Douwe Korff & Ian Brown

The inadequacy of UK data protection law in general and in view of UK surveillance laws

with some comments on the adequacy decisions on Guernsey, Jersey and the Isle of Man & on the implications for other countries and territories including Gibraltar & EU Member States

PART TWO: UK SURVEILLANCE

The second part of a two-part submission to the European Union bodies assessing whether under the EU General Data Protection Regulation the United Kingdom should be held to provide "adequate" protection to personal data.

Cambridge/London, UK

30 November 2020

Douwe Korff & Ian Brown

The inadequacy of UK data protection law – Part Two: UK surveillance

About the authors:

Douwe Korff is Emeritus Professor of International Law at London Metropolitan University and an Associate of the Oxford Martin School of the University of Oxford, a Visiting Fellow at Yale University (Information Society Project), and a Fellow at the Centre for Internet and Human Rights of the European University of Viadrina, Berlin. Among many other publications, he wrote the Council of Europe Commissioner for Human Rights' *Issue Paper* on The Rule of Law on the Internet and in the wider digital environment (2014), available at: https://rm.coe.int/ref/CommDH/IssuePaper(2014)1. He was also the lead author (with Ben Wagner, Julia Powles, Renata Avila and Ulf Buermeyer) of Boundaries of Law: Exploring Transparency, Accountability, and Oversight of Government Surveillance Regimes, comparative report covering Colombia, DR Congo, Egypt, France, Germany, India, Kenya, Myanmar, Pakistan, Russia, South Africa, Turkey, UK, USA, prepared for the World Wide Web Foundation (2017), available at: https://ssrn.com/abstract=2894490

Website: http://douwe.korff.co.uk

Ian Brown is visiting CyberBRICS professor at Fundação Getulio Vargas (FGV) Law School in Rio de Janeiro, and an ACM Distinguished Scientist. He was previously Principal Scientific Officer at the UK government's Department for Digital, Culture, Media and Sport; Professor of Information Security and Privacy at the University of Oxford's Internet Institute; and a Knowledge Exchange Fellow with the Commonwealth Secretariat and UK National Crime Agency. His books include Cybersecurity for Elections (2020, Commonwealth Secretariat, with Marsden/Lee/Veale), Regulating Code (2013, MIT Press, with Marsden), and Research Handbook on Governance of the Internet (ed., 2013, Edward Elgar). He co-founded and served on the boards of European Digital Rights, Open Rights Group, the Foundation for Information Policy Research and Privacy International; and has written for The Financial Times and The Guardian. He is a fellow of the British Computing Society, Open Forum Europe, and the International University of Japan.

Website: https://www.ianbrown.tech/about/

Douwe Korff & Ian Brown were the joint authors of Terrorism and the Proportionality of Internet Surveillance, European Journal of Criminology, March 2009, available at: SSRN: http://ssrn.com/abstract=1261194

Both have testified as experts on surveillance or surveillance law to various bodies including (between them) the Parliamentary Assembly of the Council of Europe (PACE), the European Parliament (LIBE Committee) and national parliaments including the German *Bundestag* and the UK House of Lords.

Acknowledgments:

The authors are grateful to **Eric King** and **Jim Killock** for helpful insights into the UK legal regimes relating to mass surveillance and bulk data collection.

We are also happy to acknowledge our reliance in several respects on the excellent analyses by **Chris Pounder** and **Graham Smith** in their blog entries at:
http://www.amberhawk.com/ (Chris Pounder)
http://www.cyberleagle.com/ (Graham Smith)

All errors of course remain solely ours.

CONTENTS OF PART TWO:

- o – O – o -

1. Introduction to Part Two

As explained in Part One, under Chapter V of the EU's General Data Protection Regulation (GDPR) personal data can only flow freely from the EU and the European Economic Area (EEA) to any non-EU/EEA country ("third country") if that third country has been held by the European Commission to provide "adequate" protection to the transferred data;[1] and the Court of Justice of the EU (CJEU) has held, in its *Schrems I* judgment, that this means the third country in question must provide "essentially equivalent" protection to that accorded in the EU by the GDPR, read in the light of the EU Charter of Fundamental Rights (CFR).[2] This is reflected in the Article 29 Working Party's "Adequacy Referential" adopted in November 2017 and endorsed by the European Data Protection Board in May 2018.[3]

Moreover, as also already noted there, the GDPR expressly stipulates that any adequacy assessment must include an assessment of:

> **the rule of law [and] respect for human rights and fundamental freedoms** [in the third country in question, including] relevant legislation, both general and sectoral, including concerning public security, defence, **national security** and criminal law and **the access of public authorities to personal data**, as well as the **implementation** of such legislation.
>
> (Article 45(2)(a), emphases added)

More specifically, the assessment must include an assessment of whether the rules and practices relating to **access to personal data transferred from the EU by a third country's intelligence agencies** are compatible with the rule of law and fundamental rights – again, as interpreted in the light of the Charter.

In its *Schrems II* judgment, discussed in section 3, below, the Court of Justice held that the laws and practices of the USA, under which the US National Security Agency (NSA) could gain access to EU personal data after transfer to the USA was insufficiently limited and that EU persons did not have access to appropriate remedies in relation to excessively wide access. The Court therefore held that the USA did not provide "adequate"/"essentially equivalent" protection to personal data on EU persons, and that a decision of the European Commission to the contrary was therefore invalid.

Also to be addressed in the context of an adequacy assessment are the "rules for the **onward transfer** of personal data to another third country" (also Article 45(2)(a)). More specifically, "the level of protection of natural persons ensured in the Union by this Regulation [the GDPR]" must not be "undermined" by such onward transfers (Article 44 and Recital 101).

In this Part Two of our submission, we assess the laws and practices of the UK's surveillance activities in this light. In section 2, we **describe** those activities (including the cooperation of the UK agencies with their US and other countries' counterparts in this regard, and the onward transfers of data that this involves). In section 3, sub-section 3.1, we **summarise the standards** against which those laws and practices must be assessed, as set out in European case-law and the recent "European Essential Guarantees for surveillance", and note **two further issues**: whether, if the UK is not held to provide adequate protection, its extraction of

---

1 See Part One, section 2. Hereafter, we will simply refer to the "EU"; this should be read as also encompassing the EEA.

2 See Part One, Introduction, footnote 3.

3 See Part One, section 2.1.

data on EU communications amounts to a personal data breach – as we will argue it does; and whether the UK (and the US) intelligence agencies' actions in this regard can be said to constitute "monitoring of [the] behaviour [of data subjects in the EU] as far as their behaviour takes place within the Union" in terms of Article 3(2)(b) GDPR – and whether this means that those agencies are therefore subject to the GDPR (and liable to sanctions and fines under the GDPR).

We then, in sub-section 3.2, **assess** the UK surveillance laws and practices against the EU standards. We conclude (in sub-section 3.3) that the UK's surveillance laws and practices do not meet the EU standards, and that therefore the UK should not be held to provide "adequate"/"essentially equivalent" protection compared to that accorded by EU law.

We discuss the **implications** of a decision not to declare the UK to be a third country that provides adequate protection for EU – UK personal data flows after the end of the post-Brexit transition period on 31 December 2020 in a separate section in the Executive Summary.

There, we also briefly note the implications of such a (negative) decision for:

- the UK itself;
- the other "British Islands" (Guernsey, the Isle of Man and Jersey) and for Gibraltar;
- the other "5EYES" (and other countries that indulge in mass surveillance);

and, not least:

- the implications for EU Member States.

The Executive Summary of both parts of our submission is provided with this Part Two.

Note:

Neither Part One of our submission nor the present Part Two deals with the question of whether the UK should be held to provide adequate protection to personal data transferred to it from the EU for law enforcement purposes (including in relation to access by the UK law enforcement agencies to the relevant EU databases and bodies). This is a separate issue, to be addressed under the Law Enforcement Directive. Although that directive is based on the same principles as the GDPR and like the GDPR must be read in the light of the Charter, the assessment is distinct – and we therefore leave it to others to comment on that issue (although of course there are links to our assessments).[4] Suffice it to note here that in this respect, too, serious issues have been raised that stand in the way of an LED adequacy decision.

- o – O – o -

[4] For a recent analysis, see: Centre for European Reform, *Brexit and Police and Judicial Co-Operation: Too Little, Too Late?*, Insight by Camino Mortera-Martinez, 9 November 2020, available at: https://www.cer.eu/insights/brexit-and-police-and-judicial-co-operation-too-little-too-late

2. UK surveillance

2.1 Overview

In this section, we will show the following:

- The UK's intelligence agencies, and more in particular the UK's Government Communications Headquarters (GCHQ), collect data from selected "bearers" in the transatlantic Internet cables, in bulk, in a generalised and indiscriminate manner. The UK's IAs also have legal powers to demand access to data of communication service providers (CSPs) and Internet Service Providers (ISPs) within the UK's jurisdiction in bulk, including through "back doors" into the systems of such providers. The bulk data includes data on individuals in the remaining 27 EU Member States ("EU persons").
- The UK's agencies do not only filter the bulk data to identify data relating to "known" persons of interest – in particular, persons already linked in some way to terrorism – but also analyse the bulk data to single out, by means of artificial intelligence (AI)/algorithmic/Big Data analysis of the bulk data, persons in relation to whom there was no such previous link but who the data suggests could possibly or probably be terrorists or linked to terrorism (or other threats to national security).
- In the above-mentioned activities, the UK agencies, in particular GCHQ, collaborates extremely closely with the USA's National Security Agency (NSA): to a large degree, the data, the analyses of the data, and the results of the data are treated as belonging to both agencies and are shared by them across the Atlantic.

In sub-sections 2.2 – 2.4, we describe these matters in further detail. In section 3, we assess the compatibility of the activities and of the legal regimes under which they take place with the requirements of the European Convention on Human Rights (ECHR) and the EU Charter of Fundamental Rights, as reflected in the EDPB's "European Essential Guarantees" for surveillance. Our conclusions are summarised in sub-section 3.3. The implications are discussed in the Executive Summary.

