1) EUR. DATA PROT. L. REV. 103, 103 (2017).

[571] 蘇格蘭之令狀由蘇格蘭部長（Scottish Minister）負責。本文為求精簡，以下以蘇格蘭以外地區之規定為主；IPA, *supra* note 569, §§ 21-22.

[572] 除了普通令狀外，亦有針對受保護資料、健康紀錄、或是大量敏感個人資料的特殊令狀（Class BPD Warrant）。*Id.* §§ 204-09.

[573] *Id.* § 23.

[574] *See, e.g.*, *id.* §§ 15-23, 102-04, 136-40, 204-05, 208.

doi:10.6342/NTU202504586

救措施[575]。

IPA 授權針對性以及大規模攔截[576]。IPA 的針對性攔截規定在第二部分[577]。IPA 授權針對郵政服務或電信系統傳輸的資料進行攔截[578]。針對性令狀可以針對特定個人、組織或是單一處所簽發[579]。此外亦有針對性審查令狀（Targeted Examination Warrant）以及互助令狀（Mutual Assistance Warrant）[580]。

IPA 的第五部分授權針對性的對設備進行攔截行動[581]。針對性設備攔截令狀授權對收件人的設備進行攔截，並取得(1)通訊資料、(2)設備資料[582]、以及(3)任何其它資訊[583]。

除了針對性攔截外，IPA 亦有大規模攔截的規定，主要針對攔截海外通訊[584]。IPA 的第六部分第一章主要規範針對海外資料的大規模攔截行動[585]，攔截的客體包括通訊內容以及次級資料（Secondary Data）[586]。第二章則是規定授權大規模取得

---

575 *See, e.g.*, *id.* §§ 24-25, 109-10.

576 Cian C. Murphy, *State Surveillance & Social Democracy: Lessons after the Investigatory Powers Act 2016*, *in* THE CONSTITUTION OF SOCIAL DEMOCRACY 413, 420 (Alan Bogg et al. eds., 2020); Tristan Goodman, *The Investigatory Powers Act 2016: A Victory for Democracy and the Rule of Law?*, 2018(5) THE BRISTOL L. REV. 2, 5 (2018); 在 IPA 中所使用之用語為攔截（Interception），定義為「對電信系統執行特定行為，使通信的內容於特定時間內被並非寄送者或預定的接收者的人取得」。*Id.* § 4; *see, e.g.*, *id.* § 15(1)(a).

577 IPA, *supra* note 569, §§ 15-36.

578 *Id.* §§ 43-48.

579 *Id.* § 17.

580 針對性審查令狀係指對於通訊內容進行審查之令狀；互助令狀係指根據國際互助協定，(1)要求外國提供資料蒐集的協助、(2)提供外國協助、或是(3)提供資料給發行令狀之人或其代表人之令狀。*Id.* § 15.

581 *Id.* §§ 99-135.

582 設備資料包括系統資料、附著於通訊內容之資料等。*Id.* § 100.

583 *Id.* § 99(2).

584 Goodman, *supra* note 576, at 5.

585 IPA, *supra* note 569, §§ 136-57.

586 次級資料係指系統資料，包括構成、包含於、附加於或邏輯上與通訊內容相關之資料。*Id.* §§ 136-37.

doi:10.6342/NTU202504586

資料[587]，得以要求電信營運商(1)揭露其持有之任何通訊資料、(2)其有能力取得之資料、以及(3)揭露其有能力取得之資料[588]。第三章則是授權大規模攔截設備，其中設備的定義與針對性設備攔截相同[589]。

IPA 的第七部分則是授權「保留」與「查閱」大量個人資料集[590]（Bulk Personal Datasets），而資料的「取得」則是由各情報機構自行取得，其法源基礎主要為情報系統法（Intelligence Services Act 1994）之令狀規定[591]。情報系統法僅要求在侵入私人財產或無線電時，原則上需要內閣大臣或是一位蘇格蘭部長（Scottish Minister）簽發之令狀[592]。

雖然有雙重鎖定的要求，但是傳統上在 IPA 下，司法專員僅審查決策程序的合法性，而不針對實質內容進行審查，故有批評者認為此司法審查形同虛設[593]，司法專員僅係將內閣大臣的決定進行「橡皮圖章式」的背書[594]。惟在受 CJEU 以及歐洲人權法院的判例法影響下，司法專員對比例原則已有更深入的審查，所以在此方面已有些許改善[595]

---

[587] *Id.* §§ 158-75.
[588] *Id.* § 158(6)
[589] *Id.* §§ 176-77.
[590] 其中分為類型化大量個人資料令狀（Class BPD Warrant）以及特定個人資料令狀（Specific BPD Warrants）。此外，第七部分的「個人資料（Personal Data）」之定義與 GDPR 相同。*Id.* § 199-200, 204-05; Data Protection Act 2018, c. 12, § 3(2) (UK); GDPR, *supra* note 8, art. 4(2).
[591] David Anderson, *Independent Review of the Investigatory Powers Act 2016*, SSRN, ¶ 3.15 (June 14, 2024), https://ssrn.com/abstract=4833577.
[592] Intelligence Services Act 1994, c. 13, §§ 5-6 (UK).
[593] IPA, *supra* note 569, §§ 23(1)-(2); *Judicial Review*, CTS. & TRIBUNALS JUDICIARY, https://www.judiciary.uk/how-the-law-works/judicial-review/ (last visited July 22, 2025); Mariette Jones, *Double-Lock or Double-Bind? The Investigatory Powers Bill and Freedom of Expression in the United Kingdom*, *in* CYBERSURVEILLANCE IN A POST-SNOWDEN WORLD: BALANCING THE FIGHT AGAINST TERRORISM AGAINST FUNDAMENTAL RIGHTS 3, 11 (Russel R. Weaver et al. eds., 2017).
[594] Woods, *supra* note 570, at 103-04.
[595] *Id.* at 104.

doi:10.6342/NTU202504586

此外，雖然司法專員有審查令狀之權力，但其行為不得違反(a)國家安全、(b)預防或偵查嚴重犯罪、以及(c)英國的經濟利益[596]，此限制可能會影響司法專員的有效性[597]，尤其是因為情報行動時常與國家安全有所聯繫。

第二款 監控行動的監督與救濟

IPA 授權監控體系由調查權力專員（Investigatory Powers Commissioner）負責審查政府機構行使監控職權之情形，並得以提出建議。同時，其應每年就司法專員行使職能之情形向首相提出報告[598]。調查權力專員有責任向調查權力法庭（Investigatory Powers Tribunal）提出訴訟，針對出現「重大錯誤」並且「對相關人士造成重大損害或不利」的錯誤行為進行監督[599]。

