University of Sheffield | Sheffield Centre for International & European Law

Sheffield Centre for International and European Law

School of Law

Working Paper Series

An (in)adequate Data Protection Regime after Brexit? Bulk Surveillance Powers, National Security and the Future of EU-UK Data Transfers

Sotirios Santatzoglou and Maria Tzanou

2023/3

Forthcoming in:

E. Celeste (et al.) ***Data Protection and Digital Sovereignty Post-Brexit*** **(Hart, 2023).**

SCIEL builds on a long and distinguished tradition of international and European legal scholarship at the University of Sheffield School of Law. Research in the Centre focuses on the international and European aspects of legal issues, and more broadly draws on the School's strengths in many forms of International, European and Comparative Law to consider the wider implications of current problems and the function of law in a globalised world. As part of this mission, the Centre publishes the present Working Paper Series.

Please visit www.sheffield.ac.uk/law/sciel for more information about the Centre or contact:
Email: law@sheffield.ac.uk
Twitter: @lawsheffield

The full Working Paper Series is available at
https://www.sheffield.ac.uk/law/research/clusters/sciel/working-papers

An (in)adequate Data Protection Regime after Brexit? Bulk Surveillance Powers, National Security and the Future of EU-UK Data Transfers

Sotirios Santatzoglou and Maria Tzanou*

I. Introduction

On 28th June 2021, the Commission adopted two adequacy decisions -one under the General Data Protection Regulation (GDPR)[1] and one under the Law Enforcement Directive (LED)-[2] confirming that the UK ensures a level of protection for personal data transferred from the EU that is 'essentially equivalent' to the one guaranteed by EU data protection law.[3] In its UK adequacy decision on the GDPR, the Commission included a discussion entitled 'Access and use of personal data transferred from the European Union by public authorities in the United Kingdom' that analysed the UK's legal framework for government access to personal data collected by business operators for criminal law enforcement and national security purposes.

Nevertheless, despite the Commission's adequacy findings in this respect, significant uncertainty still exists regarding the UK surveillance framework that risks jeopardising the future of the EU-UK data privacy relations. Indeed, there are important concerns and doubts as to whether the UK's national security regime is actually 'essentially equivalent' to the EU's standards, albeit the Commission's positive findings in this regard. The inadequateness of this regime is not a new issue; rather, it is deeply rooted in the UK's broader socio-political choices that prioritise security over fundamental rights concerns. The historical examination presented in the first part of this chapter reveals that this trend emerged long ago, within the broader context of law enforcement and with the in-principle agreement of the two UK main parties.

Drawing on this historical examination of the UK political setting, this chapter argues that the UK approach follows an established, *irreversible* (primary political) *path* dictating *expansionism* as the main direction in crime prevention and national security policy. Bulk surveillance powers are at the centre of this expansionist approach as they figure prominently in the UK's regulatory architecture both in the context of law enforcement and national surveillance despite a series of critical decisions by the

---

[1*] The drafting of Section II is attributed to Sotirios Santatzoglou, and that of Section III to Maria Tzanou. Sections I and IV were co-drafted. The whole manuscript was shaped by both authors.

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 (General Data Protection Regulation) [2016] OJ L119 (GDPR); European Commission, Commission Implementing Decision of 28.6.2021 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, C(2021) 4800 final.

[2] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (Law Enforcement Directive) [2016] OJ L 119/89 (LED); Commission Implementing Decision of 28.6.2021 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, C(2021) 4801 final.

[3] ibid, Article 1.

Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR). At the same time, bulk surveillance powers are one of the main concerns of EU institutions regarding EU-UK data protection relations in the post-Brexit era. Indeed, such concerns open up the post-Brexit EU-UK data privacy relationships to significant uncertainty and volatility that might undermine trust resulting in a future finding of inadequacy. Regrettably, they also erode the standards of fundamental rights protection in the UK as a whole - an unwelcome further consequence of Brexit.

Following this Introduction, the chapter is structured as follows: Section II undertakes a historical examination of the bulk powers regulatory framework in the UK by exploring its peculiar trajectory (II.A), its underpinning rationale (II.B), and its established broader use in the context of law enforcement (II.C). It then turns to the current UK national security framework, the Investigatory Powers Act (IPA) 2016 and examines in detail the political debate that preceded its adoption (II.D). Section III focuses on the EU-UK post-Brexit data protection regulatory environment, pointing out the unique position of the UK (III.A) and the interesting issues that arise regarding the extraterritorial application of EU fundamental rights in the post-Brexit context (III.B). It then explores the main vulnerabilities of the UK's national security regime (III.C). The final part offers brief conclusions (IV).

II. UK bulk surveillance and the determining impact of the political setting

A. The peculiar regulatory trajectory of surveillance powers

The legislative process concerning the regulation of surveillance powers in the UK has followed a peculiar trajectory fraught with complexities. The saga commenced from the invalidation by the CJEU of the EU Data Retention Directive,[4] which was the basis for the Regulation of Investigatory Powers Act 2000 (RIPA). At the same time, following the Snowden revelations of the hitherto unknown Government Communications Headquarters (GCHQ) surveillance practices,[5] the existence of a 'questionable' legal basis concerning the exercise of state surveillance activities had become apparent[6] raising the need to reconsider the RIPA regime.[7]

The enactment of the Data Retention and Investigatory Powers Act (DRIPA) 2014 was supposed to address the serious issues arising from its predecessor, the RIPA. DRIPA was 'quickly passed' in the Parliament[8] aiming to cure the RIPA pathologies. However, following the CJEU's *Tele2 and Watson* judgment, DRIPA was also deemed to be 'not fit for purpose'.[9] In the domestic 'Davis' (later 'Watson') judicial review, which was brought against the Secretary of State from a group of five (all-parties) parliamentarians, the High Court[10] concluded that DRIPA was incompatible with EU law as set out in

[4] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105/54.

[5] Clive Walker, Case Comment *R. (on the application of Davis) v Secretary of State for the Home Department* Divisional Court [2016] Crim. L.R. 1, 50.

[6] Burkhard Schafer, 'Surveillance for the masses: The political and legal landscape of the UK Investigatory Powers Bill' [2016] Datenschutz und Datensicherheit 592.

[7] Lorna Woods, 'United Kingdom: Draft Investigatory Powers Bill' [2016] 2 Eur Data Prot L Rev 103.

[8] Matthew White 'Data retention: serious crime or a serious problem?' [2019] PL 633.

[9] Mariette W Jones, 'Double-lock or double-bind? The Investigatory Powers Bill and freedom of expression in the United Kingdom' in Russell L Weaver, Steven I Friedland, Arnaud Raynouard, and Duncan Fairgrieve (eds), *Cybersurveillance in a Post-Snowden World: Balancing the Fight Against Terrorism Against Fundamental Rights* (CAP 2017).