2.2 Bulk interception of communications data by GCHQ

2.2.1 Background

Since at least the (first) Elizabethan era,[5] the UK government has practised surveillance, in particular the obtaining of postal and then "signals intelligence" (SIGINT), in secret and outside of any acknowledged legal framework – as the relevant agencies' traditional name, "clandestine services" already indicates. As Field Marshall Montgomery put it in his seminal work on the history of warfare:[6]

> In all secret service activities, which are handled by the central government, the operations of spies, saboteurs and secret agents generally are regarded as outside the scope of national and international law. They are therefore anathema to all accepted standards of conduct.

[5] "Sir Francis Walsingham, the Spymaster, managed the complex system, which included stations in most European countries, and hired the spies and special agents for the Queen." See Natalie Zarrelli, Queen Elizabeth I's Vast Spy Network Was The First Surveillance State, Atlas Obscura, 7 December 2016.

[6] Field Marshal Montgomery of Alamein, A History of Warfare, new edition by Jane's, 1982, p. 17.

At the international level, only very recently, following the Snowden revelations noted below, are some tentative steps being taken to adopt an international-legal framework for such agencies.[7]

Consequently, even the very existence of the Government Communications Headquarters, GCHQ, responsible for this activity since 1919,[8] was only exposed, in *Time Out* magazine, by investigative journalists Duncan Campbell and Mark Hosenball in 1976.[9] GCHQ (and the Secret Intelligence Service/MI6) were only placed on a statutory footing in 1994, under the Intelligence Services Act of that year (with the Security Service/MI5 put on a statutory basis by the Security Service Act in 1989).

Documents leaked by NSA contractor, Edward Snowden, in 2013 showed GCHQ, in a joint programme with the US NSA called "TEMPORA", "collect[ed] and store[d] vast quantities of global email messages, Facebook posts, internet histories and calls" by tapping into "the network of cables which carry the world's phone calls and internet traffic"; and that it shared those data with NSA.[10] Central to these activities was – and is – a GCHQ facility in Bude, in the south-west of England, from where those cables can be accessed.

The outlines of these activities were subsequently confirmed in a 2015 report by the House of Commons Intelligence and Security Committee (ISC) (to which we refer for fuller details).[11]

2.2.2 Indiscriminate collection in bulk

i. What is collected and how?[12]

The UK and USA intelligence agencies, alongside the other three members of the "Five Eyes" intelligence alliance (Canada, Australia and New Zealand) have access to Internet cables around the world, mainly through secret arrangements with companies owning part of the

---

[7] Cf. the suggestion by a former head of the German external intelligence service, the *Bundesnachrichten-dienst* (BND), Mr Hansjörg Geiger, that an "intelligence codex" be adopted at the international level to cover the activities of national security agencies. See section 5.2 (paras. 115 – 118) of the Explanatory Memorandum by Mr Omtzigt, the rapporteur of the Parliamentary Assembly of the Council of Europe (PACE) on mass surveillance, attached to PACE Resolution 2045(2015) on Mass surveillance, adopted on 21 April 2015, available at: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=21583&lang=en
The text of the recommendation itself can be found here: http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=21692&lang=en

[8] GCHQ marks 100 years by unveiling details of wartime spy work, The Guardian, 1 November 2019, available at https://www.theguardian.com/uk-news/2019/nov/01/gchq-marks-100-years-by-unveiling-details-of-wartime-spy-work

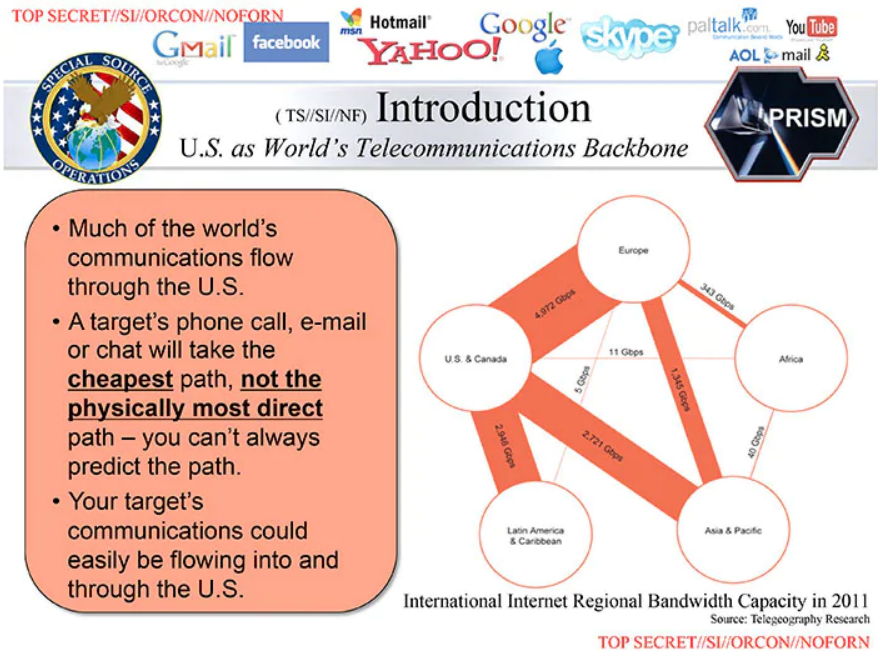
[9] See: https://www.duncancampbell.org/PDF/1976-may-time-out-the-eavesdroppers.pdf
Hosenball, who was an American national, was deported for "*[having] sought to obtain and [having] obtained for publication, information harmful to the security of the United Kingdom*". See: http://www.uniset.ca/other/css/hosenball.html

[10] *GCHQ taps fibre-optic cables for secret access to world's communications*, The Guardian, 21 June 2013, available at: https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa
On the close cooperation between the UK and the USA in this regard, see sub-section 2.4.2, below.

[11] UK House of Commons' Intelligence and Security Committee, Privacy and Security: A modern and transparent legal framework (HC 1075), 12 March 2015 (hereafter, "**the ISC Report**"),available at: http://isc.independent.gov.uk/news-archive/12march2015

[12] For further details than can be provided in this brief submission, see Open Rights Group, Collect It All: GCHQ and mass surveillance, 2015 ("**the ORG report**"), available at: https://www.openrightsgroup.org/publications/collect-it-all/
In particular Part One, Chapter One, *Passive Collection*, available separately at: https://www.openrightsgroup.org/app/uploads/2020/03/01-Part_One_Chapter_One-Passive_Collection.pdf

Internet infrastructure, or that have access to it.[13] This includes access to cables with communications to and from EU countries including France, Germany, Ireland, the Netherlands, Spain and Portugal.[14] In fact, as this US NSA "Top Secret" slides noted, "much of the world's communications flow through the US"; the USA provides the "World's Telecommunications Backbone" – and access to these flows, to this backbone, is gained in joined operations between the "Five Eyes" (see below, at 2.4).



Source: https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

Much if not most of the communications of EU persons, *to anywhere in the world*, will flow through communications systems to which the USA and the UK intelligence agencies have access.

In spite of an earlier ambition of the US NSA to "*Collect It All*",[15] in practice the NSA and GCHQ have to be selective about what data they collect, and from what sources (although their capacity is still enormous).[16]

---

13 ORG report (previous footnote), Part One, Chapter One, pp. 2 – 3. For a further detailed analysis of the U.K. practice of bulk cable interception, see Center for Democracy & Technology (CDT), Not a Secret: bulk interception practices of intelligence agencies, ("**the CDT report**") available at: https://cdt.org/insights/not-a-secret-bulk-interception-practices-of-intelligence-agencies/
This excellent report, by Eric King, "considers the historical background to bulk cable interception, the legal regime underpinning modern day practice, and recounts chronologically the U.K.'s gradual official confirmation of its bulk cable interception capabilities. Analysis of the official confirmed bulk interception process is then undertaken, reviewing how the U.K. system undertakes bearer selection, filtering, automatic selection for examination, and examination by human analysts."

14 See the image on p. 4 of Part One, Chapter One, of the ORG report.

15 "*In the summer of 2008, Gen. Keith Alexander, the recently resigned director of the National Security Agency, posed an audacious question to intelligence analysts at the Menwith Hill eavesdropping station in North Yorkshire, in the United Kingdom: 'Why can't we collect all the signals all the time?*'" See: https://www.thedailybeast.com/the-nsa-can-collect-it-all-but-what-will-it-do-with-our-data-next

16 "*The documents show that GCHQ has secret agreements with companies providing at least 114 access points to 63 undersea cables or landing stations. … In 2010 GCHQ was able to access 592 channels of 10 Gigabits*

In particular, they select for direct access bearers within the transatlantic cables[17] that land in Cornwall, UK (and other places around the world where they have facilities, such as Malta, Japan, the Caribbean and Oman),[18] those that appear to offer the most valuable intelligence, e.g., because they carry substantial amounts of data from global trouble spots, or from where there are significant numbers of jihadists or other terrorists.[19] But it appears that in practice there are not always links to such obvious, legitimate targets (see below).

In the UK, the warrants under which bulk interception takes place must state the "operational purpose" of the warrant, i.e., of the reason for selecting a particular bearer. But the list of operational purposes is not public.[20] The UK Government gives as an example, "attack planning by ISIL in Syria against the U.K."[21] But the specification need not be that precise; it merely needs to be more specific than the very broadly-phrased statutory purposes of "*the interests of national security or the purpose of preventing or detecting serious crime, or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security*". That is not so different from the US definition of "foreign intelligence information" in the Foreign Intelligence Surveillance Act (FISA) under which the UK's partner, the USA, carries out its global surveillance: such information ("FII") includes "*information with respect to a foreign power or foreign territory that relates to the national defense, national security, or conduct of foreign affairs of the United States.*"[22]

---

per second each, and could egress (send home for analysis) around a tenth of that capacity. GCHQ hopes to more than treble that capacity in the future." ORG report, p. 4. This includes hundreds of millions of "telephone events" daily (600 million each day in 2012) (*idem*, p. 3). Cf. CDT report (footnote 13, above), fn. 18 on p. 9 for further details.