監控行動的授權由司法專員批准。司法專員由首相諮詢高階法官後任命，其必須為現任或前任的高階法官，並且有三年任期保障，除有失能或行為不當以外，不得被隨意撤換[600]。司法專員執行業務之情況由調查權力專員向首相以及議會報告[601]，但是沒有需要向首相及議會負責之規定，故具備一定之獨立性。

調查權力法庭（Investigatory Powers Tribunal）為獨立之司法機關，實質相當於法院[602]。調查權力法庭為保護敏感資訊，不得向申訴者揭露可能危及國家安全、預

---

596 IPA, *supra* note 569, § 229(6).
597 Woods, *supra* note 570, at 104.
598 調查權力專員同時具備司法專員身分，兩者均由英國首相任命，並且需要高等司法人員推薦。IPA, *supra* note 569, §§ 227-32, 234.
599 *Id.* § 231.
600 *Id.* §§ 23, 227(1)-(2).
601 *Id.* § 234.
602 朱富美（2023），〈由英國「調查權力法庭」運作論科技偵查法之人權保障機制〉，《監察院月刊》，

doi:10.6342/NTU202504586

防和偵查犯罪、影響英國經濟利益、或是履行情報部門職能之相關資訊，僅得提供事實以及決定之摘要資訊[603]。有觀點認為此監督的行使門檻過高，並且英國政府認為通知受監控人士其受監控的事實並非必要，惟 CJEU 認為知情對於個人行使權利至關重要[604]。

IPA 引入了對於調查權力法庭判決的上訴機制，可以向英格蘭及威爾斯上訴法院（Court of Appeal）或是蘇格蘭高等民事法院（Court of Session）（以下統稱「上訴法院」）提出上訴，惟僅有在(1)上訴涉及重要原則或實務議題，或是(2)存在其他有力理由允許上訴時，始得進行上訴，並且需要得到調查權力法庭或是上訴法院的核准，此高門檻可能會使原告無法獲得救濟[605]。

第三款 美國法與英國法之比較以及可優先調整事項

英國情報體系在制度層面與美國有明顯的差異。首先是 IPA 授權的攔截行動均需要司法專員的批准，其具備之法官資格以及獨立性保障，並且個別授權特定攔截行動，相較於 FISC 較為粗略的授權監控計劃，可以更有效的進行監督。惟司法專員與 DPRC 法官的獨立性相當類似，其制度設計上均非法院，僅係司法專員之資格以前任或現任高階法官為限。此外，司法專員的任期保障為三年，較 DPRC 之四年短，卻被認為具備獨立性，故應可反映出，DPRC 法官具備相當高之獨立性。

29 期，頁 26。

603 朱富美，前揭註 602，頁 27; IPA, *supra* note 569, § 231.

604 Woods, *supra* note 570, at 104.

605 *Id.* at 105; IPA, *supra* note 569, § 242.

doi:10.6342/NTU202504586

IPA 發出令狀之目的也較 EO 14086 的規範寬鬆。EO 14086 聚焦在國家安全領域，並且 FISC 授權的監控目標亦是，但是 IPA 卻將英國的經濟利益也納入得發出令狀之目的，為更加寬泛之授權。此外，IPA 在授權監控行動的理由中，國家安全本身即為授權情報行動之理由，相較之下 EO 14086 列舉國家安全事由的規範方式更加嚴格。IPA 亦將英國的經濟利益作為授權監控行動的理由，可見在授權上 IPA 較美國更加寬鬆。

其次調查權力法庭的事後監督。在制度上調查權力法庭為真正之法院，並且其決定可以上訴至上訴法院，與 DPRC 有明顯之差異。雖然起訴與上訴均有較高的門檻，但是其以法律設立，並且為司法機構之本質亦可以帶來較有效之救濟。此外，相較於 DPRC 僅告知申訴人結論之設計不同，調查權力法庭提供事實與決定的摘要，在情報機構之機密性以及人民的知情權上取得了平衡。調查權力法庭與 DPRC 之制度設計各有優劣，何者能提供更有效的救濟仍有待 DPRC 實際運作後始能得知。

綜上，英國與美國的情報體系差異主要體現在監督與授權的立法架構，在事前授權及事後監督的組織及功能均有差異。英國的雙鎖授權機制為保護水準較高的事前獨立授權，惟其在取得大量個人資料集時卻不一體適用。此外，監督與授權機制雖然有法院得以提供救濟，惟其較高的起訴與上訴門檻亦降低了保護水準。本文認為，英國與美國的制度設計在保護水準上各有優劣，而其保護水準較高者為美國情報法規可以借鑑者。基此本文認為，美國應考慮者為對 FISC 進行改革，其中主

doi:10.6342/NTU202504586

要有兩個層面。

第一個層面是使 FISC 授權個別監控計劃。首先，歐洲人權法院認為大規模蒐集的事前監督及事後審查同等重要[606]，英國亦有司法專員進行事前監督，以及調查權力法院進行事後審查。目前美國已有 DPRC 進行事後審查，故完善事前監督為更迫切的改革。其次，FISC 原本即為審查監控計劃的法院，也有 FISCR 負責上訴案件，其編制人數與英國的司法專員人數相距不遠，故應能以較小的成本將其改制為授權個別監控計劃的法院[607]。

第二個層面是納入必要性與比例原則的審查。FISC 原本僅有合目的性審查，而不論是 CJEU 的標準或是 IPA 的規範均有必要性與比例原則的要求。在發布 EO 14086 後，美國已經開始接受必要性與比例原則的用語，美國國內也有類似概念的實踐，EDPB 也認為美國法的解釋能提供足夠之保護，故應能直接將之納入 FISA 第 702 條內。

本節所提出對FISC進行的改革並不一定會大幅限縮美國情報機構的情報功能，但是其所提供的程序保障可以彰顯美國與歐盟合作的誠意以及決心，也解決了部分 CJEU 對制度保障不足的擔憂。

FISC 的授權模式問題自 Schrems I 案時期即存在，惟在美國持續進行的改革

606 *See supra* text accompanying note 379.