[10] *R. (on the application of Davis) v Secretary of State for the Home Department*, [2015] EWHC 2092 (Admin).

Digital Rights Ireland.[11] This was because the CJEU had found communications data retention only permissible if the objective is to fight serious crime[12], a threshold not provisioned in DRIPA. At the appeal stage of the 'Davis/Watson' judicial review, the Court of Appeal referred the case to the CJEU,[13] but by then it had already become clear that (again) new legislation was needed to correct and expand upon DRIPA, as the UK legal framework regulating surveillance was 'in tatters'.[14]

One would reasonably expect that by then the UK government would have learned from the judicial lessons. The Investigatory Powers Bill (IPB) was announced in May 2015, introduced to the House of Commons in March 2016 and received royal assent on 29 November 2016. During the parliamentary debates, it was evident that MPs (and the government) understood well that the Bill was legalising 'excessive powers' whilst the 'Watson'/'Davis' case was 'midway between the CJEU and the Court of Appeal' with the expectation to confirm the CJEU's approach restricting data retention to serious crime purposes.[15] Indeed, in December 2016, the CJEU issued its decision in *Tele2 and Watson* confirming 'the fight of *serious* crime' as the threshold for the retention of communications data.[16]

The UK government conceded the incompatibility of the newly enacted IPA with EU law and planned its amendment[17] to address (among other things) the missing 'serious crime' threshold. In the meantime, following a challenge from the *National Council for Civil Liberties*, the High Court[18] ruled the IPA 2016 to be incompatible with EU law – 'partially because access to retained data was not limited to the purposes of fighting serious crime'.[19] The judgment set 1 November 2018 as the deadline for amending legislation to draw up 'an alternative scheme'.[20] Indeed, as a commentator noted, while the IPA 'was meant to clarify and settle electronic surveillance powers, it [was] itself unsettled'.[21] In 2018, the Court of Appeal confirmed that the DRIPA was incompatible with EU law.[22] On 31 October 2018, the Data Retention and Acquisition Regulations Act (DRARA) was enacted addressing the contentious issues arising from RIPA and IPA, including the introduction of a serious crime threshold, especially when indiscriminate bulk surveillance practices were involved.

B. Underlying reasons

The above saga is explained by the political *hastiness* in preparing and voting the relevant laws, an unwelcome practice for legislation of such significance.[23] This peculiar legislative trend primarily

---

[11] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* and Karntner Landesregierung and Others), ECLI:EU:C:2014:238.

[12] White (n 8).

[13] *R. (on the application of Davis) v Secretary of State for the Home Department* [2015] EWCA Civ 1185; [2016] 1 C.M.L.R. 48. The Court of Appeal disagreed with the High Court and referred to CJEU - Jennifer Cobbe 'Casting the dragnet: communications data retention under the Investigatory Powers Act' [2018] PL 10,11; White (n 8) 633.

[14] Schafer (n 6).

[15] House of Commons, Investigatory Powers Bill, Hansard, Volume 611, Monday 6 and Tuesday 7 June 2016; see in particular Sir Keir Starmer, Column 1067.

[16] Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och telestyrelsen; Secretary of State for the Home Department v Watson*, EU:C:2016:970; see also discussion White (n 8) 633.

[17] White (n 8) 633-34.

[18] *The National Council for Civil Liberties (Liberty), R (On the Application Of) v Secretary of State for the Home Department & Anor* [2018] EWHC 975 (27 April 2018).

[19] White (n 8) 633, 34.

[20] ibid.

[21] Christos Boukalas, 'Overcoming Liberal Democracy: 'Threat Governmentality' and the Empowerment of Intelligence in the UK Investigatory Powers Act' in Austin Sarat and Patricia Ewick (eds), *Studies in Law, Politics, and Society* (Emerald 2020) 1.

[22] White (n 8) 633, 34.

[23] Case Comment, 'Data protection law to be rewritten following court ruling', *Comp. & Risk* 2015, 4(4), 17-18

demonstrates the *distancing* of policy from judicially established standards -both at the national and the EU level- on matters of communications surveillance. This *distancing* reflects a policy direction leaning favourably towards the legitimisation of extended state surveillance by intelligence services and the police. The granting of extended surveillance powers to intelligence agencies sets the UK policy in *distancing* not only with judicial values, but also with the policy practice of major EU continental states. As Brants indicated, unlike the UK, in the Netherlands, 'intrusive police investigation is a primary concern', and the policy emphasis is on the adherence of agencies to the rules of proportionality and necessity, as required by European courts.[24] Indeed, the British differentiation in the regulation of surveillance powers can be attributed to the UK's 'historical and political context'.[25] It can be linked to the Tories as an 'increasingly surveillance' and 'police friendly' party,[26] and to the Labour Party broadly failing to exercise effective opposition on these matters.[27] Regrettably, it has resulted in accepting the intelligence sector as 'determining the law' governing surveillance.[28]

These political hermeneutics form an appropriate appreciation of the British regulatory landscape concerning surveillance powers. In particular, the risk of asymmetrical terrorist threats has been proffered as a reason behind this political approach and hence the need to develop 'total intelligence' to fight this 'new type of enemy'.[29] Nevertheless, it should be noted that this explanatory perspective is limited. As the then Home Office Secretary Theresa May stated in the Forward of the draft IPB, surveillance powers are also essential to the fight against wider crime, such as tackling child sexual exploitation, dismantling serious crime cartels, taking drugs and guns off the streets.[30] The roots of this permissive regulation can be traced, to the nature of British criminal policy that goes beyond the evolution of terrorism legislation. It is, thus, crucial to place the UK national security regulation within the broader context of the country's criminal policy. The following section examines the historical evolution of this policy approach.

C. A criminal policy leaning to authoritarianism

The crime rhetoric had 'played a prominent role' in Thatcher's 1979 election, but during her premiership criminal policy was marked by 'principled pragmatism' as it was 'broadly "liberal" in its 'intentions and effects'.[31] A policy shift towards authoritarian solutions became evident in the early 1990s, during Major's conservative government. The appointment of Michael Howard as home secretary in 1993 signified a 'turning point' for the British criminal policy.[32] What was called the 'moment of Howard' embodied both a rhetoric and commitment *rejecting* 'the long-standing policy of prison as a last resort'.[33] Howard's U-turn was summarised in his catch-phrase 'Let us be clear - Prison

---

[24] Chrisje Brants, Adam Jackson, Tim Wilson 'A Comparative Analysis of Anglo-Dutch Approaches to 'Cyber Policing': Checks and Balances Fit for Purpose? [2020] J. Crim. Law 451, 467.

[25] Schafer (n 6).

[26] Ibid.