[17] A "bearer" can be a fibre within a cable, or indeed an optical channel within a fibre. For a detailed description, see the ISC Report (footnote 5, above), footnote 48 (to para. 55).

[18] See the ORG report (footnote 12, above), section 1.2, Collaboration with companies to tap international optic cables, on pp. 2 – 4, with reference to this chart:
https://edwardsnowden.com/wp-content/uploads/2014/11/partner_cables.pdf

[19] The ISC report (footnote 5, above) is not very specific in this regard, and partly redacted. It says, in relation to the second part of the programme (as discussed below, at 2.3.2.i, below), that: "*[The selected bearers] are not chosen at random: they are deliberately targeted as those most likely to carry communications of intelligence interest. (For example, GCHQ are currently targeting bearers likely to be carrying communications of ***.)*" (para. 66, original redaction).

[20] This means that the limitation on the use of the warrants are not set out in the legislation itself – which is one of the essential requirements of EU law. See sections 3 an 4, below.

[21] "Factsheet - Bulk Interception," U.K. Government (2015) available at:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/473751/Factsheet-Bulk_Interception.pdf (cited in CDT report [footnote 13, above], fn. 48).

[22] 50 U.S. Code § 1801 – Definitions, section (e):

(e) "Foreign intelligence information" means—

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

In practice, the US's NSA has used its mass surveillance powers to obtain information on political targets (such as the EU or even NATO allies)[23] including salacious information that could be used to put pressure on individuals in diplomatic relations,[24] and bulk access to financial data.[25] Reportedly, the NSA also cooperated with European countries in carrying out military-industrial espionage on allies.[26] We fear that the words "*interests [that are] relevant to the interests of national security*" can easily be stretched to also cover such overreach, and note the extremely close (hand-in-glove) relationship between the USA and the UK in these activities, as discussed below, at 2.4.

ii. Is it targeted or indiscriminate?

As Eric King points out:[27]

> There are a number of different terms to describe such collection practices, each with contested definitions. Terms like mass surveillance, bulk collection, and targeted or untargeted interception all have different meanings to different stakeholders in different countries, and there isn't yet a common lexicon. This report will use the terms bulk collection and bulk interception interchangeably, following the loose definition provided by the US National Academy of Sciences.

This is as follows:[28]

> If a significant portion of the data collected is not associated with current targets, it is bulk collection; otherwise, it is targeted. There is no precise definition of bulk collection, but rather a continuum, with no bright line separating bulk from targeted.

---

[23] Cf. *Attacks from America: NSA Spied on European Union Offices*, Spiegel International, 29 June 2013, available at:
https://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html

[24] Alfred McCoy, *Surveillance and Scandal*, Monthly Review, 1 July 2014, available at:
http://monthlyreview.org/2014/07/01/surveillance-and-scandal/

[25] Cf. *SWIFT Suspension? EU Parliament Furious about NSA Bank Spying*, Spiegel International, 18 September 2013, available at:
https://www.spiegel.de/international/europe/nsa-spying-european-parliamentarians-call-for-swift-suspension-a-922920.html

[26] See: *Hemmelige rapporter: USA spionerede mod danske ministerier og forsvarsindustri*, (Secret reports: The United States spied on Danish ministries and the defense industry), based on a whistleblower report that the US NSA cooperated with the Danish secret service to access underseas communication cables, to spy on various European countries including Norway, Sweden, Germany, France and the Netherlands, DR, 15 November 2020, available at:
https://www.dr.dk/nyheder/indland/hemmelige-rapporter-usa-spionerede-mod-danske-ministerier-og-forsvarsindustri
Also a related report with details of military-industrial espionage through this cooperation*: Kilder: NSA snagede i det danske milliardindkøb af kampfly* (Sources: NSA spied into the Danish billion-dollar purchase of fighter jets), DR, 15 November 2020, available at:
https://www.dr.dk/nyheder/indland/kilder-nsa-snagede-i-det-danske-milliardindkoeb-af-kampfly
As reported in the Netherlands with suggestions of similar cooperation there: *Amerikaanse NSA bespioneert Europese bondgenoten, waaronder Nederland* (America's NSA spies on European allies including the Netherlands), Volkskrant, 15 November 2020, available at:
https://www.volkskrant.nl/nieuws-achtergrond/amerikaanse-nsa-bespioneert-europese-bondgenoten-waaronder-nederland~bdbcdfe4/ ($)

[27] CDT report (footnote 13, above), p. 5.

[28] Summary, Bulk Collection of Signals Intelligence: Technical Options, National Academy of Sciences, 2015, available at:
http://nap.edu/19414

> The committee acknowledges that use of the word "significant" makes its definition imprecise as well.

We use the term "bulk collection" in the same way.

The UK Government suggests that the data collecting is "targeted", and the UK Parliament's Intelligence and Security Committee (ISC) also concluded that there was no "*ubiquity of surveillance*" and that "*GCHQ cannot conduct indiscriminate blanket interception of all communications*" (read: of all communications over the entire global Internet). The committee added that "*[i]t would be unlawful for them to do so, since it would not be necessary or proportionate, as required by RIPA [now the IPA].*"[29]

However, it should be stressed that when the agencies tap into a selected bearer, they (at that time) screen <u>all</u> the data that flow through that bearer, <u>indiscriminately</u>, <u>in bulk</u>.

As Eric King puts it:

> Once bearers are selected or accessed, then a copy of everything flowing through it is collected including communications and associated communications data.

In this, he quotes the UK Government's own observations (submissions) to the European Court of Human Rights, which acknowledged:

> In practical terms, "accessing" means making a copy of the communications and associated communications data flowing down the bearer.[30]

There is some deliberate obfuscation here. The ISC says that some filtering takes place *at the selected bearer*:[31]

> One of the major processing systems operates on all those bearers which GCHQ have chosen to access (approximately ***) out of those they can theoretically access. **<u>As the internet traffic flows along those chosen bearers</u> (***), the system compares the traffic against a list of specific 'simple selectors' (these are specific identifiers – *** – relating to a target).** GCHQ currently have approximately *** such selectors, relating to approximately *** individual targets.
>
> ***
>
> **Any communications which match the specific 'simple selectors' are automatically collected. All other communications are automatically discarded.**

However, the latter statement is immediately qualified, albeit in a footnote:[32]

> **GCHQ also collect <u>all</u> the Communications Data associated with these communications (described as 'Related Communications Data' in RIPA) before extracting that which is most likely to be of intelligence value.**

The ISC Report refers to RIPA as "defin[ing] CD as the basic 'who, when and where' of a communication" (para. 136). This broadly corresponds to "traffic and location data" as

---

29 ISC report (footnote 11, above), para. 58.

30 U.K. Observations to the European Court of Human Rights in the *Big Brother Watch* case, May 2019, quoted in CDT report (footnote 13, above), footnote 65.

31 ISC report (footnote 11, above), paras. 61 – 63. The asterisks indicate redactions from the full report, noting information that was excluded from the public version. That includes all of paragraph 62. Emphases added.

32 *Idem*, footnote 56 (to para. 63)

defined in EU law (although apparently, Related CD can also contain some elements of content).[33]

The bulk extraction and retention of such communications data is also confirmed in a later section of the report:[34]

> **Related CD (RCD) from interception:** GCHQ's principal source of CD is as a by-product of their interception activities, i.e. **when GCHQ intercept a bearer, they extract all CD from that bearer.** This is known as 'Related CD'. **GCHQ extract all the RCD from all the bearers they access through their bulk interception capabilities.**

This summary paragraph on the issue is therefore misleading:[35]

> **It has been suggested that GCHQ's bulk interception is indiscriminate. However, one of the major processes by which GCHQ conduct bulk interception is targeted. GCHQ first choose the bearers to access (a small proportion of those they can theoretically access) and then use specific selectors, related to individual targets, in order to collect communications from those bearers. This interception process does not therefore collect communications indiscriminately.**

This is only true if the words "collect[ing] communications" are read as only referring to the **content** of communications.

The UK NGO *Open Rights Group* (ORG), which has studied the system in detail on the basis of available official and leaked documents, describes the process, in particular in relation to the TEMPORA program exposed by Edward Snowden, as follows:[36]

> **TEMPORA: making the Internet manageable**
>
> …
>
> The latest development in bulk collection and processing in the UK is called TEMPORA, and brings Big Data technologies to state surveillance. Since the 1990s most communications, including voice calls, have moved to submarine cables and many to the Internet.
>
> The system was launched in 2011 after several years of trials that started in 2008, and it is a joint effort of several GCHQ programmes, including Mastering the Internet (MTE) and Global Telecoms Exploitations (GTE).The TEMPORA system has been described as a time machine that can "slow down the Internet" to better allow the

---

33 "Traffic data" are defined in EU law as "*any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof*"; and "location data" are defined as "*any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service*" (e-Privacy Directive 2002/58/EC, Article 3(b and (c))). They include times and length of a communication as well as telephone numbers, IP addresses (which can indicate the user and the likely geographical location) and websites accessed.

34 *Idem*, para. 134, at (iii), Bold title original; other emphases added.

35 *Idem*, para. 64, original emphasis in bold, underlining added.

36 Open Rights Group (ORG), GCHQ and UK Mass Surveillance, Part One, Chapter One, *Passive Collection*, section 1.3, *TEMPORA: making the Internet manageable*, and sub-section 1.3.1, *Access and collection*. Underlining of main headings, bold emphasis of sub-headings and core terms, and text in square brackets added. Available at:
https://www.openrightsgroup.org/app/uploads/2020/03/01-Part_One_Chapter_One-Passive_Collection.pdf
Further details are provided in CDT report (footnote 13, above), pp. 5 – 14 (general technical information on interception) and pp. 14 – 25 (the specific UK actions). We have added to the ORG descriptions quoted in the text cross-references to the sections in the CDT report in which Eric King discusses the same matters.

agency to sift through the information. **TEMPORA does this by storing a few days of almost unfiltered Internet data, effectively creating an "Internet buffer".**

According to Snowden, the British TEMPORA is the first "full take" system developed by any intelligence agency[37] **that allows wholesale Internet traffic to be collected, instead of forcing a preselection of materials.** Not every bulk collection system from GCHQ is fed into TEMPORA, but apparently the majority are and there is a growing trend. As of May 2012, there were TEMPORA capabilities at three processing centres – which appear to correspond to Bude, Oman and Cheltenham.