607 截至 2025 年 8 月為止，英國司法專員的人數為 15 人；FISC 法官的人數為 11 人。*Current Membership - Foreign Intelligence Surveillance Court*, U.S. FOREIGN INTEL. SURVEILLANCE CT., https://www.fisc.uscourts.gov/current-membership-foreign-intelligence-surveillance-court (last visited Aug. 12, 2025); *Judicial Commissioners*, IPCO, https://www.ipco.org.uk/who-we-are/judicial-commissioners/ (last visited Aug. 12, 2025); *Investigatory Powers Commissioner*, IPCO, https://www.ipco. org.uk/who-we-are/investigatory-powers-commissioner/ (last visited Aug. 12, 2025).

doi:10.6342/NTU202504586

中均無對 FISC 的審查密度進行修正，在川普更加強硬的作風下，進行改革的可能性進一步降低。本文認為，英國與美國的情報法規各有優劣，但是英國與美國所受到之壓力卻截然不同，故應進一步討論 CJEU 在面對潛在的法律程序中應如何應對，以及重新思考 CJEU 對情報法規的要求是否合理。

第三節 歐美資料跨境資料傳輸議題評析——以情報法規為中心

CJEU 在 Schrems I 與 Schrems II 案中對歐盟資料隱私保護的基本權審查向來採取非常嚴格的審查標準，相較於其他基本權利，CJEU 似乎更加重視資料隱私的保護[608]。在此背景下，情報法規的資料隱私保護水準即難易達到 CJEU 的標準，而此衝突不僅存在與美國的跨境資料傳輸議題上。

CJEU 在歐盟內案件中曾經表示，國家基於國家安全名義要求電子通訊服務者代為蒐集、保留及傳輸資料的行為無法適用歐洲聯盟條約第 4 條第 2 款的國家安全例外，應適用與美國相同的資料保護限制[609]。此解釋方式引發了多數成員國強烈的不滿，認為其會對國家主權的核心職能造成威脅。

為了對抗此司法解釋造成的限制，法國及其盟友試圖藉由電子隱私規則（ePrivacy Regulation）的改革以繞過 CJEU 有關資料蒐集與保留的判例法，最終

608 薛景文（2021），〈從 *Schrems I & II* 論美歐隱私權保障落差對自由貿易規範之影響〉，《第 21 屆國際經貿法學發展學術研討會論文集》，頁 501。

609 Theodore Christakis, *How Europe's Intelligence Services Aim to Avoid the EU's Highest Court—and What It Means for the United States*, LAWFARE (Mar. 8, 2021), https://www.lawfaremedia.org/article/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states?utm_source=chatgpt.com.

doi:10.6342/NTU202504586

可能導致 Schrems II 案與其它先行裁決或判決所建立的司法監督機制被立法層面的國家安全豁免架空[610]。雖然最終電子隱私規則因為缺乏共識以及條文過時而未能通過[611]，但是也顯示出歐盟成員國亦難以完全接受 CJEU 的高標準。

在歐美跨境資料傳輸議題上，CJEU 向來是最大的阻礙者。在美國以及歐盟執委會下持續的努力合作下，因為 Schrems 持續不斷提出訴訟壓力，使雙方的合作終究需要通過 CJEU 的司法審查。CJEU 之高標準難以被美國完全接受，而雙方在數位貿易上的合作又至關重要。本節將探討 CJEU 之高標準是否合理且公平，以及其應調整其標準之理由。

第一項 歐盟的情報行動

歐盟的情報機構體系實際上也無法達到 CJEU 的要求。斯諾登事件曝光時，不僅揭露了美國的監控計劃，事實上亦涉及針對英國和德國之指控[612]，顯示出歐盟本身之情報體系亦有缺陷。英國在斯諾登事件後進行的立法，本質上係將監控行為進行透明化，但其被認為並沒有實質變更監控作法，甚至加強了國家的權力，包括大規模蒐集[613]。

---

610 *Id.*

611 *The ePrivacy Directive and the Evolution of Data Privacy in the EU: What You Need to Know*, COOKIEBOT (Apr. 17, 2025), https://www.cookiebot.com/en/eprivacy-regulation/#:~:text=Ultimately%2C%20the%20European%20Commission%20officially,minors%20(Article%2028)"..

612 Lora Anne Viola, *The Limits of Transparency as a Tool for Regulating Surveillance: A Comparative Study of the United States, United Kingdom, and Germany*, *in* TRUST AND TRANSPARENCY IN AN AGE OF SURVEUILLANCE 21, 29-30 (Lora Anne Viola & Pawel Laidler eds., 2021)

613 *Id.* at 33-36.

doi:10.6342/NTU202504586

德國方面則是被指控其聯邦情報局（Bundesnachrichtendienst，下稱「BND」）與 NSA 合作實行監控行動，且 BND 之監控行動亦缺乏法律基礎。2016 年德國通過了改革 BND 之法規，但亦被認為僅是將原先非法之監控活動合法化，甚至擴展和保護 BND 之行動。2022 年的聯邦情報局法（Gesetz über den Bundesnachrichtendienst）則為蒐集海外通訊提供更強的法律基礎，並引入新的控制機制，總體而言係使蒐集海外資訊合法化，並使 BND 的監控權力更加精確[614]。

除了 BND 以外，德國聯邦國防軍（Bundeswehr，下稱「德國國防軍」）亦會進行秘密監控行動，但卻缺乏獨立有效的監督。唯一有權實質審查德國國防軍情報行動者為德國資料保護與資訊自由聯邦委員會（Bundesbeauftragter für den Datenschutz und die Informationsfreiheit，BfDI），其可以指出德國國防軍的權力濫用行為以及行為缺失，但是並無權要求採取補正行動。此監管空缺也可能被 BND 等其它情報機構濫用，透過與德國國防軍的合作以迴避自身受到的法律限制[615]。

在斯諾登事件後，美國的情報體系因為資料傳輸框架的爭議兩次被 CJEU 所審查，在此期間進行了大幅度的改革，特別是透過 EO 14086 對情報行動的限制。但如同 Schrems I、Schrems II 案中 CJEU 所為之分析，以及目前 DPF 與 EO 14086 所受到之檢視，美國之情報機構監控權力仍難以符合 CJEU 所定下之標準。而英國

614 *Id.* at 36-39.
615 Corbinian Ruckerbauer et al., *Legal and Oversight Gaps in Germany's Military Intelligence*, ABOUT:INTEL (June 26, 2024), https://aboutintel.eu/germanys-military-intelligence/?utm_source=chatgpt.com.