[27] Cian Murphy, 'State Surveillance and Social Democracy' in Alan Bogg, Jacob Rowbottom and Alison L Young (eds), *The Constitution of Social Democracy: Essays in Honour of Keith Ewing* (Hart Publishing 2020).

[28] Boukalas (n 21) 2-4.

[29] ibid 9, 10.

[30] *Draft Investigatory Powers Bill*, November 2015, Cm 9152.

[31] David Faulkner, 'The End of the Beginning of an Era? Politics and Punishment under Margaret Thatcher's Government', in Martin Wasik and Sotirios Santatzoglou (eds), *The Management of change in criminal justice: Who knows best?* (Palgrave Macmillan 2015) 34.

[32] Sotirios Santatzoglou and Martin Wasik, 'Who knows best? in Martin Wasik and Sotirios Santatzoglou (eds), *The Management of change in criminal justice: Who knows best?* (Palgrave Macmillan 2015) 14.

[33] Joe Sim, P*unishment and Prisons: Power and the Carceral State*, (Sage 2009).

works'.[34] This political move aimed to bring a weakening conservative government in touch with the public,[35] the 'silent majority'[36] and their common sense logic. This political choice shifted criminal policy, gradually, towards an authoritarian formula.[37]

From 1997 onwards, the subsequent New Labour governments, faithful to the electorally successful Blair's credo of *tough-on-crime*, clearly endorsed, strengthened and widened this criminal policy transition in terms of both rhetoric *and* commitment. In this way, the successive New Labour governments ensured that the *law-and-order* territory was not a Tory dominated political arena as they listened to the 'ordinary people's' concerns over crime and to their common-sense solutions.[38]

Hence, Howard's moment marked the start of an era of *politicisation* linking crime policy to electorate interests, as the main political parties argued over their competence to fight crime through the greater use and enactment of criminal laws.[39] Crime prevention, law enforcement and punishment became *distant* from the less-appealing to electorate concepts of proportionality and necessity. Criminal policy became integral to the political readiness to respond with immediate legislative action to the populist press' headlines concerning crime and public safety. As Ashworth observed, this politicisation trend resulted in an unprincipled and chaotic overgrowth of criminal laws and policy:

> '[criminal law] … is a multi-purpose tool, often creating the favourable impression that certain misconduct has been taken seriously and dealt with appropriately.'[40]

Notably, a further feature of this trend was the occurrence of a political *soft consensus* between the two major UK parties concerning the adoption of conservative, social authoritarian formulas of criminal policy.[41] As Downes and Morgan put it: 'In the twenty-first century we may be witnessing some underlying agreement in law and order' where 'political squabbles […] are largely about relative levels of expenditure on law and order services, police numbers and the like'.[42] Indeed, the *politicisation* trend has been characterised by the absence of political argumentation over issues of principle concerning the shaping of the boundaries of criminal law and criminal justice. A crude statistical example of this trend is evidenced in the growth of imprisonment in the UK. In 2016, the rate of imprisonment in England and Wales was 'the 8th highest among EU countries and the highest amongst western European jurisdictions'[43] (with countries of a higher rate coming from the former Soviet bloc).

The direction towards the expansion of control measures in the UK has been particularly evident though the extended use of modern technologies.[44] The strong political attraction in the UK to science and emerging technologies was demonstrated as early as 1999 with the additional funding of the

---

[34] Speech to the Conservative Party conference, October 6, 1993, https://www.michaelhoward.org, Prison_Works.

[35] Santatzoglou and Wasik (n 32) 15.

[36] Colin Brown 'Howard seeks to placate 'angry majority': Home Secretary tells party that balance in criminal justice system will be tilted towards public' *The Independent* (6 October 1993).

[37] Sir Leon Radzinowicz, 'Penal Regressions' [1991] CLJ 428.

[38] Andrew Rutherford, 'An Elephant on the doorstep', in Penny Green and Andrew Rutherford (eds), *Criminal Policy in Transition* (Hart Publishing 2000); Santatzoglou S & Wasik (n 32) 17.

[39] Santatzoglou and Wasik (n 32) 17.

[40] Andrew Ashworth, 'Is the criminal law a lost cause?' [2000] LQR 225, 226.

[41] Santatzoglou and Wasik (n 32) 25,26. This was the case even during the coalition government period, despite the participation of the Liberal Democrats, as the case of the government's youth crime control policy demonstrated; see for example, Roger Smith, 'Troubling Troubled or Troublesome?' in Martin Wasik and Sotirios Santatzoglou (eds), *The Management of change in criminal justice: Who knows best?* (Palgrave Macmillan 2015)

[42] David Downes and Rod Morgan, 'Overtaking on the left?' in Mike Maguire, Rod Morgan, and Robert Reiner (eds) *The Oxford Handbook of Criminology* (OUP 5th edn. 2012).

[43] Georgina Sturge, *UK Prison Population Statistics*, Commons Library Research Briefing (29 October 2021) 30

[44] Importantly, critics of the IPA extended use of bulk surveillance also stress the largeness of DNA databases and/or the wide use of CCTV sets; see for example, Jones (n 9).

incoming New Labour government – over £300 million over five years – for the rapid expansion of the *National DNA Database*, which ended as the largest genetic information database in the world.[45] The database was seen as 'Tony Blair's flagship scheme to store the genetic fingerprints of every criminal in Britain'.[46] Within the political (and law enforcement) chambers, the storing of 6 million profiles was considered an 'uncomplicated success story' of crime detection and reduction justifying the uncritical disregard of questions of civil liberties and human rights.[47]

This pattern of politically driven bulk expansion of crime control biotechnology can be also observed in the UK's use of CCTV. Indeed, the extensive use of CCTV by public authorities for the purpose of crime prevention is closely linked with the 'looking-for-the- needle-in-the-haystack' approach that followed RIPA.[48] The use of CCTV as a mainstream crime prevention measure can be traced to UK conservative government policy choices in 1996.[49] The subsequent 'dramatic increase' of these systems following governments' generous funding reflected the public popularity of the measure, and the political belief in potential benefits of 'being seen to be doing something visible' against crime.[50] Nevertheless, despite the generation of large data sets from CCTV records, there was 'rather little serious debate' regarding civil liberties issues or scientific evidence concerning the effectiveness of these systems.[51] In fact, in the early days of CCTV bulk expansion, 'political parties […] raised few critical questions',[52] focusing instead on the 'apparent plausibility [CCTV] (must work)'[53] as a crime solution. This approach disregarded crucial issues, such as that CCTV could also 'capture not only what individuals do, but also whom they meet […] whether it be with potential business partners, lovers, political allies, or (non-criminal) friendship with offenders'.[54]

This long-ongoing – since the mid-1990s – bipartisan UK government obsession with extensive crime prevention and control measures is the main reason for the adoption of a bulk- oriented political logic regarding the use of control measures. From the growth of imprisonment to the CCTV expansion, the logic is the same: bulk use of powers. Within this political setting, considerations of a measured and ethical use of interventions are not sufficiently discussed or are faced with indifference during the political legislative process. The political soft consensus of social authoritarianism across the two main UK parties has upheld without much criticism the sanctity of bulk crime prevention and control and arguably also defined the legislative process of national security bulk surveillance powers. It is exactly within this ongoing broader socio-political and historical background that the IPA was negotiated in the UK Parliament.