The exact capacity is difficult to assess and it is clearly evolving in any case. Der Spiegel reported that overall the agency has installed the relevant equipment to access 200 of these channels – but not all at the same time - and there are plans to extend TEMPORA's potential reach to 1500 processors.[38] Other documents indicate that in May 2012 GCHQ had the capacity to feed 46 channels of 10 Gb/s at any time each into their "full take" system.[39]

…

Access and collection[40]

Rules for ingestion into the system[41]

Despite its extensive capabilities, GCHQ has more access to data in cables than the available capacity to process it and send it home for further analysis – called to egress by the agency, so the raw material has to be preselected. According to the documents, the system has tools to create rules that "promote traffic into the Internet buffer capability".

Deep packet capture inspection (and injection)[42]

The bulk collection of Internet data itself involves huge processing. A cable splitter may initially divide the light for collection, but this flow of data is not very useful for the agencies. Raw Internet data is composed of small "packets" of data. Any processing of data requires the ability to look into individual packets. The equipment physically connected to the cables is also able to inject data back into the pipe. These machines with dual capacity to read and write directly to the backbone of the Internet form the global TURMOIL system, are run by the NSA, but with extensive UK participation.

Volume Reduction[43]

The selective ingestion involves discarding traffic that takes up a lot of space but has low intelligence value, such as consumer videos and file-sharing media downloads. They then keep things like email, chats, etc. [and all "Related CD – see above DK/IB]. Some 30% of the total traffic [including all "Related CD" – DK/IB] is ingested. Several documents mention a system called "massive volume reduction"

---

37 http://www.spiegel.de/netzwelt/netzpolitik/Internetueberwachung-so-maechtig-sind-xkeyscoretempora-und-prism-a-914300.html [original note]

38 http://www.spiegel.de/netzwelt/netzpolitik/Internetueberwachung-tempora-ist-schlimmer-als-prism-a907337.html [original note]

39 https://www.eff.org/files/2014/06/23/gchq_report_on_the_technical_abilities_of_tempora.pdf http://www.spiegel.de/media/media-34103.pdf [original note]

40 CDT report (footnote 13, above), *Bulk Collection in Practice*, p. 20 ff.

41 *Idem*, *Collection*, pp. 20 – 22.

42 On the technical aspects, see *idem*, *Collection – Intercepting Cable Traffic*and *extraction*, pp. 12 – 13.

43 *Idem*, on the technical issues: *Filtering*, p. 13, and on the specific UK situation: *Filtering*, p. 22.

(MVR)[44] - and clarify that MVR is not available at every TEMPORA instance. However, it is not completely clear whether there are two separate systems for initial selection and volume reduction or just one.

In any case, as Eric King explained:[45]

> **In order to filter, you need to intercept; communications cannot be filtered unless they are first intercepted.**

And as he explained in his later, more detailed report, quoting the UK Government's own observations to the ECtHR's Grand Chamber:[46]

> **It is not possible to extract specified communications, or particular communications to or from a specified identifier, from the bearer.[47] Instead, in the bulk cable interception context, all the communications on the bearer have to be collected in a single act of interception.**

In sum:

- **very large amounts of data – including all communications metadata (including traffic- and location data) are extracted from all selected bearers indiscriminately, in bulk;**
- **the vast majority of data subjects to which the metadata relate – which for many bearers will include large numbers of EU persons – will have no links with terrorism, threats to national security or serious crime whatsoever;**
- **while much of the other data are filtered out fairly quickly through "simple" or "complex" queries, the metadata are retained for longer, to allow for their use in algorithmic analyses and profiling (as discussed in section 2.3.3, below); and**
- **at least some of the data including content data will be filtered out for further inspection for purposes that are not aimed at countering serious threats to national security, but rather, to gain some politically or economically advantageous insights into actions of adversaries and allies alike.**

This has significant implications under the EU Charter of Fundamental Rights, as we will note and discuss below, at. 3.2, under the heading "*Assessment*".

iii. How intrusive is it?

The ISC was told that related communications data is now as intrusive, and in many cases more intrusive – more revealing of a person's most intimate activities, be they political,

---

44 http://www.wired.co.uk/news/archive/2013-06/24/gchq-tempora-101 [original note]

45 Witness Statement of Eric King on behalf of Privacy International in the case before the UK Investigatory Powers Tribunal in *Privacy International v. the Secretary of State for Foreign and Commonwealth Affairs & Government Communication Headquarters* (Case No. IPT/13/92/CH), 8 June 2014, para. 45, emphasis added, available at: https://privacyinternational.org/sites/default/files/2018-03/2014.06.08%20Eric%20King%20witness%20statement.pdf

46 CDT report, (footnote 13, above), p. 12.

47 See "*for technical reasons, it is necessary to intercept the entire contents of a fibre optic cable (or "bearer") in order to obtain any intercepted communications or communications data from it at all.*" United Kingdom's Observations on the Grand Chamber's Questions to the Parties (3 May 2019). [original footnote]

religious, medical or sexual – than most content data.[48] The UK Government and the secret intelligence agencies disputed this. In the words of the Director General of MI5:[49]

> The suggestion that, by knowing which websites people have visited, that that is some substantial step up in intrusion, is not one I accept. Life is different these days. But browsing through different websites, much like browsing telephone calls made and where people go in their daily lives along the street, I am not sure these things are substantially different. What is transacted in the content would require an intrusive warrant.

But from an EU legal perspective that view must be discarded: the European Court of Human Rights was:[50]

> **not persuaded that the acquisition of related communications data is necessarily less intrusive than the acquisition of content.** For example, the content of an electronic communication might be encrypted and, even if it were decrypted, might not reveal anything of note about the sender or recipient. The related communications data, on the other hand, could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with.

The CJEU also stresses, if anything more strongly than the ECtHR, that communications data are highly revealing, can be used to create **profiles** of individuals, and are therefore "**no less sensitive than the actual content of communications**":[51]

> The interference with the right enshrined in Article 7 of the Charter entailed by the transmission of traffic data and location data to the security and intelligence agencies must be regarded as being particularly serious, **bearing in mind inter alia the sensitive nature of the information which that data may provide and, in particular, the possibility of establishing a profile of the persons concerned on the basis of that data, such information being no less sensitive than the actual content of communications.** In addition, it is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.

In sum:

The "Related communications data" that are extracted by the UK's GCHQ from the selected bearers indiscriminately, in bulk, and retained for some time, are highly revealing of the lives of the tens or hundreds of thousands of individuals to which they may relate, including EU persons (the vast majority of whom will have no links to terrorism or serious crime), can

---

[48] Witness Statement of Eric King on behalf of Privacy International (footnote 45, above), paras. 136 – 138.

[49] *Idem*, para. 140, with reference to the D-G's oral evidence to the ISC on 8 May 2014. The UK expressed the same view in its submissions in the *BBW* case: see para. 349 of the judgment (next footnote).

[50] ECtHR First Section judgment in *Big Brother Watch [BBW] v. the United Kingdom*, 13 September 2018 (referred to the Gran Chamber on 4 February 2019 and still pending there), para. 356, emphasis added, available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-186048%22]}

[51] CJEU *Privacy International* Grand Chamber judgment of 6 October 2020, para. 71; *LQDN and Others* Grand Chamber judgment of the same date, para. 117.

lead to them being profiled, and may have a chilling effect on their enjoyment of other rights such as the rights to freedom of communication, expression and association.

These concerns are strongly reinforced in relation to algorithmic analysis of the data, as discussed in section 2.3.3, below,

That too has important implications under the Charter of Fundamental Rights.

2.3 How the data are used

2.3.1 Introduction

The ISC report notes two elements to GCHQ's bulk interception programme:[52]

> GCHQ's bulk interception capability is used either to investigate the communications of individuals already known to pose a threat, or to generate new intelligence leads, for example to find terrorist plots, cyber attacks or other threats to national security.

Below, we briefly describe the (overlapping) parts to the programme, while noting likely new technical developments in particular in relation to the second part (the "new threat" detection).

2.3.2 Monitoring of individuals already "known" to pose a threat

As ORG explains, the first part of the programme is:[53]

> an "investigative tool", targeted at "specific identifiers relating to a known suspect" to be analysed by intelligence operatives.

The parliamentary Intelligence and Security Committee has stated these "known suspects" or "known threats" may be targeted in the UK by means of more traditional communication interception,[54] but the data collected in bulk from the Internet bearers are also filtered to find information on such known suspects or threats, by means of "simple selectors":[55]

> Any communications which match the specific 'simple selectors' are automatically collected. All other communications are automatically discarded.[56] …
>
> In practice, while this process has been described as bulk interception because of the numbers of communications it covers, it is nevertheless targeted since the selectors used relate to individual targets: ***.[57]

We note again the obfuscation about what constitutes "collecting" of data.[58] As the first quoted sentence makes clear, "*[a]ny communications which match the specific 'simple selectors' are automatically collected. All other communications are automatically discarded.*" But this implies that initially, all the communications – the entire traffic – that flows through a selected bearer is intercepted, and only then filtered, resulting in either the continued retention of information that matches any of the simple selectors, or the

---

52 ISC report (footnote 11, above), p. 28.

53 ORG report, para. 17.

54 ISC report, p. 3; cf also para. 56, on p. 27.

55 *Idem*, para. 61. The statistics in this paragraph have been obscured, hence our omission of the relevant – to the non-privileged reader, useless – sentence.