doi:10.6342/NTU202504586

與德國同樣受到指控，但改革的程度又更顯不足，卻並未受到類似美國，可能會因為適足性認定無效而造成經濟損失的壓力。

基於 CJEU 針對美國情報體系行為審查所採取之高標準，實際上高過歐盟內部之情報體系受到的譴責，故在 Schrems II 案過後，論者針對 Schrems 背後可能存在之動機以及潛在之支持勢力提出了質疑[616]。歐盟在資料保護議題上對美國的立場被認為可能是保護主義的體現，是針對美國在科技產業發展的嫉妒心理，以美國的角度觀察更是如此[617]。另外即使動機純粹是為保護個人的資料隱私權利，亦有觀點認為獲取個人資料也促成了歐盟產業的成功，而目前的狀況過度重視保護基本權利[618]。

不論歐盟係基於欲保護自身之科技與資訊產業、或是欲針對美國之情報體系並給予差別待遇，又或是兩者均是，對於歐盟過分針對美國之質疑以及帶來之爭議始終會存在。歐盟內部的意見也並不統一，對於與美國的合作，CJEU 是主要的反對方，縱觀英國與德國的情報體系，其所設想的資料保護水準是否不切實際？美國的情報體系又是否對資料隱私的侵害過於嚴重？值得進一步思考。

第二項 白皮書——資料隱私侵害是否如此嚴重？

情報機構對資料隱私的侵害確實存在，並且不易被發覺。惟在 Schrems I 及

616 Marc Rotenberg, Schrems II*, from Snowden to China: Toward a New Alignment on Transatlantic Data Protection*, 26 (2) EUR. L.J. 141, 149 (2020).
617 Ruben de Bruin, *A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence*, 13(2) HASTINGS SCI. & TECH. L.J. 127, 143 (2022).
618 *Id.* at 153-54.

doi:10.6342/NTU202504586

Schrems II 案中，CJEU 並未對現實情況細緻分析，而是自規範層面下手，論述其程序保障之不足以及授權監控範圍過於廣泛。

美國在 Schrems II 案後為利於各界了解美國針對歐美跨境資料傳輸之合法基礎所採行之保障措施以及相關資訊，由其商務部、美國司法部以及情報總監辦公室在 2020 年 9 月共同發表了 Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after *Schrems II* 白皮書（下稱「白皮書」）[619]。在其中得以觀察資料隱私保護在現實層面所面對之風險。

首先，美國方面表示多數美國公司之資料並不引起情報機構之興趣，並且 EO 12333 亦不包括強制私營公司揭露資料之規範，FISA 第 702 條亦有事前之司法審查，且大多數公司也從未收到根據 FISA 第 702 條揭露資料之命令[620]。

其次，美國政府與歐盟成員國之間長期存在分享情報機構所獲得資料之安排，以應對各種威脅，對歐盟重要之公共利益有所貢獻，若中斷 FISA 第 702 條之蒐集，將對歐盟公共利益造成嚴重的不利影響[621]。

再者，白皮書強調 FISC 在審查監控計劃時並非如同 CJEU 在 Schrems II 案中認為僅是程序性的，而是有實質之認證，實際上，美國政府更強調適當性而非必要性以及比例原則。另外白皮書也指出實際上此種監控行為是有救濟機制的，並且有

---

[619] 郭戎晉(2021)，〈論個人資料跨境傳輸與數位經貿之互動與規範設計──以歐盟法院 Schrems 案影響為觀察對象〉，《2021 數位貿易政策論壇－科技．人文．數位貿易》，頁 235。

[620] U.S. Dep't of Com. et al., Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers After *Schrems II* 2-3 (2020) [hereinafter White Paper], https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF.

[621] *Id.* at 3-5.

doi:10.6342/NTU202504586

在美國法院中成功得到救濟之案例[622]。

白皮書亦表示，歐盟成員國亦會進行針對性蒐集以及大規模蒐集，並且也有缺乏實質性規範者，故美國政府認為傳輸到美國之資料在情報監控相關的隱私保護方面已享有較在歐盟內持有之資料相當或更高之保護[623]。另外，在海外傳輸資料實際上均有機會被各國之情報機構獲取，而 CJEU 卻未考慮此細節，Schrems II 案亦未考慮多項相關之保障措施，例如國家情報優先框架、情報機構內部程序以及監察長之調查和執法行動等[624]。

總體而言，白皮書說明了諸多原因以表達美國情報監控體系並不如 CJEU 所認為者般對歐盟人民之資料隱私造成重大侵害，並認為資料傳輸至美國所受到之保護水準並不比在歐盟境內不足，以及認為實際上歐盟資料透過商業傳輸至美國並不會受到更多之侵害。

與本文前述之觀點相似，白皮書亦認為歐盟的情報體系與美國相比，並未提供更好的隱私保護。在歐盟內部，以及與歐盟有良好合作關係的英國均未能達到 CJEU 的標準的情況下，對美國採取極高的標準似乎不切實際，也並不公平。此外，白皮書亦表示，實際上多數商業資料並未受到美國情報機構的侵害。本文認為，CJEU 應重新思考對情報法規的要求，以及情報行動對個人資料隱私實際上的侵害程度。

---

622 *Id.* at 6-12.
623 *Id.* at 15-16.
624 *Id.* at 16-22.

doi:10.6342/NTU202504586

第三項 CJEU 之高標準之合理性？

雖然川普政府之態度顯示出其應不會再次為了 DPF 的存續而改革美國的情報法規，也未顯示出配合的態度，惟本文認為，美國過去的一系列改革已經釋出足夠誠意。CJEU 也或許也應接受情報體系本質上即難以完全符合其高要求，尤其是法律體系與歐盟迥異的美國。CJEU 亦應考量歐盟的政治與經濟需求。在歐盟個人在個人資料保護立法規範嚴峻下，可能迫使機構將個人資料處理活動完全移出歐盟領域，導致歐盟在科技創新領域上被排除於全球市場之外[625]。

此外，即便歐盟成員國亦受到 CJEU 高標準之限制，其影響亦限於國內情報法規之運作，或是需要進行立法上的調整。而對與美國而言，CJEU 對其情報法規之不滿將反映於跨境資料傳輸的受阻上，不僅影響美國公司，亦可能對歐盟本身的數位經濟發展造成負面影響。本文認為，CJEU 堅持其高標準造成之影響過於巨大，在情報法規衝突的存在期間，雙方的經濟活動所受之衝擊可能不合比例。此外，GDPR 與適足性認定應係屬於商業傳輸的範疇，將情報法規作為雙方合作的主要阻礙點之一，似有不妥。

在歐盟成員國與美國均難以接受 CJEU 對資料隱私權利的保護水準的背景下，CJEU 是否應持續堅持其高標準，並在潛在的 Schrems III 案中再次使 DPF 的適足性認定失效，值得再次思考。