D. The IPA 2016 and the surveillance bulk powers debate

45

[46] Martin Bright and Gaby Hinsliff, 'Police snub Blair's DNA bank' *The Observer* (3 Sep 2000).

[47] Aaron Opolu Amankwaa and Carole McCartney, 'The effectiveness of the UK national DNA database' [2019] Forensic Sci. Int.: Synergy 45, 46-47.

[48] Schafer (6).

[49] Eric L Piza, Brandon C Welsh, David P Farrington, and Amanda L Thomas 'CCTV surveillance for crime prevention - A 40-year systematic review with meta-analysis' [2019] Criminol Public Policy 136.

[50] Kate A Painter and Nick Tilley, 'Seeing and being seen to prevent crime', in Kate A Painter and Nick Tilley (eds), *Surveillance of public space: CCTV, street lighting and crime prevention*, (Crime Prevention Studies 1999); Rachel Armitage, 'To CCTV or not to CCTV? A review of current research into the effectiveness of CCTV systems in reducing crime' (Narco, 2002) 8.

[51] Ibid.

[52] Ibid.

[53] Armitage (n 50) 8.

[54] Painter and Tilley (n 50).

The enactment of the IPA 2016 was seen as 'an improvement to the previous situation'.[55] This is, in particular, because of the introduction of the so-called 'double lock' procedure, under which a surveillance warrant issued by the Secretary of State must be subject to review by a 'judicial commissioner',[56] providing – according to the UK government – a 'fundamental safeguard'.[57]

However, the IPA was criticised for its 'ambivalence'[58] and strongly opposed by civil liberties groups.[59] Bulk powers surveillance was seen as the major controversy of the legislation.[60] The IPA legalised the employment of bulk powers placing an obligation on companies to assist in such operations and 'bypass encryption',[61] thus resulting in a form of mass state surveillance. [62] During the bill consultation, David Anderson KC, as Independent Reviewer of Terrorism Legislation, warned of the controversial nature of bulk powers which 'may be seen as placing control in the hands of the state'.[63] Early critics pointed out that the bulk practice is indiscriminate in nature with the apparent potential of 'bringing individuals who are not of interest to the authorities under a form of surveillance'.[64] In the context of communications data surveillance, the IPA established bulk retention as the *rule* rather than the exception thereby permitting the general and indiscriminate data retention with no legitimate aim.[65]

The UK Parliament debate provides a telling case study of the bipartisan soft consensus legitimising the use of bulk powers. During the Report stage debate of the IPB that took place in the Parliament on the 6th and 7th June 2016, small opposition parties (such as the Liberal Democrats and the Scottish National Party-SNP), along with Harriet Harman MP, chair of the Joint Committee on Human Rights, and few Conservative and Labour backbenchers, raised a number of criticisms regarding bulk powers. It was pointed out that a Bill 'of huge constitutional significance' was allocated 'fewer than two full working days to debate it on Report.'[66] Conservative MP McPartland noted that 'the carte blanche on bulk powers should not be the first resort; it should always be the last resort';[67] whilst conservative MP Clarke indicated the expansionist character of the Bill noting that a serious threshold is required for all bulk powers surveillance.[68] SNP MP McLaughlin stressed that the regulation of bulk powers was 'perhaps one of its most controversial parts',[69] noting that:

> "At the heart of the matter is the retention of intimate personal details regarding the tens of millions of ordinary citizens of this country who do not merit such information being held by the state. […] The offline analogy is instructive. If we were asked by the state to deposit our membership forms for various organisations—political parties, campaign groups, golf clubs—or forms with our direct debit details, health records and other such bulk information into a big safe on the understanding that only the security services would have access to it, we would rightly baulk at such a proposal. Just because such a system is being proposed online and without the

[55] Lorna Woods, 'The Investigatory Powers Act 2016' [2017] 3 Eur Data Prot L Rev 13.
[56] Section 227 IPA.
[57] Jones (n 9).
[58] ibid 8, 11.
[59] Cobbe (n 13) 11.
[60] Ibid.
[61] Jones (n 9) 10.
[62] Vaibhav Chadha, 'Balancing the privacy v. surveillance argument: a perspective from the United Kingdom' Eur. J. Int. Relat [2022] 190, 196.
[63] David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015) para 2.7
[64] Woods (n 7) 104.
[65] Schafer (n 6); Cobbe (n 13) 18; White (n 8) 642; Boukalas (n 21); Gemma Davies, 'Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers' JCL [2020] 407, 425.
[66] House of Commons (n 15) Joanna Cherry Column 1148.
[67] House of Commons (n 15) Stephen McPartland Column 1092.
[68] House of Commons (n 15) Ken Clarke Column 1122.
[69] House of Commons (n 15) Ann McLaughlin Column 1053.

consent of the individuals concerned does not make it acceptable—in many ways, it makes it much worse."[70]

Nevertheless, these arguments demonstrating the problematic expansion of surveillance powers were ignored during the two days parliamentary debate. Instead, a by-partisan soft consensus between the Conservative party and the Labour party emerged as the 'Opposition and the Government […] worked together on the Bill'[71]; and 'made good progress'[72]. In this regard, the Labour Party stated that it had adopted 'a responsible and pragmatic approach' to the Bill;[73] evident in 'the very constructive way' in which Labour dealt with the government's proposals.[74] This alignment between the two main UK parties demonstrated a consensus on the necessity of bulk powers for intelligence agencies.