56 GCHQ also collect all the Communications Data associated with these communications (described as 'Related Communications Data' in RIPA) before extracting that which is most likely to be of intelligence value. We return to this issue in Chapter 6. [original footnote]

57 Almost all of the 'simple selectors' relate to ***. However, GCHQ also search for a small number of ***. ***. [original footnote]

58 See section 2.2.2.ii, above.

discarding of information that does not match any simple selector. But in EU data protection-legal terms, the data are collected when they are taken from the bearers. You cannot filter unless you first collect. The language used seeks to obscure that fact – and thereby hides the fact that data on many, many more people are collected (that is: extracted from the bearers) than are "collected" (read: thereafter further retained) after initial filtering.

2.3.3 Identifying new threats and previously unknown persons "of interest"

i. Identifying new threats through "complex selectors" and "selection rules"

This part of the programme is described in the ISC report, with significant redactions, as follows:[59]

> Another major processing system by which GCHQ may collect communications is ***, **where GCHQ are looking to match much more complicated criteria with three or four elements**, for example.[60] Unlike the simple selectors used in the first process, this technique requires ***.
>
> This process operates across a far smaller number of bearers – GCHQ choose just *** of the bearers out of those they can theoretically access.[61] **These bearers are not chosen at random: they are deliberately targeted as those most likely to carry communications of intelligence interest.** (For example, GCHQ are currently targeting bearers likely to be carrying communications of ***.)
>
> **As a first step in the processing under this method, ***. *** the system applies a set of 'selection rules'.** As of November 2014, there were *** selection rules. ***. Examples of these initial selection rules are:
>
> - include ***;
> - include ***; and
> - discard communications ***.
>
> As a result of this selection stage, the processing system automatically discards the majority (***) of the traffic on the targeted bearers. The remainder is collected ***. These communications are the ones that GCHQ consider most likely to contain items of intelligence value.
>
> ***.
>
> **GCHQ's computers then perform automated searches using complex criteria (***) to draw out communications of intelligence value.** By performing searches combining a number of criteria, the odds of a 'false positive' are considerably reduced. ***.
>
> While analysts may create **additional bespoke searches based on the complex criteria**, the system does not permit them to search freely (i.e. they cannot conduct fishing expeditions). GCHQ explained: "***".
>
> **The individual communications which match these complex searches** number approximately *** items per day. These **are made available, in list form, to analysts for possible examination and storage** (we consider the criteria for examination later in this chapter).

---

59 ISC report (footnote 11, above), paras. 65 – 73, emphases added, footnotes that simply cross-refer to "Written Evidence – GCHQ", with a date, omitted. All the information is based on this written evidence.

60 GCHQ have a number of other capabilities of this type, including: ***. [original footnote]

61 These are a subset of the same bearers that are accessed under the method already described. [original footnote] We understand the reference to "the method already described" to refer to the filtering by means of simple selectors.

These rather obscure paragraphs deserve some parsing. First of all, it is notable that the second paragraph says that "*[t]his process"* – i.e., the "complex selector" filtering – *"operates across a far smaller number of bearers*" (presumably, than the "simple selector" filtering is applied to); and that "*[t]hese bearers are not chosen at random: they are deliberately targeted as those most likely to carry communications of intelligence interest.*" This suggests that the filtering by means of "simple selectors", described at 2.3.2, above, is less targeted – that for that process there is essentially no selection; that the "simple selector" filtering is indeed applied indiscriminately to all the bearers to which GCHQ has access at any one time.

Secondly, the fourth paragraph (after the bullet-points) again uses the terms "collecting" and "discarding" confusingly – but again actually confirms that what the ISC (and GCHQ) call "collecting" in fact happens after the bulk extraction of the data, i.e., after the information has already been collected in plain language.

Thirdly, there is the claim that "*[b]y performing searches combining a number of criteria, the odds of a 'false positive' are considerably reduced.*" That may be true for clearly specified selectors or rules, e.g., a search for "male AND Muslim AND aged 18 – 28 AND Syrian national" will throw up less false positives than a search that uses only one or a few of these search terms. But as we shall note in the next section, the problem of excessive false positives (and excessive false negatives) cannot be avoided in Big Data datamining operations. In that next section, we will also note that the reference to the analysts not being allowed to "*conduct fishing expeditions*" is misleading in the context of such more sophisticated operations.

ii. Identifying new threats and previously unknown persons "of interest" through more sophisticated data mining

THE BULK DATA

The Bulk communications data

The ISC report distinguished between **content** of communications and "**information associated with [extracted] communications**", and made a further distinction in the latter:[62]

> [Information associated with those communications] include[s] both **Communications Data (CD)** [**metadata** – DK/IB] … (which is limited to the basic 'who, when and where' and is described in greater detail in Chapter 6),[See below] and other information derived from the content (which we refer to as **Content-Derived Information, or CDI**),[63] including the characteristics of the communication[64] ***.

In fact, in Chapter 6 of the report (mentioned in the above quote), the Committee identified a further category, "**Communications Data Plus**", and provided the following descriptions of the different categories in relation to telephone calls (while stressing that these were not formal categories or definitions in the law):[65]

---

62 *Idem*, para. 80, emphasis added.

63 The technical term used to describe this information is 'content-derived metadata'. However, given the confusion regarding the term 'metadata' (which we address in Chapter 6), for ease the Committee will refer to this type of information as 'Content-Derived Information' throughout. [original footnote]

64 *** [original footnote] "Characteristics of a communication" could cover such issues as to the nature of the devices used, or the use of sophisticated encryption, or routing of the communication through the anonymity-preserving ToR network (see: https://www.torproject.org/).

65 *Idem*, para. 142.

Type of information	**Example (in relation to a telephone call)**
Communications Data [metadata]	The numbers and date/time of a telephone call
'Communications Data Plus'	Details of the person or organisation called, which could reveal details about a person's private life (e.g. if it was a call to a particular medical helpline, or a certain type of dating or sex chat line); *details of web domains visited or the locational tracking information in a smartphone*
Content-Derived Information	The accent of an individual speaking during the call *(which can only be obtained through access to the content)*
Content	What was said during the call

Note: In the above chart, we have added further examples of what is covered by the different terms, provided by the Committee in the paragraph under the chart, in *italics*.[66] For further details of what constitutes "communications data" (metadata), see below.

On communications data (metadata), the ISC furthermore quoted an earlier report by the Committee as follows:[67]

> The Committee provided a detailed explanation and examples of CD [metadata] in its Report '*Access to communications data by the intelligence and security Agencies*', dated February 2013:
>
> *CD is the information created when a communication takes place – for example, the time and duration of the contact, telephone numbers or email addresses, and sometimes the location of the device from which the communication was made. More detailed examples are as follows:*
>
> - *Landline telephones: details about numbers dialled by a telephone; time/dates calls are made and received; name and address details of the person who pays the line rental.*
> - *Mobile telephones: as above, but also the approximate location from which a call/text was made or received by a handset.*
> - *Internet telephony: the online username, login name or account name from which a call is made or received; the date/time of the call; and the internet addresses (IP addresses) of the computers used.*
> - *Email: the email addresses of the sender and recipient; the date/time of the message; and the internet addresses (IP addresses) of the computers used.*

66 See para. 143 of the report.
67 *Idem*, para. 129.

- *Instant/social messaging: the online user, login name or account name from which a message is sent or received; the date/time the message was sent; and the internet addresses (IP addresses) of the computers used.*
- *Web browsing: the IP address of the device being used to access the Internet; time and date of logon and logoff; record of web domains visited.*

It is, we feel, important for the EU recipients of this submission to be aware of the extremely broad sweep of these data – all collected in bulk, also from bearers in undersea cables that carry the communications of large numbers of individuals in the EU.

Additional bulk personal datasets

Apart from collecting communications data and especially metadata in bulk, the UK intelligence agencies also have access to other large bulk personal datasets – although all details about them are redacted in the ISC report:[68]

> In addition to obtaining intelligence through capabilities such as interception, **the Agencies also acquire Bulk Personal Datasets containing personal information about a large number of people.** Bulk Personal Datasets may relate to the following types of information:
>
> i) ***;
>
> ii) ***;
>
> iii) ***;
>
> iv) ***;
>
> v) ***.
>
> …
>
> Bulk Personal Datasets may be acquired through overt and covert channels. The Agencies' current holdings include: ***.[69]
>
> The number of Bulk Personal Datasets that each Agency holds fluctuates over time as they acquire new datasets, and they have told us that those which have not proven to be of intelligence value are deleted. As of mid-2014:
>
> - SIS held *** Bulk Personal Datasets;
> - MI5 held ***; and
> - GCHQ held ***.
>
> **The Committee was told that the Agencies may share Bulk Personal Datasets between them where they consider this to be lawful, necessary and proportionate.**
>
> **These datasets vary in size from hundreds to millions of records. Where possible, Bulk Personal Datasets may be linked together so that analysts can quickly find all the information linked to a selector (e.g. a telephone number or ***) from one search query. ***.**

We believe – but of course cannot prove since these details are kept secret – that these additional bulk personal datasets may well relate to financial matters such as bank card

---

[68] *Idem*, para. 151 and 154 – 156, emphases added, footnote references to undisclosed sources and to "*Written Evidence – GCHQ*" and "*Oral Evidence – SIS*" omitted.

[69] The Director General of MI5 has explained that "in 2008, the Government deliberately… added Section 19 of the Counter-Terrorism Act [2008], which is an explicit licensing to those who might share data, that doing so overrides any other duties of confidentiality they might have about data, where a case is made that it is necessary to share that for national security". (Oral Evidence – MI5, 8 May 2014.) [original footnote]

transactions, wire transfers or bank account details, travel information (in particular Passenger Name Records or PNRs), local government information such as who is registered at a particular address, etcetera.