---

[625] 郭戎晉，前揭註 619，頁 242-43。

doi:10.6342/NTU202504586

第四節 小結

本章總結了歐美跨境資料傳輸的主要問題，並透過分析與美國情況類似的英國的情報法規，以進行對比，並瞭解美國與英國情報授權體系孰優孰劣，以及指出美國法的主要缺陷。FISC 的授權範圍為美國法與歐盟標準之間最大的差異，惟在歐美多年的衝突下，美國透過 PPD 28 以及 EO 14086 進行的改革中均未有相關的規範，可能代表美國更傾向將個別化情報目標的權限交予情報機構本身，並無妥協的意願。在川普欲提高對行政機關的掌控力，以及相當重視情報體系的功能的背景下，本文認為美國對 FISC 進行改革的可能性仍然不高。

CJEU 在資料隱私保護權利的高標準不僅為歐美跨境資料傳輸帶來阻礙，在歐盟成員國間亦有反對的意見，並曾付諸行動。在美國的情報法規的基本權利保護水準並不明顯低於英國與德國的情況下，CJEU 在潛在針對 DPF 適足性認定的法律程序中，是否應持續堅持其高標準，值得重新思考。除了情報法規本質上可能難以符合 CJEU 的要求以外，本文認為，DPF 喪失適足性認定帶來的政治與經濟影響也應納入考量。

doi:10.6342/NTU202504586

第陸章 結論

在這個資訊科技快速發展的時代，資料作為科技的基礎，特別是在近期高速發展之人工智慧領域的重要性將此議題帶至新的高度。歐美跨境資料傳輸議題產生的爭議，係始於美國情報體系過於廣泛之權力，以及美國與歐盟對資料隱私之定位之本質上之差異，導致安全港協議在斯諾登事件爆發後被放大檢視，並開啟日後一系列之訴訟，以及美國對於情報機構監控體系之改革。

本文先行闡述美國情報法規以及歐盟資料保護法規，並介紹兩者的歷史以及問題。在 Schrems I 案之前，美國情報法規受到其監控過廣的批評；歐盟的資料保護法規在立法以及轉換的過程中也遭遇困難。在斯諾登事件爆發後，一方監控過於廣泛、一方規範嚴格的衝突浮上檯面，並開啟了一系列的訴訟以及改革。

CJEU 在 Schrems II 案中立下了嚴格且詳細的標準，主要針對美國的情報法規，美國也透過 EO 14086 以及 DPF 進行回應。回顧美國歷來的改革，本文認為，美國已經付出相當的誠意，進行了大規模的改革，並且仍在進行中。惟在經過一系列的改革，並再次透過 DPF 與歐盟進行合作後，多數論者仍認為美國的整體保護水準並不足以達到 CJEU 的高標準。

本文隨後分析了美國欲達成 CJEU 標準所欠缺的改革，以及美國現行的政策，認為美國所需的改革幅度過大，川普政府應不會完全接受 CJEU 的標準。惟本文仍認為，為保持雙方的經濟與政治合作關係，維持 DPF 的存續有至關重要的影響。透過分析英國在斯諾登事件後的立法——IPA，本文認為，美國在情報法規下的權

doi:10.6342/NTU202504586

利保護議題上已經做出了大量讓步，也並未明顯落後於其他歐洲國家，雖然其仍有改革的空間，但是 CJEU 是否應據此再次武斷的使 DPF 失去適足性認定，仍有思考的空間。

最後，本文認為，歐美跨境資料傳輸議題的衝突已綿延逾十年，應有其難以完全解決之難處。美國在過程中釋出誠意進行讓步，但仍不願完全接受 CJEU 標準；而 CJEU 則是在過程中立下了其高標準，雙方無法完全達成共識，未來也可能持續如此。在此背景下，僅能持續觀察未來潛在的訴訟，以期歐美雙方能持續尋找出解決的方式。

doi:10.6342/NTU202504586

參考文獻

中文文獻

期刊

朱富美（2023），〈由英國「調查權力法庭」運作論科技偵查法之人權保障機制〉，《監察院月刊》，29 期，頁 26-27。

張志偉（2018），〈歐盟資料保護基本規則導論〉，《月旦司律評》，創刊號，頁 164-172。

廖淑君（2020），〈論我國因應 GDPR 施行之措施－以個人資料之跨境傳輸為核心議題〉，《商業法律與財金期刊》，3 卷 1 期，頁 115-140。

劉靜怡（2019），〈淺談 GDPR 的國際衝擊及其可能因應之道〉，《月旦法學雜誌》，286 期，頁 5-31。

戴豪君、林其樺 (2018)，〈政府與產業因應 GDPR 之調適措施〉，《台灣經濟論衡》，16 卷 3 期，頁 15-29。

簡毓寧、張馨云、王世明（2019），〈我國面對歐盟 GDPR 個資保護浪潮之因應與挑戰：日本經驗之借鏡〉，《經濟前瞻》，186 期，頁 53-56。

其它

郭戎晉（2021），〈論個人資料跨境傳輸與數位經貿之互動與規範設計──以歐盟法院 Schrems 案影響為觀察對象〉，《2021 數位貿易政策論壇－科技．人文．數

doi:10.6342/NTU202504586

位貿易》，頁 205-251。

薛景文(2021)，〈從 *Schrems I & II* 論美歐隱私權保障落差對自由貿易規範之影響〉，《第 21 屆國際經貿法學發展學術研討會論文集》，頁 487-541。

doi:10.6342/NTU202504586

英文文獻

期刊

Chen, Tsai-fang (2023), *Non-Discrimination Under the Most-Favoured-Nation Obligation and Adequacy Decisions in the General Data Protection Regulation*, ASIAN JOURNAL OF WTO & INTERNATIONAL HEALTH LAW & POLICY 309.

Connolly, Matthew (2024), *Will the EU-US Data Privacy Framework Survive Schrems III?*, 27 TRINITY COLLEGE LAW REVIEW 87.

Croner, George W. (2023), *FISA Section 702's Challenging Passage to Reauthorization in 2023*, 14 JOURNAL OF NATIONAL SECURITY LAW & POLICY 55.

de Bruin, Ruben (2022), *A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence*, 13(2) HASTINGS SCIENCE & TECHNOLOGY LAW JOURNAL 127.

Determann, Lothar et al. (2024), *American Privacy Rights Act - A First Glance at the US Congress's Newest Comprehensive Privacy Bill*, 6(4) JOURNAL OF DATA PROTECTION AND PRIVACY 1.

Dimović, Zoran (2024), *Analysing the EU Data Privacy Implications Resulting from Executive Order 14086: A Legal Perspective*, 16(1) LEXONOMICA 85.