Among the conservatives, the endorsement of bulk powers was accepted from the Eurosceptic right-wing end of the party to its centre-right Europhile side. The former justified the indiscriminate surveillance on the 'constant state of threat' and the 'international security war […] [and the] war on the online fraudsters and the paedophiles' that the government was waging;[75] whilst the latter argued for the significant utility of 'the needle in the haystack' approach.[76] In fact, it was pointed out that although what is searched is indeed 'a needle in a haystack', 'bulk powers are essential for building up that network in order to be able to search';[77] and thereby to 'discover new threats from people who were previously unknown and identify patterns of behaviour'.[78] In this way, the conservative party presented the bulk approach to surveillance as necessary reflecting, as one conservative (pro-European) MP put it, 'the reality' despite its controversial nature,[79] which shows that none of these powers are 'unnecessary or disproportionate'.[80]

The Labour opposition, in line with the soft consensus approach on the expansionism of criminal policy, adopted a *sitting on the fence* approach otherwise minimally questioning the bulk surveillance powers. A characteristic example of the former was the Labour's two-fold suggestion: (a) to set an overarching privacy clause and (b) to set an independent review of "the operational case for the bulk powers".[81] Unsurprisingly, the government accepted both 'demands'. Ironically the suggested clause did not set any binding effect on the decision makers;[82] something which indicates its toothless effect. Also, ironically, the latter 'demand' led to the Anderson 2016 'Report of the Bulk Powers Review', which concluded with the operational vitality of bulk powers.[83] Regarding the labour amendments aiming at minimal limitations to bulk powers, their proposed definition of 'serious crimes' was to cover offences with a provisioned imprisonment of more than six months. As Labour MPs stated, 'we felt that that was proportionate'.[84] Ironically, two years later, during the consultation to amend the IPA, the government conceded that their proposed six-month imprisonment threshold concerning the retention of

[70] House of Commons (n 15) Ann McLaughlin Column 1058.
[71] House of Commons (n 15) John Hayes Minister for Security Column 981.
[72] House of Commons (n 15) Keir Starmer Column 1065.
[73] House of Commons (n 15) Andy Burnham Column 952.
[74] House of Commons (n 15) James Berry Column 1135.
[75] House of Commons (n 15) Suella Fernandes Column 1085.
[76] House of Commons (n 15) Dominic Grieve, Chair of the Intelligence Services Committee, Column 1059.
[77] House of Commons (n 15) Tom Tugendhat Column 1082.
[78] House of Commons (n 15) Seema Kennedy Column 1082, Stephen Hammond Column 1087.
[79] House of Commons (n 15) Dominic Grieve, Chair of the Intelligence Services Committee, Column 1059.
[80] House of Commons (n 15) Stephen Hammond Column 1087.
[81] House of Commons (n 15) Sir Keir Starmer Column 883.
[82] Woods (n 55)
[83] D. Anderson Q.C *Report of the Bulk Powers Review* August 2016 see pp.119-128. Anderson acted in his capacity as Independent Reviewer of Terrorism Legislation.
[84] House of Commons (n 15) Andy Burnham Column 1120

communication data[85] did not sufficiently reflect the notion of 'serious crime' as established by the CJUE, thereby accepting the increase to 12 months.[86]

This non-conflictual debate of the IBP Report is another evidence of the politicisation of criminal and national security policy in the UK and the interrelated bipartisan soft consensus in embedding bulk powers in IPA. The centrality of bulk powers within the IPA's architecture demonstrates the 'legal buttressing' of the 'anti-legal logic' of indiscriminate surveillance within the rule of law framework.[87] Nevertheless, it should be stressed that this is the outcome of a long-established bi-partisan political consensus in the UK rooted in expansive law enforcement powers. Importantly, the boundaries of this setting are not limited to the extreme sides of the political spectrum but rather include the critical political zone in the UK which is extended between the centre-right and the centre-left. This is why this soft authoritarian direction legitimising bulk powers appears irreversible. The question then is about its consequences within the EU-UK data protection regulatory space.

III. Surveillance in the post-Brexit EU-UK data protection relations

A. International data transfers and the UK uniqueness

In many ways, the UK occupies a unique position among the third countries engaging in international data transfers with the EU. The UK is the only third country enjoying a former EU Member State status[88] and has, therefore, for decades implemented EU primary and secondary in law in general and data protection law in particular. The UK has also been subject to the CJEU's jurisprudence until 31st January 2020. The European Union Withdrawal Act (EUWA) 2018 directly incorporated applicable EU legislation into the UK's legal order.[89] Hence, the GDPR is considered 'retained EU law'[90] in the UK and Part 3 of the Data Protection Act (DPA) 2018[91] - which transposes the Law Enforcement Directive (LED) - constitutes 'EU-derived domestic legislation'.[92]

Besides the previous Member State status, the UK is also subject to international human rights law commitments shared by the EU, as a member of the Council of Europe, the European Convention on Human Rights (ECHR), the Convention for the protection of individuals with regard to the processing of personal data (Convention 108+) and its submission to the jurisdiction of the European Court of Human Rights (ECtHR).[93] Hence, the ECtHR case law has had a significant positive effect on the compliance of UK surveillance frameworks and mechanisms with the Convention's rights. For instance, the UK Investigatory Powers Tribunal (IPT), considered by the ECtHR in 2010 as providing

---

[85] Home Office, *Investigatory Powers Act 2016 Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data,* (November 2017)

[86] Home Office, *Investigatory Powers Act 2016: Response to Home Office Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data* (June 2018); White (n 8) 635,636

[87] Boukalas (n 21) 9,16

[88] See also EDPB, 'Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom', adopted on 13 April 2021, para 35.

[89] European Union Withdrawal Act 2018 https://www.legislation.gov.uk/ukpga/2018/16/contents See also Joseph Savirimuthu and Maria Tzanou 'The United Kingdom'. In *International Encyclopaedia of Laws: Privacy and Data Protection*, edited by Jos Dumortier, Pieter Gryffroy, Ruben Roex & Yung Shin Van Der Sype. Alphen aan den Rijn, NL: Kluwer Law International, 2022.

[90] Section 6 EUWA 2018.

[91] Data Protection Act 2018 <https://www.legislation.gov.uk/ukpga/2018/12/contents>.

[92] Section 6 EUWA 2018.

[93] Commission adequacy decision on GDPR, para 19.

inadequate remedies, was found in 2018 as providing 'a robust judicial remedy to anyone who suspected that his or her communications had been intercepted by the intelligence services'.[94] Indeed, the IPT has progressively evolved over the years from 'passively reviewing the law to actively intervening in it',[95] with the European Data Protection Board noting that it 'functions as a proper court in the meaning of Article 47 Charter of Fundamental Rights of the European Union'.[96]

Compliance with data protection rules and enforcement in the UK is carried out by an independent supervisory authority, the Information Commissioner's Office (ICO), although the ICO's role in the area of national security processing is limited.[97] For instance, according to Schedule 11 of section 110 DPA 2018, intelligence services are not obliged to communicate personal data breaches to the ICO.