THE USES OF THE BULK DATA

We have written (together, separately and/or with others) about the use of bulk data collection and use for more than 15 years, in relation to predictive policing,[70] the fight against terrorism,[71] national security[72] and border control/PNR data.[73] We believe that the ISC report in particular fails to note the more problematic uses of the bulk personal data by the UK intelligence agencies, in particular the use of Big Data datamining technologies to "identify" individuals as (possible or probable) terrorists or other threats to national or public security. Below, we briefly note both the acknowledged and the less clearly acknowledged uses of the bulk datasets.

Linking "known" Subjects of Interests and events

SIS explained that the additional bulk personal datasets:[74]

> ... are increasingly used to identify the people that we believe that we have an interest in; and also to identify the linkages between those individuals and the UK that we might be able to exploit. ***.

And GCHQ added that:[75]

> they consider Bulk Personal Datasets to be an increasingly important investigative tool, which they use primarily to 'enrich' information that has been obtained through other techniques:
>
> ***.

"Link analysis" of all the bulk personal datasets – the bulk communications data and the other datasets –can be used to identify and map networks of "known" or suspected terrorists, serious criminals or other bad people. It is by now common in police and forensic investigations, especially in relation to retrospective analysis (checking links between individuals and events that have occurred).[76]

---

70 Ian Brown and Douwe Korff, Privacy and Law Enforcement, study for the UK Information Commissioner, 2004, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3737428

71 Douwe Korff, Protecting the Right to Privacy in the Fight Against Terrorism, Issue Paper of the High Commissioner for Human Rights of the Council of Europe, November 2008, available at: https://rm.coe.int/ref/CommDH/IssuePaper(2008)3

72 E.g., Ian Brown & Douwe Korff, Terrorism and the Proportionality of Internet Surveillance, European Journal of Criminology, March 2009, available at: http://ssrn.com/abstract=1261194

Ian Brown & Douwe Korff, Foreign surveillance: law and practice in a global digital environment, European Human Rights Law Review, 2014(3) (April 2014), available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2521433

73 Douwe Korff & Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards, report prepared for the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD) of the Council of Europe, June 2015, available at: https://rm.coe.int/16806a601b

74 *Idem*, para. 152, reference to "*Oral Evidence – SIS*" omitted.

75 *Idem*, para. 153, reference to "*Written Evidence – GCHQ*" omitted.

76 See: https://en.wikipedia.org/wiki/Link_analysis

It is however important to add a note of caution. The "*people that [the agencies] believe that [they] have an interest in*" are described in the ISC report (no doubt reflecting the agencies' own terminology) as "**Subjects of Interest**".[77] An "SoI" is defined as: *"an individual investigated by the Agencies because they are suspected of being a threat to national security."*[78] But this is quite far removed from a "suspect" as defined in criminal law, i.e., a person in relation to whom there are reasonable grounds to suspect s/he has committed an offence. In deciding whether to designate a person as an SoI, the intelligence agencies (in the UK as elsewhere) apply a (much) lower standard of evidence.

Being identified as a person with links to an SoI casts the net yet further. It can include, for instance, a person who has on several occasions called, or who on several occasions was called by, an SoI, or who on several occasions was in (roughly) the same location as an SoI, or both. **There is no doubt that many of the individuals whose are noted in a link analysis of an SoI's contacts will be entirely innocent people.** But at least, in such cases based on established facts (calls made, places visited), it will often be possible to exclude such innocent people from further inquiries (and invasions of their privacy and other rights).

Automated processing

ORG reports that the US NSA and GCHQ use advanced technologies to analyse bulk data, even without or before the involvement of humans, including the use of:[79]

- **automated natural language processing software** that can read and (pre-)analyse the contents of communications to extract those of likely or possible intelligence interest without the need for human access to that content;
- **acoustic (voice biometric) technologies** used for identification, extraction, and analysis of voice and voice signals, including foreign language (and accent) voice recognition, duplicate voice identification, and methods of measuring voice enhancement;
- **facial recognition software –** that can match photos and videos of individuals across many datasets and platforms, and that GCHQ has reportedly used to tap into the private webcam communications of innocent Yahoo! Subscribers "as an experiment".

As the ORG report points out:[80]

> These development have far-reaching implications for regulating surveillance. Claims that intrusion only takes place when humans are involved in "reading, listening to, or looking at" are hard to sustain, give the information that can be gleaned by computers alone.

"Identifying" possible other Subjects of Interest through AI-based datamining

The ISC report acknowledges that the UK intelligence agencies also carry out more sophisticated analyses than the above-mentioned filtering by means of "simple" or "complex

---

77 ISC report (footnote 11, above), para. 20, on p. 14.

78 *Idem*, footnote 14.

79 ORG report (footnote 12, above), Part One Chapter Three, Putting mass surveillance to use, in particular section 3.4.2, *Machine processing*. This part of the report is also separately available in pdf at: https://www.openrightsgroup.org/app/uploads/2020/03/03-Part_One_Chapter_Three-Analytics_and_usage.pdf

80 *Idem*, p. 11.

selectors" and "selection rules", or by relatively straight-forward "link analysis", by referring to agencies' capacities that:[81]

> involve the Agencies casting their nets wider and analysing large volumes of information, which enable the Agencies also to find **linkages, patterns, associations or behaviours** which might demonstrate a serious threat requiring investigation.

The report is somewhat coy about what this actually entails. It says that:[82]

> **GCHQ's bulk interception capability is used primarily to find patterns in, or characteristics of, online communications which indicate involvement in threats to national security.** The people involved in these communications are **sometimes already known**, in which case valuable extra intelligence may be obtained (e.g. a new person in a terrorist network, a new location to be monitored, or a new selector to be targeted). **In other cases, it exposes previously unknown individuals or plots** that threaten our security which would not otherwise be detected.

And that:[83]

> GCHQ have established that they can analyse CD to find **patterns** in it **that reflect particular online behaviours that are associated with activities such as attack planning**, and **to establish links**. (***.)

These quotes indicate the use of advanced datamining of the bulk personal datasets to identify elements and links between elements that no-one would have thought were relevant or linked in advance.[84] As an industry expert put it: [85]

> Big data [mining] is not just about lots of data, it is about having the ability to extract meaning; to sort through the masses of data elements **to discover the hidden pattern, the unexpected correlation**.

Moreover, the algorithms used in the analyses are increasingly **self-learning**, i.e., constantly dynamically re-generated and refined through loops linking back to earlier analyses, in theory constantly improving the outcome, through "**artificial intelligence**". More specifically, in the search for (further) "SoIs", the software creates constantly self-improving and refining **profiles** against which it matches the massive amounts of data – and in the end, it produces

---

81 *Idem*, para. 18, at ii, on p. 13, emphasis added. The ISC adds to this in brackets that "*[t]hese capabilities nevertheless require some degree of targeting in order to ensure that a human eye only looks at that which is most likely to be of intelligence value.*" We will come to that later in this section. It is of course somewhat ironic that the ISC refers on the one hand to the agencies "casting their nets widely", while at the same time claiming that "they cannot conduct fishing expeditions".

82 *Idem*, para. 90, emphases added.

83 *Idem*, para. 130, emphases added.

84 The discussion in the text paraphrases in particular the overview of the issues in Douwe Korff & Marie Georges, Passenger Name Records, data mining & data protection: the need for strong safeguards (footnote 73, above), section I.iii, *The dangers inherent in data mining and profiling*, that itself drew on and referenced the earlier papers listed in footnotes 70 – 72, above.
For further technical and other details and analysis, see ORG report (footnote 12, above), Part One Chapter Three, Putting mass surveillance to use, in particular section 3.4, *Additional issues with processing*. This part of the report is also separately available in pdf at:
https://www.openrightsgroup.org/app/uploads/2020/03/03-Part_One_Chapter_Three-Analytics_and_usage.pdf

85 Art Coviello, executive chairman of RSA, the security division of EMC, see:
http://www.computerweekly.com/news/2240178641/Embrace-big-data-to-enable-better-security-says-RSA
(emphasis added)

lists of individuals that the algorithm suggests may (possibly or probably) be terrorists, or associates of terrorists.

There are three main problems with such algorithmic "Subject of Interest"-detection.

First of all, there is what is known as **the base-rate fallacy**. This phrase is used to refer to the mathematically unavoidable fact that if you are looking for very rare instances in a very large data set (such as terrorists in a bulk database of communications or transactions), then no matter how well you design your algorithm, *you will always end up with either excessive numbers of "false positives" (cases or individuals that are wrongly identified as belonging to the rare class), or "false negatives" (cases or individuals that do fall within in the rare, looked-for category, but that are not identified as such), or both*.

It is important to stress the mathematical inevitability of this: you cannot improve the data set, or the algorithm, to avoid these debilitating results. **You cannot avoid the base-rate fallacy**.[86]

Secondly, even the best designed algorithms will have (usually unconsciously) **built-in biases**:[87]

> predictive techniques and 'rational discrimination' – statistical techniques used to inform decision making by 'facilitating the identification, classification and comparative assessment of analytically generated groups in terms of their expected value or risk' – perpetuate and enforce social inequality.

And third, the dynamic algorithms, the profiles they create and, worst, the outcomes they lead to, are becoming **unchallengeable**: even the original programmers, let alone the users of the systems, are after some time no longer able to explain the basis for the "identification" – read: labelling – by a computer of a person as a (possible or probable) terrorist or threat.

In our opinion, it must be assumed that the UK intelligence agencies use the bulk datasets precisely for the purpose of "identifying" – labelling – individuals whose details appear in them as "Subjects of Interest" on the basis of algorithmic analyses. Not only is that what bulk personal datasets – Big Data – are specifically used for. It is also what the US NSA is deeply involved in – and as noted in the next section, the UK's GCHQ works hand in glove with the NSA in its terrorist-detection programmes.

---

[86] See the well-known security blogs on the issue by Bruce Schneier:
Why Data Mining Won't Stop Terror, 9 March 2005, at:
https://www.schneier.com/essays/archives/2005/03/why_data_mining_wont.html
Data Mining for Terrorists, 9 March 2006, at:
https://www.schneier.com/blog/archives/2006/03/data_mining_for.html
The latter cross-refers to a CIA handbook that usefully covered the issue, with this link:
http://www.cia.gov/csi/books/19104/art15.html#ft145 – but that link no longer works.