Gemar, Stephen (2020), *A Crucial Aspect of National Security in Need of Reform: Section 702 of the FISA Amendments Act*, 65 SOUTH DAKOTA LAW REVIEW 489.

Gerke, Sara & Delaram Rezaeikhonakda (2023), *Privacy Shield 2.0- A New Trans-Atlantic Data Privacy Framework Between the European Union and the United States*, 45(2) CARDOZO LAW REVIEW 351.

Goodman, Tristan (2018), *The Investigatory Powers Act 2016: A Victory for Democracy and the Rule of Law?*, 2018(5) THE BRISTOL LAW REVIEW 2.

doi:10.6342/NTU202504586

Jamison, Shaun G. (2019), *Creating a National Data Privacy Law for the United States*, 10(1) Cybaris® 1.

Jaycox, Mark M. (2021), *No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333*, 12 HARVARD NATIONAL SECURITY JOURNAL 58.

Jung, Niklas (2016), *Abolition of the Safe Harbor Agreement – Legal Situation and Alternatives*, 17 EIKV-SCHRIFTENREIHE ZUM WISSENS- UND WERTEMANAGEMENT [EIKV SERIES ON KNOWLEDGE AND VALUE MANAGEMENT] 1.

Machtiger, Peter G. (2020), *Fixing PPD-28: Implementation Issues and Proposed Revisions for Privacy Protections in Signals Intelligence*, JOURNAL OF LEGISLATION AND PUBLIC POLICY 227.

Pedersen, Jan Helge Brask (2024), *The EU-US Data Privacy Framework and the Schrems Saga: Is there Light at the End of the Tunnel?*, 2024(2) ZEITSCHRIFT FÜR EUROPARECHTLICHE STUDIEN [JOURNAL OF EUROPEAN LEGAL STUDY] 213.

Perumal, Vanessa (2022), *The Future of U.S. Data Privacy: Lessons from the GDPR and State Legislation*, 12(1) NOTRE DAME JOURNAL OF INTERNATIONAL & COMPARATIVE LAW 99.

Reidenberg, Joel R. (2001), *E-Commerce and Trans-Atlantic Privacy*, 38(3) HOUSTON LAW REVIEW 717.

Rotenberg, Marc (2020), Schrems II*, from Snowden to China: Toward a New Alignment on Transatlantic Data Protection*, 26 (2) EUROPEAN LAW JOURNAL 141.

Rudden, Lydia (forthcoming 2025), *Fragmented Data Privacy Laws: Time for Federal Legislation*, 2025 BOSTON COLLEGE INTELLECTUAL PROPERTY AND TECHNOLOGY FORUM.

Schwartz, Paul (2013), *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARVARD LAW REVIEW 1966.

doi:10.6342/NTU202504586

Shaffer, Gregory (2022), *Reconciling Trade and Regulatory Goals: The Prospects and Limits of New Approaches to Transatlantic Governance Through Mutual Recognition and Safe Harbor Agreements*, 9 COLUMBIA JOURNAL OF EUROPEAN LAW 29.

Terpan, Fabien (2018), *EU-US Data Transfer from* Safe Harbour *to* Privacy Shield*: Back to Square one?*, 3(3) EUROPEAN PAPERS 1045.

Woods, Lorna (2017), *The Investigatory Powers Act 2016*, 2017(1) EUROPEAN DATA PROTECTION LAW REVIEW 103.

Xu, Wanxiu et al. (2024), *Global Data Governance at a Turning Point? Rethinking China-U.S. Cross-Border Data Flow Regulatory Models*, 55(106061) COMPUTER LAW & SECURITY REVIEW: THE INTERNATIONAL JOURNAL OF TECHNOLOGY LAW AND PRACTICE 1.

專書論文

Jones, Mariette (2017), *Double-Lock or Double-Bind? The Investigatory Powers Bill and Freedom of Expression in the United Kingdom*, *in* CYBERSURVEILLANCE IN A POST-SNOWDEN WORLD: BALANCING THE FIGHT AGAINST TERRORISM AGAINST FUNDAMENTAL RIGHTS 3 (Russel R. Weaver et al. eds.).

Murphy, Cian C. (2020), *State Surveillance & Social Democracy: Lessons after the Investigatory Powers Act 2016*, *in* THE CONSTITUTION OF SOCIAL DEMOCRACY 413 (Alan Bogg et al. eds.).

Tzanou, Maria (2021), *Schrems I and Schrems II/ Assessing the Case for the Extraterritoriality of EU Fundamental Rights*, *in* DATA PROTECTION BEYOND BORDERS: TRANSATLANTIC PERSPECTIVES ON EXTRATERRITORIALITY AND SOVEREIGNTY, 1 (Federico et al. eds.).

Viola, Lora Anne (2021), *The Limits of Transparency as a Tool for Regulating*

doi:10.6342/NTU202504586

Surveillance: A Comparative Study of the United States, United Kingdom, and Germany, *in* TRUST AND TRANSPARENCY IN AN AGE OF SURVEUILLANCE 21 (Lora Anne Viola & Pawel Laidler eds.)

其它文章

Chauvin, Noah C. (forthcoming 2025), *Increasing Congressional Oversight of FISA Section 702 After RISAA*, 92 TENNESSEE LAW REVIEW (on file with SSRN).

法規

15 U.S.C. § 45.

28 C.F.R. § 201.4 (2022).

28 C.F.R. § 201.7(c) (2022).

49 U.S.C. § 41712 (1978).

Data Protection Act 2018, c. 12 (UK).

Executive Order No. 12,333, 46 Fed. Reg. 59941 (December 8, 1981).

Executive Order No. 14,086, 87 Fed. Reg. 62283 (October 7, 2022).

Executive Order No. 14,117, 89 Fed. Reg. 15421 (February 28, 2024).

Executive Order No. 14,215, 90 Fed. Reg. 10447 (February 24, 2025).

Federal Trade Commission Act, 15 U.S.C. §§ 41-58 (1914).

Foreign Intelligence Surveillance Act, 50 U.S.C. § 1881 (2018).

Intelligence Services Act 1994, c. 13 (UK).

Investigatory Powers Act 2016, c. 25 (UK).

National Security Act, 50 U.S.C. § 3024(f).

Presidential Policy Directive -- Signals Intelligence Activities, NATIONAL ARCHIVES, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-

doi:10.6342/NTU202504586

directive-signals-intelligence-activities.

Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 90 Fed. Reg. 1636 (January 8, 2025) (to be codified at 28 C.F.R. pt. 202).