Against this background, a Commission adequacy finding appeared relatively easy in the UK case as its 'data protection rules […] in many aspects closely mirror the corresponding rules applicable' within the EU.[98] Indeed, the UK did not seem to pose the challenges that the Commission faces when encountering the US legal framework and surveillance regimes.[99] That being said, a flexible approach to allow the swift operation of international data transfers seems to have been adopted in the case of the UK as well. As the Commission confirmed, 'the adequacy standard […] does not require a point-to-point replication of Union rules. Rather, the test lies in whether, through the substance of data protection rights and their effective implementation, supervision and enforcement, the foreign system as a whole delivers the required level of protection.'[100] This appears to be in accordance with the CJEU's recently developed flexible approach when reviewing foreign law. Under this, the Court has fleshed out an amended test on the merits for assessing external surveillance interferences. This test requires that limitations to fundamental rights (i) must be provided for by law; (iii) their legal basis must itself define the scope of the limitation on the exercise of the right concerned; (iii) to satisfy the requirement of proportionality, the legislation in question must lay down clear and precise rules governing the scope and application of the relevant measures and impose 'minimum safeguards, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse'; and, (iv) the third country must provide 'effective and enforceable data subject rights' for persons whose personal data is transferred.[101]

Overall, the UK as third country comes from a starting point of close alignment with the EU that puts it at a clear advantageous position compared with other third countries with which the EU has or is pursuing data transfer agreements. As a commentator has noted 'the UK will have the strongest personal data relationship with the EU outside of the EEA and Switzerland.'[102]

---

[94] ECtHR (Chamber, First Section), Big Brother Watch and Others v the United Kingdom, *Big Brother Watch and others v. United Kingdom*, [2018] ECHR 722, para 265; ECtHR (Grand Chamber), *Big Brother Watch and others v. United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15, 25 May 2021 Grand Chamber, para 415.

[95] Bernard Keenan, 'The Evolution of Elucidation: The Snowden Cases Before The Investigatory Powers Tribunal' (2022) 85(4) *MLR* 906, 933.

[96] EBPB, Opinion 14/2021, para 25.

[97] See Savirimuthu and Tzanou (n 91), para 241 and references therein.

[98] Commission adequacy decision on GDPR (n 1), para 16.

[99] See Maria Tzanou, 'Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights' in Federico Fabbrini (et al.) (eds.) *Data Protection Beyond Borders Transatlantic Perspectives on Extraterritoriality and Sovereignty* (Hart Publishing, 2020).

[100] Commission adequacy decision on GDPR (n 1), para 4.

[101] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2020] ECLI:EU:C:2020:559 (*Schrems II*); Tzanou (n 101), 114. It should be noted that under this flexible approach, the CJEU avoids applying directly to external situations the analytical framework of Article 52(1) CFR. See also EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, para 24.

[102] David Erdos, 'The UK and the EU Personal Data Framework After Brexit: Another Switzerland?', Paper No. 15/2021, March 2021, 2 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3811296.

B. Brexit, national security and the extraterritorial application of EU fundamental rights

Data flows post-Brexit raise two main sets of issues concerning the interrelationship of national security and the extraterritorial application of EU fundamental rights: (a) the scope of review when national security is at stake; and (b) the extraterritorial application of EU fundamental rights in this context.

Both matters are closely interlinked but for the moment we will approach them separately before we point out their respective interconnections. First, the question of applicability of EU law in the context of national security measures in general and international data transfers in particular raises a number of issues. In *Privacy International*,[103] a seminal case decided after the Brexit referendum but before the UK's formal departure from the EU, on a preliminary reference question received by the IPT, the CJEU clarified once and for all an issue of particular importance to the UK (and all Member States): the applicability of EU law to domestic national security legislation.[104] The issue had arisen in several cases over the past few years,[105] with Member States insisting that intelligence services' activities relating to the maintenance of public order and the safeguarding of internal security and territorial integrity are part of their essential functions and, consequently, fall within their exclusive competence pursuant to Article 4(2) TEU.

The CJEU took the opportunity in *Privacy International* to put the debate to bed by introducing a fundamental distinction: national laws that require Electronic Communications Service Providers (ECSPs) to retain or grant access to data to national authorities for the purpose of safeguarding national security fall within the scope of the ePrivacy Directive and, therefore, the CFR and EU law more broadly.[106] By contrast, national laws that do not impose any obligations on ECSPs, but directly implement national security measures fall outside the scope of the ePrivacy Directive (and EU law) even if these derogate from the principle of confidentiality of electronic communications established in the ePrivacy Directive.[107] The crucial aspect of the distinction concerns the involvement of ECSPs and the allocation of data processing obligations to these.[108] Any obligations imposed on ECSPs trigger the application of the ePrivacy Directive no matter the purpose for the access to the data. If, however, the data is directly retained by national authorities without the compelled cooperation of ECSPs, the ePrivacy Directive is not applicable - in this case such measures must comply with national constitutional law requirements and the ECHR.

However, national security raises a particular paradoxical situation in the context of international data transfers. Pursuant to Article 4(2) TEU, national security remains the sole responsibility of each Member State but as clarified in *Privacy International*, Member States' national security measures do fall within the scope of EU law when personal data is retained by service providers. However, when assessing the adequacy of a third country, the Commission is obliged under Article 45(2)(a) to take account of 'the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, *including concerning public security*, *defence, national security* and criminal

---

[103] Case C-623/17 *Privacy International* v *Secretary of State for Foreign and Commonwealth Affairs and Others* ECLI:EU:C:2020:790.

[104] The Court defined national security as 'the primary interest in protecting the essential functions of the State and the fundamental interests of society [which] encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities.' See Joined Cases C 511/18, C 512/18 and C 520/18 *La Quadrature du Net and Others v Premier Ministre and Others* ECLI:EU:C:2020, para 135.

[105] *Tele2* (n 18)*;* Case C-207/16 *Ministerio Fiscal* ECLI:EU:C:2018:788.

[106] *Privacy International* (n 103), para 39.

[107] *La Quadrature du Net* (n 106), para 103. The Court recognised, however, that these rules may be subject to the application of the LED.

[108] Maria Tzanou and Spyridoula Karyda, 'Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga?' (2022) 28 (1) *European Public Law* 123.

law *and the access of public authorities to personal data*'.[109] Hence, the UK finds itself in an unusual position: if it still were an EU Member State it could in principle benefit from the exception under Article 4(2) TEU which, following *Privacy International*, it would allow it to avoid scrutiny of its national security framework -at least when data retention through service providers is not at stake-; but, ironically, by leaving the EU, as a third country, such scrutiny is unavoidable as the UK became subject of the GDPR's adequacy regime.[110]

In fact, in the 2021 Commission's decision on the adequate protection of personal data by the UK on the basis of the GDPR, the discussion on 'access and use of personal data transferred from the EU by public authorities in the UK' is longer that the actual analysis of the UK's general data protection regime spanning in over 57 pages[111] - while the discussion of the UK's overall data protection framework is actually found in only 31 pages.