[87] David Barnard-Wills' paraphrase of Oscar Gandy's main book on the topic, Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage, 2009, in *Surveillance & Society* 8(3): 379-381, at:
http://www.surveillance-and-society.org/ojs/index.php/journal/article/viewDownloadInterstitial/gandy_chance/gandy_chance
For the book itself, see: http://www.ashgate.com/isbn/9780754679615

In that respect, we agree with this analysis:[88]

> Many UK citizens are not concerned about the State having access to their innocuous emails and texts, particularly if this will allow law enforcement agencies to reduce the threat of terrorist attacks.
>
> However, intelligence services collect citizens' online communications data and run profiling algorithms to detect the characteristics of a potentially high-risk person, passenger or consignment. When law enforcement agents use algorithms that reflect unexamined generalizations about what constitutes a high-risk person, these practices may lead to erroneous conclusions that can result in negative outcomes that affect not only the lives of individuals but also of specific sections of society. If, for example, the indicators on which profiling is based relate to religious beliefs, ethnic or national origin, types of websites visited, flights booked to particular destinations, connections to specific groups of people or an individual, or political affiliations or occupation, the net is cast very wide and will include law abiding citizens.
>
> Whilst it is possible to derive profiles that provide valuable insights to intelligence services about suspected terrorists, it is also inevitable that intelligence services will arrive at incorrect conclusions about individuals, or groups of people. Inaccurate profiling can result in a flag being allocated to an individual, which may have repercussions in terms of a law-abiding citizen being subjected to more in-depth surveillance, arrest and detention for a number of days without charge, deportation, limitations on that individual's ability to gain entry to another country, or to secure certain types of employment and other forms of discrimination.

In relation to the issue of whether the UK should be granted a positive adequacy decision, the point becomes whether EU individuals – whose data are also obtained in bulk by the UK agencies – should be equally worried about the use of algorithms to assess whether they pose a risk to the UK (or the USA) – whether a "warning flag" should be attached to them.

2.4 UK-USA (and wider "5EYES") collaboration

Under the so-called UKUSA Agreement, signed in March 1946, GCHQ shares extensive information with its US counterpart, the US National Security Agency, NSA, and with the other partners in the wider "5EYES" arrangement (officially referred to as "FVEY"), Australia, Canada and New Zealand. The existence of the "5EYES" arrangement was first disclosed by an NSA employee in 1972, but the UKUSA Agreement was still kept secret for some years after that, and only released in 1976.[89]

In fact, both historically and currently, US and UK intelligence collection and analyses activities are a joint, integrated effort, along with the other three countries.

---

[88] Rachel O'Connor, Is Cameron proposing to legislate, inadvertently, for a Police State in the UK? Why citizens should urge caution, balance and proportionality, 21 January 2015, on the "TrustElevate" *groovyfuture* blog, available here: http://groovyfuture.com/is-cameron-proposing-to-legislate-inadvertently-for-a-police-state-in-the-uk-why-citizens-should-urge-caution-balance-and-proportionality/

[89] It was originally called the British-US Communication Intelligence Agreement, BRUSA, and built on a less formal agreement dating to 1943. It is available from the UK national archives and the NSA website at: http://discovery.nationalarchives.gov.uk/details/r/C11536914 https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/ukusa/agreement_outline_5mar46.pdf (in pdf format)

This is explained with ample references in the witness statement of *Privacy International*'s then deputy director, Eric King, to the Investigatory Powers Tribunal in the case brought by *PI* against the agencies.[90] A few brief quotes from his statement (with the appropriate paragraph references) may suffice here:[91]

> The **highly integrated relationship between the US and the UK intelligence services** must be viewed within the context of a long-standing intelligence sharing arrangement that binds together the intelligence activities of the two countries, along with Australia, Canada and New Zealand. The agreement provides for the **full exchange of intelligence collected**, the division of tasks amongst agencies of the five States to prevent duplicity, high levels of cooperation, including provision for jointly run facilities, and the extensive dissemination of intelligence analysis. (para. 70)
>
> **[The "5EYES" arrangement was established] for the purpose of sharing intelligence but primarily signals intelligence** derived from the interception of communications travelling and transmitted by fibre optic cables, radio waves, satellites, and other forms of wireless telegraphy. (para. 71)
>
> … **from the outset, the relationship was a highly integrated one, particularly as it concerned the cooperation of American and British agencies** (para. 73)
>
> [I]n addition to facilitating collaboration, the [UKUSA] agreement suggests that **all intelligence material is shared between Five Eyes States by default**. (para. 76)
>
> [The "5EYES" arrangement includes **division of tasks** between the participating agencies] (paras. 78 – 79) **It relies on [the agencies] shar[ing] the collection burden and the resulting intelligence yield**.[92] (para. 79)
>
> **The level of co-operation under the UKUSA agreement is so complete that "*the national product is often indistinguishable.*"**[93] This has resulted in former intelligence officials explaining that the close-knit cooperation that exists under the UKUSA agreement means "*that SIGINT customers in both capitals seldom know which country generated either the access or the product itself*."[94] Another former British signals intelligence officer has said that "*[c]ooperation between the two countries, particularly, in SIGINT, is so close that it becomes very difficult to know who is doing what [...] it's just organizational mess*."[95] (para. 80)
>
> The relationship is so close that one senior member of Britain's intelligence community told the Guardian[96]38 "*[w]hen you get a GCHQ pass it gives you access to the NSA too.* ***You can walk into the NSA and find GCHQ staff holding senior management positions, and vice versa.***" (para. 81)

---

90 See footnote 45, above.

91 The full section on *Intelligence Sharing Practices* runs to six pages, from para. 70 to para. 89, and is followed by a further lengthy section on *UK Access to US Signals Intelligence* (paras. 90 – 125) that appears to be much wider than assumed by the Strasbourg Court in the *BBW* case, as noted at 3.2, below. All the footnotes to the quotes in the text are original, taken from Eric King's witness statement. Original italics, emphases in bold added. Text in square brackets and paragraph references in ordinary brackets are our own.

92 *Safeguarding Canada's security through information superiority*, CSEC website.

93 Aldrich, *Transatlantic intelligence and security co-operation* (2006).

94 Lander, "*International intelligence cooperation: an inside perspective*," 17 Cambridge Review of International Affairs 3 (2007) p.487.

95 Britain's GCHQ 'the brains,' America's NSA 'the money' behind spy alliance," *Japan Times* (18 November 2013).

96 Hopkins, "From Turing to Snowden – how US-UK pact forged modern surveillance," *The Guardian* (2 December 2013)

Many intelligence facilities run by the Five Eyes parties are jointly operated, even jointly staffed, by members of intelligence agencies of Five Eyes countries. Each facility collects SIGINT, which can then be shared with the other Five Eyes members. (para. 62)

[DK/IB Comment: We believe this includes Bude which "*From its inception … has been an Anglo-American co-operative project. It was the United States National Security Agency (NSA) that paid for most of the infrastructure and the technology. The running costs, like payments for the staff, were paid by GCHQ, who also provided the land. The intelligence that was collected by the Bude satellite station was shared between NSA and GCHQ, and was jointly processed.*"[97]

"*The TAT-14 undersea cable landing at Bude was identified as one of few assets of "Critical Infrastructure and Key Resources" of the US on foreign territory, in a diplomatic cable leaked to WikiLeaks.*"[98]]

[T]he GCHQ base at Bude, in the South West of England, [is] also jointly staffed. *The Guardian* reported that GCHQ and the US National Security Agency ("NSA"), in addition to jointly developing the TEMPORA program, jointly examine material collected under the programme at Bude, where some 300 GCHQ analysts and 250 NSA analysts are located.[99] It is assumed that a continuation of the arrangement highlighted by Colonel William F. Friedman in which "*an interchange scheme was started under which men from each agency would work two or three years at the other*"[100] continues to be in effect, and that GCHQ staff are also located in the US at NSA run bases. (para. 86)

Full access was provided to NSA by Autumn 2011. An additional 850,000 NSA employees and US private contractors with top secret clearance reportedly also have access to GCHQ databases.[101]

As we already noted in section 2.4, the extensive – indeed, it would appear, comprehensive – data sharing arrangement between the "5EYES" agencies, and more in particular between GCHQ and the NSA, means that data on individuals in the EU, and in particular their communications data, collected in bulk by GCHQ, will (continue to) be made available also to the NSA – and indeed analysed in the manner described earlier jointly by GCHQ and NSA staff.

In terms of the GDPR, this sharing will, at least from 1 January 2021, involve the "onward transfer" of the data on individuals in the EU from the UK to the USA. We note the

97 Wikipedia entry on GCHQ Bude (with reference to Richard J Aldrich, GCHQ, London, 2010, UK: Harper Press. pp. 342–343. ISBN 978-0-00-731266-5), at: https://en.wikipedia.org/wiki/GCHQ_Bude

98 https://wikileaks.org/plusd/cables/09STATE15113_a.html

99 An early version of TEMPORA is referred to as the Cheltenham Processing Centre, additionally codenamed TINT, and is described as a "joint GCHQ/NSA research initiative". The Guardian quotes an internal GCHQ report that claims "GCHQ and NSA avoid processing the same data twice and proactively seek to converge technical solutions and processing architectures." It was additionally reported that NSA provided GCHQ with the technology necessary to sift through the material collected. The Guardian reported that 300 analysts from GCHQ and 250 from NSA were directly assigned to examine the collected material, although the number is now no doubt much larger. GCHQ have had staff examining collected material since the project's incarnation in 2008, with NSA analysts brought to trials in Summer 2011. [last two sentences from this footnote moved to the main text]

100 Clark, *The Man Who Broke Purple, The Life of Colonel William F Friedman, Who Deciphered the Japanese Code in World War II* (1977), p. 208.