U.S. CONSTITUTION amendment IV.

U.S. CONSTITUTION amendment X.

U.S. CONSTITUTION.

網路資料

ABOUT HERITAGE, https://www.heritage.org/about-heritage/mission.

About us, NOYB, https://noyb.eu/en/about-us.

Adequacy Decisions, EUROPEAN COMMISSION, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

Adequacy of the protection afforded by the EU-U.S. Data Privacy: Framework European Parliament Resolution of 11 May 2023 on the Adequacy of the Protection Afforded by the EU-US Data Privacy Framework (2023/2501(RSP)), EUROPEAN PARLIAMENT (May 11, 2023), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.pdf.

Anderson, David, *Independent Review of the Investigatory Powers Act 2016*, SSRN (June 14, 2024), https://ssrn.com/abstract=4833577.

Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE 1 (April, 2024), https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.

Barrett, Ted et al., *Senate passes, Biden signs surveillance bill despite contentious debate*

doi:10.6342/NTU202504586

over privacy concerns, CNN (April 21, 2024), https://edition.cnn.com/2024/04/19/politics/fisa-senate-negotiations/index.html.

Biden Jr., Joseph R., *National Security Memorandum on Partial Revocation of Presidential Policy Directive 28*, (October 7, 2022), https://irp.fas.org/offdocs/nsm/nsm-14.pdf.

BOARD MEMBERS, https://www.pclob.gov/Board/Index.

Bromund, Ted, *The U.S. Must Draw a Line on the EU's Data-Protection Imperialism*, THE HERITAGE FOUNDATION (January 9, 2018), https://www.heritage.org/government-regulation/report/the-us-must-draw-line-the-eus-data-protection-imperialism.

Chowdhury, Maureen et al., *Congress Certifies Trump's 2024 Election Win*, CNN (January 7, 2025), https://edition.cnn.com/politics/live-news/election-certification-trump-01-06-25.

Christakis, Theodore, *How Europe's Intelligence Services Aim to Avoid the EU's Highest Court—and What It Means for the United States*, LAWFARE (March 8, 2021), https://www.lawfaremedia.org/article/how-europes-intelligence-services-aim-avoid-eus-highest-court-and-what-it-means-united-states?utm_source=chatgpt.com.

Closure of the injunction issued against GOOGLE, CNIL (August 1, 2023), https://www.cnil.fr/en/closure-injunction-issued-against-google#:~:text=On%2031%20December%202021%2C%20in,to%20accept%20them%2C%20within%20three.

Commission Implementing Decision of XXX Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data Under the EU-US Data Privacy Framework, EUROPEAN COMMISSION (December 13, 2022), https://commission.europa.eu/document/download/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en?filename=Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf

doi:10.6342/NTU202504586

Countries in the EU and EEA, GOV.UK, https://www.gov.uk/eu-eea.

Current Membership - Foreign Intelligence Surveillance Court, UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT, https://www.fisc.uscourts.gov/current-membership-foreign-intelligence-surveillance-court.

D.C. Federal Court Rules Termination of Democrat PCLOB Members Is Unlawful, HUNTON (May 22, 2025), https://www.hunton.com/privacy-and-information-security-law/d-c-federal-court-rules-termination-of-democrat-pclob-members-is-unlawful.

Dutta, Satwik & John H.L. Hansen, *Navigating the United States Legislative Landscape on Voice Privacy: Existing Laws, Proposed Bills, Protection for Children, and Synthetic Data for AI*, ARXIV (July 29, 2024), https://arxiv.org/abs/2407.19677.

EDPB Report on the first review of the European Commission Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, EDPB (November 4, 2024), https://www.edpb.europa.eu/system/files/2024-11/edpb_report_20241104_reportonfirstreviewofeu-u.s.dpf_en.pdf.

Edward Snowden: Leaks that Exposed US Spy Programme, BBC (January 17, 2014), https://www.bbc.com/news/world-us-canada-23123964.

European Commission Gives EU-US Data Transfers Third Round at CJEU, NOYB (July 10, 2023), https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

Facebook and Instagram fined €390m over GDPR breaches, ILN (January 5, 2023), https://www.irishlegal.com/articles/facebook-and-instagram-fined-eur390m-over-gdpr-breaches.

FAQs, NOYB, https://noyb.eu/en/faqs.

Fazlioglu, Müge, *IAPP-EY Annual Privacy Governance Report 2021*, EY 4 (2021),

doi:10.6342/NTU202504586

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4227244.

Hengesbaugh, Brian & Lukas Feiler, *How Could Trump Administration Actions Affect the EU-US Data Privacy Framework?*, IAPP (February 26, 2025), https://iapp.org/news/a/how-could-trump-administration-actions-affect-the-eu-u-s-data-privacy-framework-.

Hughes, J. Trevor & Angela Saverice-Rohan, *IAPP-EY Annual Privacy Governance Report 2019*, EY (2019), https://f.hubspotusercontent20.net/hubfs/525875/IAPP_EY_Governance_Report_2019.pdf.

Intelligence Community Directive 204: National Intelligence Priorities Framework, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE 1 (January 7, 2021), https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf.

Investigatory Powers Commissioner, IPCO, https://www.ipco.org.uk/who-we-are/investigatory-powers-commissioner/.

Joel, Alex, *Necessity, Proportionality, and Executive Order 14086*, AMERICAN UNIVERSITY WASHINGTON COLLEGE OF LAW 1 (May 2023), https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1101&&context=research&&sei-redir=1&referer=https%253A%252F%252Fscholar.google.com%252Fscholar%253Fhl%253Dzh-TW%2526as_sdt%253D0%25252C5%2526q%253Deo%252B14086%2526btnG%253D#search=%22eo%2014086%22.

Judicial Commissioners, IPCO, https://www.ipco.org.uk/who-we-are/judicial-commissioners/.

Judicial Review, COURTS AND TRIBUNALS JUDICIARY, https://www.judiciary.uk/how-the-law-works/judicial-review/.

New Biden Executive Order On EU–US Data Transfers Fails to Adequately Protect

doi:10.6342/NTU202504586

Privacy, ACLU (October 7, 2022), https://www.aclu.org/press-releases/new-biden-executive-order-eu-us-data-transfers-fails-adequately-protect-privacy.

New Trans-Atlantic Data Privacy Framework largely a copy of "Privacy Shield". noyb Will Challenge the Decision., NOYB, https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu.

Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, EUROPEAN COMMISSION 1 (November 23, 2016), https://ec.europa.eu/newsroom/article29/items/640157.