Second, the application of EU fundamental rights raises interesting issues in the Brexit context – even more than before. Indeed, the use of EU fundamental rights to review domestic measures has always been 'controversial' in the UK.[112] This controversy had already commenced long before Brexit when the UK was still a Member State.[113] For instance, prior to the signing of the Lisbon Treaty, the UK government was eager to secure a protocol stating that the CFR did not 'extend' the ability of the CJEU to declare any UK practice or law invalid,[114] with the then UK Prime Minister declaring that he would 'not accept a treaty that allows the Charter of Fundamental Rights to change UK law in any way'.[115] After Brexit, unsurprisingly, the CFR ceased to have an independent existence in UK law[116] as well as to be relevant to the interpretation of other retained EU law or form part of UK law as it has not been classified as retained EU law.[117]

Yet, while the CFR is no longer applicable to the UK after its departure from the EU, the potential 'extraterritorial' application of the Charter in the context of international data transfers is still very much on the table. The dominant position seems to be that the Charter applies regardless of territorial criteria[118] - what matters is whether a situation is covered by an EU competence.[119] In international data transfers, said applicability derives from the Commission's powers to act in the context of adequacy decisions.[120] This approach is closely linked to the elevation of data protection to the level of a fundamental right that makes the EU's exercise of jurisdiction 'not just […] permissive

---

[109] Emphasis added.

[110] This paradox was not lost by commentators. For instance, see Edoardo Celeste, 'Data Protection', in Federico Fabbrini (ed), *The Law & Politics of Brexit. Volume 3. The Framework of Future EU- UK Relations* (OUP, 2021), 197, 209.

[111] From page 31 to page 88, from paragraph 112 to paragraph 272.

[112] See Damian Chalmers et al., 'European Union Law', Fourth edition, (CUP, 2019), 281; Andrew D. Murray, 'Data transfers between the EU and UK post Brexit?' (2017) *IDPL* 149.

[113] See House of Commons European Scrutiny Committee, *The Application of the EU Charter of Fundamental Rights in the UK: A State of Confusion*, 43rd Report, Session 2013-14, HC 979, 13.

[114] Protocol on the Application of the Charter to Poland and the United Kingdom, Art. 1(1).

[115] George Jones, 'Blair's EU safeguards "may not be watertight"', *The Telegraph,* 26 June 2007.

[116] EU Withdrawal Act 2018.

[117] See also Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ('DPPEC Regulations'). For a detailed analysis of the UK legal framework, see Savirimuthu and Tzanou (n 91).

[118] See among others Angela Ward, 'Article 51 - Field of Application' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights : A Commentary* (Hart Publishing 2014); Violeta Moreno-Lax and Cathryn Costello, 'The Extraterritorial Application of the EU Charter of Fundamental Rights: From Territoriality to Facticity, the Effectiveness Model' in Steve Peers and others (eds), *The EU Charter of Fundamental Rights : A Commentary* (Hart Publishing 2014); Eva Kassoti, 'The Extraterritorial Applicability of the EU Charter of Fundamental Rights : Some Reflections in the Aftermath of the Front Polisario Saga' (2020) 2 European journal of legal studies 117; Chiara Macchi, 'With Trade Comes Responsibility: The External Reach of the EU's Fundamental Rights Obligations' (2020) 11 Transnational Legal Theory 409.

[119] Moreno-Lax and Costello (n 119); Kassoti (n 119).

[120] On the basis of Article 16 TFEU and Article 45 GDPR.

(discretionary), but also mandatory'.[121] This means that transborder data flows could be regarded as part of the EU institutions' fundamental rights protective duty.'[122] It is now established case law that data subjects whose personal data are transferred to a third country should be afforded a level of protection 'essentially equivalent' to that guaranteed within the EU by 'the GDPR, *read in the light of the Charter*'.[123]

The UK, therefore, finds itself in a second paradoxical situation. While as an EU Member State it tried to secure an opt-out from the CFR, currently, as a third country it cannot escape the extraterritorial application of the CFR in the context of data transfers with the EU. In fact, the external, EU scrutiny of the UK legal framework on the basis of EU fundamental rights will intensify and focus mainly on the UK public authorities' access to personal data in the fields of law enforcement and national security, rather than the general data processing in the commercial context – where conversely the UK broadly aligns with the EU requirements.[124]

Thus, paradoxically, after Brexit, national security matters have become the rationale for an increased EU review of the UK legal framework in the context of transborder data transfers and the main venue of the extraterritorial application of EU fundamental rights through potential legal challenges.[125] Regrettably, this leaves UK citizens (and EU citizens residing in the UK) in a 'zero-sum game'[126]: after the UK's departure from the EU, there is no longer a fundamental right to data protection in the UK[127] and the potential extraterritorial application of the CFR will be primarily relevant in the fields of law enforcement and national security, but not in general, 'everyday' data processing situations.

C. Persisting issues of the UK's national security regime

The IPA 2016 poses two main problems in the context of international data transfers: (a) the bulk metadata data surveillance; and (b) the bulk interception of communications.[128] Both issues have been identified as problematic in the CJEU's case law concerning international data transfers making the fate of the Commission's adequacy decision on the UK uncertain.

A first problem concerns the 'bulk acquisition of metadata' under the IPA 2016.[129] Such bulk acquisition covers data that is collected by telecommunication operators in the United Kingdom directly from the users of telecommunication services. There is no official definition of 'bulk powers' under UK law, but these are understood to include 'the collection and retention of large quantities of data acquired by the Government through various means (i.e. the powers of bulk interception, bulk acquisition, bulk equipment interference and bulk personal dataset acquisition and which can subsequently be accessed

---

[121] Cedric Ryngaert and Mistale Taylor, 'Symposium on the GDPR and International Law: The GDPR as Global Data Protection Regulation ?' (2019) *AJIL Unbound* 5, 6.

[122] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press, 2013) , 129–33.

[123] *Schrems II* (n 101), paras 101, 104-105. Emphasis added.

[124] Savirimuthu and Tzanou (n 91).

[125] This point was made by the House of Lords EU Committee in its report 'Beyond Brexit: policing, law enforcement and security' (March 2021) https://committees.parliament.uk/publications/5298/documents/52902/default/, which noted that 'now that the UK is a third country it will be held to higher standards by the EU in respect of data protection… it will no longer be able to benefit from the national security exemption in the EU Treaties' and 'there is abundant scope for legal challenge on data protection grounds'.

[126] Murray (n 113).

[127] Article 8 EUCFR. See Maria Tzanou, The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance (Hart Publishing, 2017).

[128] A further problem concerns the sharing of UK intelligence data with the Five Eyes countries agencies (US, Canada, New Zealand, Australia). See European Parliament, 'The adequate protection of personal data by the United Kingdom', European Parliament resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom (2021/2594(RSP)), P9_TA(2021)0262, para 16(d).

[129] Chapter 2 of Part 6 of the IPA 2016.

by the authorities.'[130] This could come within the CJEU's definition of 'generalised and indiscriminate' data retention that the CJEU found to be incompatible with the CFR in *Privacy International* and, therefore, prohibited under EU law even if required by intelligence agencies for national security purposes.[131]

The Commission in its adequacy decision attempted to clarify that 'bulk power' 'does not equate to "mass surveillance".[132] More specifically, it drew a distinction between bulk powers which 'incorporate limitations and safeguards designed to ensure that access to data is not given on an indiscriminate or unjustified basis' and 'mass surveillance' undertaken without conditions or safeguards.[133] Pursuant to this, bulk powers in the UK: i) can only be used 'if a link is established between the technical measure that a national intelligence agency intends to use and the operational objective for which such measure is requested';[134] ii) are available to intelligence agencies only;[135] iii) are subject to a warrant issued by the Secretary of State and approved by a Judicial Commissioner;[136] and, iv) in choosing the means to collect intelligence, 'regards must be given to whether the objective in question can be sought by "less intrusive means"' building on the principles of proportionality and necessity and prioritising targeted over bulk collection.[137] Nevertheless, as it was noted above, this Labour suggested provision is generally regarded as toothless as its binding effect is dubious.

Yet, notwithstanding that the IPA 2016 provides for certain safeguards, including the 'double-lock procedure', the Commission seems to be walking on a tightrope here as the peremptory rule of the CJEU is that bulk data retention is prohibited in general - even when undertaken by intelligence authorities. The CJEU has only allowed in *La Quadrature du Net* a general, indiscriminate preventive data retention when Member States are confronted with a 'serious' threat to national security 'which is shown to be genuine and present or foreseeable'.[138] This is permitted for a limited period of time which is strictly necessary and cannot exceed a foreseeable period;[139] and is subject to limitations and strict safeguards that protect effectively the personal data of the persons concerned against the risk of abuse.[140] However, under the IPA 2016, bulk surveillance is not exceptional as permitted in *La Quadrature du Net*; instead, it entails general bulk powers of intelligence agencies, which are not depended on a particular serious threat or time-limited. Furthermore, the limitations on the use of intelligence services 'bulk powers' are not defined in the law itself - as required by the CJEU -[141] but they are instead left to the discretion of the Secretary of State subject to review by the Information Commissioner.[142] It seems, therefore, that the Commission has chosen to ignore the CJEU's data retention red lines in its adequacy decision concerning the UK.[143] Nevertheless, we argue that these are

---

[130] Commission adequacy decision on GDPR (n 1), para 216.
[131] *Privacy International* (n 103), para 81.
[132] Commission adequacy decision on GDPR (n 1), para 216.
[133] Ibid.
[134] Ibid, para 217.
[135] Ibid.
[136] Ibid.
[137] Ibid.
[138] *La Quadrature du Net* (n 106), para 136.
[139] Ibid, paras 137 & 138.
[140] Ibid, para 138.
[141] See *Schrems II* (n 101).
[142] See European Parliament resolution on the adequate protection of personal data by the UK, para 16 (b); Douwe Korff and Ian Brown, 'The inadequacy of UK data protection law: Executive Summary', Data protection and digital competition blog, 30. 11. 2020 < https://www.ianbrown.tech/wp-content/uploads/2020/11/Korff-Brown-Submission-to-EU-re-UK-adequacy-ExecSumm-DK-IB201130.pdf>, 6.
[143] Tzanou and Karyda (n 109). See also EDPB, 'Adequacy Referential', WP 254 rev. 01 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

not going to magically disappear because some procedures and limitations exist in the IPA 2016. Legal challenges to the Commission's adequacy decisions on this basis might, therefore, be expected in the future, especially if we experience a hardening of the UK's stance on these matters.

The second issue concerns the 'bulk interception' carried out by UK intelligence services.[144] This refers to 'the interception of communications in the course of their transmission sent or received by individuals who are outside the British Islands'.[145] For example, the Government Communications Headquarters' (GCHQ) 'Tempora' programme, which was mentioned in the Snowden revelations, intercepts communications in real time through fibre-optical internet backbone cables, and allows for processing of the data at a later stage.[146]

Such bulk interception includes both the *content* of communications as well as *metadata* and is capable of capturing EU originating data, which are considered 'overseas-related communications'.[147] Access to the content of communications, however, constitutes a breach of the 'essence' of the right to privacy, according to established CJEU case law.[148] The CJEU first indicated this in *Digital Rights Ireland*,[149] and went on to hold in *Schrems I* - a case that concerned international data transfers to the US - that the essence of the fundamental right to privacy was violated because the US mass online surveillance programmes granted access on a generalised basis not only to communications metadata but to the actual *content* of electronic communications.[150] This pronouncement of the Court sets out another red line the Commission seemed to ignore in its UK adequacy decision, focusing instead on the different safeguards applicable to bulk interception.[151]

IV. Conclusion

As George Eliot stated 'among all forms of mistake, prophecy is the most gratuitous'.[152] Nevertheless, two main conclusions arise from the study of the UK's political landscape in the context of national security, and law enforcement more broadly. First, bulk surveillance powers are here to stay. They are long rooted in the UK's socio-political environment, they reflect a basic consensus between the two main parties and, thus, appear irreversible.

Second, the issues related to these powers highlighted in the previous section are the UK's main vulnerabilities in the context of its data protection relations with the EU post-Brexit. Bulk powers and access to the content of intercepted communications constitute red lines for the CJEU and, thus, make the Commission's UK adequacy decision – which has not been yet scrutinised by the CJEU - a ticking 'timebomb'.[153] They also demonstrate that the Commission opted for a *proceduralised* approach to UK bulk surveillance that fails to pay due attention to substantive requirements, including several CJEU's prohibitive rules.[154] Admittedly, the UK is no longer directly subject to the CJEU's jurisprudence, falling rather under the more permissive case law of the ECtHR, which has found bulk surveillance to comply with the Convention if it is subject to specific conditions and safeguards.[155]

---

[144] Section 136 of the IPA 2016.
[145] Commission adequacy decision on GDPR (n 1), para 219.
[146] See European Parliament resolution on the adequate protection of personal data by the UK, para 12.
[147] Ibid.
[148] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650 (Schrems I), para 94.
[149] *Digital Rights Ireland* (n 13).
[150] *Schrems I*, para 94.
[151] See Commission adequacy decision on GDPR (n 1), para 218 ff.
[152] Part 1, Ch. 10, Middlemarch 1872
[153] See also Celeste (n 111), 214.
[154] See Tzanou and Karyda (109).
[155] See ECtHR (Grand Chamber), *Big Brother Watch and others v United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15, 25 May 2021, para 323; Tzanou and Karyda (n 109) and discussion therein.

Nonetheless, it is safe to say that these problems are not going to disappear any time soon, making the EU-UK data privacy space even more uncertain - a characteristic of the EU-UK post-Brexit relations in general.