Oremus, Will & Andrea Jiménez, *Trump's Push Against Foreign Tech Rules Could Backfire, Critics Say*, THE WASH. POST (February 27, 2025), https://www.washingtonpost.com/politics/2025/02/27/trump-data-eu-tech-regulations/?utm_source=chatgpt.com.

President Trump's America First Priorities, THE WHITE HOUSE (January 20, 2025), https://www.whitehouse.gov/briefings-statements/2025/01/president-trumps-america-first-priorities/.

PRIVACY SHIELD, https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

Report from the Commission to the European Parliament and the Council on the First Periodic Review of the Functioning of the Adequacy Decision on the EU-US Data Privacy Framework, EUROPEAN COMMISSION (October 9, 2024), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-EU-US-Data-Privacy-Framework-report-of-the-Commission-on-how-the-framework-is-functioning_en.

Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD 1 (September 28, 2023), https://documents.pclob.gov/prod/Documents/OversightRe

doi:10.6342/NTU202504586

port/054417e4-9d20-427a-9850-862a6f29ac42/2023%20PCLOB%20702%20Report%20(002).pdf.

Representative Cathy McMorris Rodgers, CONGRESS.GOV, https://www.congress.gov/member/cathy-rodgers/M001159.

Ruckerbauer, Corbinian et al., *Legal and Oversight Gaps in Germany's Military Intelligence*, ABOUT:INTEL (June 26, 2024), https://aboutintel.eu/germanys-military-intelligence/?utm_source=chatgpt.com.

Schardein, Kyler, *Transatlantic Tech Tensions-The Future of the U.S.-EU Data Privacy Framework*, ASP (March 21, 2025), https://www.americansecurityproject.org/transatlantic-tech-tensions-the-future-of-the-u-s-eu-data-privacy-framework/.

Senators, UNITED STATES SENATE, https://www.senate.gov/senators/index.htm.

Sridhar, Divya, *Trump Administration Playing Truth or Dare with EU-US Data Privacy Framework*, INFOSECURITY MAGAZINE (May 5, 2025), https://www.infosecurity-magazine.com/opinions/trump-eu-us-data-privacy-framework/?utm_source=chatgpt.com.

The American Privacy Rights Act, CONGRESS.GOV (May 31, 2024), https://www.congress.gov/crs-product/LSB11161.

The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against GOOGLE LLC, EDPB (January 21, 2019), https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en.

The ePrivacy Directive and the Evolution of Data Privacy in the EU: What You Need to Know, COOKIEBOT (April 17, 2025), https://www.cookiebot.com/en/eprivacy-regulation/#:~:text=Ultimately%2C%20the%20European%20Commission%20officially,minors%20(Article%2028)"..

doi:10.6342/NTU202504586

Trans-Atlantic Data Privacy Framework, EUROPEAN COMMISSION (2022), https://ec.europa.eu/commission/presscorner/api/files/attachment/872132/Trans-Atlantic%20Data%20Privacy%20Framework.pdf.

Trump Administration Embraces Heritage Foundation Policy Recommendations, THE HERITAGE FOUNDATION (January 23, 2018), https://www.heritage.org/impact/trump-administration-embraces-heritage-foundation-policy-recommendations?utm_source=chatgpt.com.

Wizner, Ben et al., *Trump on Surveillance, Protest, & Free Speech*, ACLU 1, https://www.aclumaine.org/sites/default/files/trump_memo_surveillance_protest_and_free_speech.pdf.

Xu, Wanxiu et al., *Whose Victory? A Perspective on Shifts in US-China Cross-Border Data Flow Rules in the AI Era*, THE PACIFIC REVIEW 1, 5 (February 5, 2025), https://www.tandfonline.com/doi/full/10.1080/09512748.2025.2462239#abstract.

歐盟文件

2000 O.J. (L 215) 16.

Commission Decision of 15 June 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, Under Directive 95/46/EC (Notified Under Document Number C(2001) 1539), 2001 O.J. (L 181) 9.

Commission Decision of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, 2000 O.J. (L 215) 7.

Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive

doi:10.6342/NTU202504586

95/46/EC of the European Parliament and of the Council, 2010 O.J. (L 39) 5.

Commission Implementing Decision (EU) 2016/1250 Of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 281) 31.

Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 Amending Decisions 2001/497/EC and 2010/87/EU on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries and to Processors Established in such Countries, Under Directive 95/46/EC of the European Parliament and of the Council, 2016 O.J. (L 344) 100.

Commission Implementing Decision (EU) 2021/1773 of 28 June 2021 Pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the Adequate Protection of Personal Data by the United Kingdom (Notified Under Document C(2021) 4801), 2021 O.J. (L 360) 69.

Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (Text with EEA relevance), 2021 O.J. (L 199) 31.

Commission Implementing Decision EU 2023/1795 of 10 July 2023 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Level of Protection of Personal Data Under the EU-US Data Privacy Framework, 2023 O.J. (L 231) 118.

Commission Implementing Regulation (EU) 2021/1772 of 28 June 2021 Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the Adequate Protection of Personal Data by the United Kingdom (Notified Under Document C(2021)4800) (Text with EEA Relevance), 2021 O.J. (L 360) 1.

doi:10.6342/NTU202504586

Council Decision (EU) 2020/135 of 30 January 2020 on the Conclusion of the Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (Text with EEA Relevance), 2020 O.J. (L 29) 1.

Council Decision (EU) 2020/2252 of 29 December 2020 on the Signing, on Behalf of the Union, and on Provisional Application of the Trade and Cooperation Agreement Between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part, and of the Agreement Between the European Union and the United Kingdom of Great Britain and Northern Ireland Concerning Security Procedures for Exchanging and Protecting Classified Information, 2020 O.J. (L 444) 2.

Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 Amending Annex XI (Electronic Communication, Audiovisual Services and Information Society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022], 2018 O.J. (L 183) 23.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31.

Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework, EDPB 1, 9 (Feb. 28, 2023), https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC,

doi:10.6342/NTU202504586

2016 O.J. (L 119) 1.

Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers, 2011 O.J. (L 55) 13.

條約

Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses, EU-U.S., May 18, 2016, https://www.hunton.com/privacy-and-information-security-law/assets/htmldocuments/uploads/sites/18/2016/06/ST_8557_2016_INIT_EN.pdf.

Charter of Fundamental Rights of the European Union, 2000 O.J. (C 361) 1.

Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221.

其它

Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd & Maximillian Schrems, ECLI:EU:C:2020:559 (July 7, 2020).

Case C-362/14, Maximillian Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (October 6, 2015).

doi:10.6342/NTU202504586