101 These last two sentences quoted are taken from footnote 42 to King's Witness Statement.

incompatibility of this onward transfer with the GDPR in section 3.2, and discuss the implications in section 4.1 (implications for the UK) and 4.4 (implications for the EU Member States) of the Executive Summary.

While the UK was an EU Member State, perhaps not much could be done about this under EU law. However, now that the UK is no longer an EU Member State this can, and we submit must, be addressed urgently, in general and in the context of the matter of a UK adequacy decision.

- o – O – o -

3. Issues, standards and assessment

3.1 Issues and applicable standards

3.1.1 Introduction

Since this submission is about the question of whether the UK, as a "third country", should be granted a positive adequacy decision under the GDPR, and this part of the submission is about the implications of the UK surveillance operations summarised at 2, above, the most immediately applicable standards for assessments are those set out by the Court of Justice of the European Union (CJEU) in its recent *Schrems II* judgment.[102] In that judgment, the Court held that the USA could not be held to provide "adequate" protection of personal data because it gave its agencies, notably its National Security Agency (NSA) excessively wide powers of access to data including data transferred from the EU under the so-called "Privacy Shield", and did not provide EU data subjects with a judicial remedy equivalent to that envisaged in Article 47 of the EU Charter of Fundamental Rights.

Other judgments by the CJEU, and by the European Court of Human Rights (ECtHR), also shed light on the European human rights standards that state agencies (and state laws) must meet in relation to surveillance, including the following:

Court of Justice of the European Union judgments and opinion:[103]

- CJEU judgment of 8 April 2014 in joined cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others* and *Kärntner Landesregierung and Others* (***DRI***);
- CJEU judgment of 21 December 2016 in joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson and Others* (***Tele2/Watson***);
- CJEU judgment of 6 October 2015 in case C-362/14, *Maximillian Schrems v Data Protection Commissioner* (***Schrems I***);
- CJEU Opinion 1/15 of 26 July 2017 on the EU – Canada Draft PNR Agreement (***EU-CAN PNR Opinion***);
- CJEU judgment of 6 October 2020 in joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and others* (***LQDN***);
- CJEU judgment of 6 October 2020 in case C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others* (***PI***).

---

102 CJEU Grand Chamber judgment in case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* ("*Schrems II*"), 16 July 2020, available at: http://curia.europa.eu/juris/liste.jsf?num=C-311/18

103 For the full references to *Schrems II*, see the previous footnotes. All other CJEU judgments are available from the Court's website at: http://curia.europa.eu/juris/recherche.jsf?language=en

European Court of Human Rights judgments:[104]

- ECtHR judgment of 6 September 1978 in *Klass and others v Germany* (***Klass***);
- ECtHR judgment of 26 April 1985 in *Malone v the United Kingdom* (***Malone***);
- ECtHR admissibility decision of 29 June 2006 on the application of Gabriele Weber and Cesar Richard Saravia v Germany (***Weber and Saravia***);
- ECtHR judgment of 1 July 2008 in *Liberty and others v the United Kingdom* (***Liberty***);
- ECtHR judgment of 18 May 2010 in Kennedy v the United Kingdom (***Kennedy***);
- ECtHR judgment of 4 December 2015 in *Roman Zakharov v Russia* (***Zakharov***);
- ECtHR judgment of 13 September 2018 in Big Brother Watch (***BBW***) (referred to the Grand Chamber on 4 February 2019 and still pending there).

Although *Schrems I* and *II* assessed surveillance by a third country (in both cases, the USA) under the GDPR "adequacy" tests discussed in Part One of our submission,[105] while the other CJEU judgments related to mandatory processing by commercial entities in Member States under the surveillance laws of those Member States, the standards are notably similar[106] – which is not surprising since in both cases they derive from the EU Charter of Fundamental Rights. Also, the same principles that apply to mandatory data retention by such entities in order to allow access to the retained data by the state authorities (as set out in the CJEU *DRI* and *Tele2/Watson* judgments) also apply to transmission of data to and access to data held by such entities with a view to its use by such authorities (as addressed in the *PI* and *LQDN* judgments). They also essentially correspond to the standards set by the ECtHR (with some differences, noted below, at 3.1.2).

The European Data Protection Board has produced a recommendation containing a set of (updated) "**European Essential Guarantees for surveillance measures**" (hereafter: **EEGs**)[107] that sum up these standards, with the aim of providing:[108]

> elements to examine, whether surveillance measures allowing access to personal data by public authorities in a third country, being national security agencies or law enforcement authorities, can be regarded as a justifiable interference or not … [as] part of the assessment to conduct in order to determine whether a third country provides a level of protection essentially equivalent to that guaranteed within the EU

---

104 All ECtHR judgments and admissibility decisions are available from the Council of Europe's HUDOC website at:
http://hudoc.echr.coe.int/sites/eng/Pages/search.aspx

105 See Part One of our submission, section xxx.

106 Cf. Graham Smith's *Cyberleagle* blog of 15 October 2020, *Hard questions about soft limits*, available at:
https://www.cyberleagle.com/2020/10/hard-questions-about-soft-limits.html#comment-form

107 EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, adopted on 10 November 2020, available at:
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf
The recommendation builds on an earlier WP29 working document, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) (WP237), adopted by the WP on 13 April 2016 in response to the *Schrems I* judgment, but takes into account the important subsequent case-law of both the Luxembourg and Strasbourg Courts, in particular *Schrems II*.

108 *Idem*, paras. 7 -, p. 5.

Below, we provide an overview of the main standards set out in the EEGs document and add some points of our own – in particular, the first two points, and the final one on profiling – with references.

In sub-section 3.2, we apply the standards adduced below to the UK law and practices set out in section 2, above. We summarise our conclusions in sub-section 3.3, and discuss the implications in section 4 of the Executive Summary.

3.1.2 Main issues and applicable standards

The main standards that should be applied, and the main issues that should be taken into account in assessing the UK's (or any third country's)[109] law and practices in relation to surveillance, are the following:

1. **Metadata are personal data:**

   Communications metadata (referred to in UK surveillance law as "related communications data" and broadly corresponding to traffic and location data in terms of the EU e-Privacy Directive; hereafter "metadata") – i.e., the "who, what and where" of communications – are personal data within the meaning of that term in EU data protection law including the GDPR.

   References: Since at least 2000, the Article 29 Working Party has consistently held that IP addresses are personal data, see WP29, Privacy on the Internet - An integrated EU Approach to On-line Data Protection (WP37), adopted on 21.11.2000, since repeatedly reaffirmed. On the need to apply data protection law strictly to all metadata, see in particular WP29 Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC), adopted on 4 April 2017 (WP247), *passim*.

2. **Metadata are no less sensitive than content data:**

   Metadata are highly revealing, can be used to create profiles of individuals, and are therefore "no less sensitive than the actual content of communications".

   References: CJEU *PI* judgment, para. 71, quoted at 2.2, above, under the heading "*How intrusive is it?*". Cf. also ECtHR *BBW* judgment, para. 356. See also point 8, below.

3. **Any form of processing of personal data (including metadata) for intelligence purposes constitutes an interference with fundamental rights:**

   Any processing of any personal data (including metadata) originally collected and used for other purposes such as commerce, medical treatment, travel, or to facilitate communications, for intelligence purposes constitutes an interference with the fundamental rights of the individuals to which the data relate – the data subjects; this includes mandatory retention of data beyond the normal retention period so as to allow them to be accessed by the intelligence agencies, compulsory active transmission or making available of the data to the intelligence agencies, as well as (more or less passively) allowing those agencies to access or extract such data from the relevant systems (such as servers, cables, bearers or routers). In relation to mandatory data retention, the compulsory retention is one interference; subsequent access to the retained data constitutes a "further" or "separate" interference. Moreover, "[T]he operation of having personal data transferred from a Member State

[109] And indeed any Member State's – but that is a separate matter, complicated by the exclusion of national security activities by Member States from EU laws including the Charter: see section 4.3, below. In this section, we limit ourselves to the implications in relation to adequacy decisions on third countries, more specifically the UK.

to a third country constitutes, in itself, processing of personal data" (*Schrems II*, para. 83).

References: Cf. CJEU *DRI* judgment, paras. 34 – 35; CJEU *LQDN* judgment, paras. 115 – 116; ECtHR *Malone* judgment, para. 64; ECtHR *Amman* judgment, para. 70. The WP29 working document refers to the latter two cases on p. 6 and list "the collection, storage, access or use and dissemination of personal data from an individual for purposes for which it was not originally transferred, but for national security or intelligence purposes" as "limitations to or interferences with fundamental rights to privacy and data protection" (p. 5). The EDPB's EEGs refer to mandatory data retention and "other types of data processing, such as the transmission of data to persons other than users or access to that data with a view to its use" – all of which constitute interferences with fundamental rights (including the right to privacy and confidentiality of communications, and the right to data protection) (para. 16 on p. 7). See also the broad definition of "processing" in Article 4(2) GDPR.

4. There is already an interference with data subject rights if their data are mandatorily retained – or collected – by the intelligence agencies; it is not the case that there is only such an interference if a human agent accesses the retained – or collected and stored – data; that is a "further interference".

Reference: This is explicitly stated in *DRI*, paras. 34 – 35 with regard to compulsorily retained data, but the principle clearly also applies to data that are actually collected by the intelligence agencies (e.g., by extracting them from Internet cables or by means of "back doors" from the systems of communication- or Internet service providers and storing those data for subsequent analysis and access).

5. All such interferences must be based on "law", be limited to what is strictly "necessary" and "proportionate" to the intelligence purpose in question – which must be a "legitimate" purpose.

(Articles 8 – 11 ECHR; Article 52 CFR)

More specifically:

5.1 ***Re* "law" (1):** The rules under which the interference is authorised – i.e., the relevant national law of the third country in question – must be accessible (i.e., published), legally binding, clear and precise (i.e., "foreseeable" in its application in the sense that "*[t]he domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures*").

References: All of these requirements are standard requirements under the ECHR and the CFR, reiterated in the EEGs paras. 27 – 31, with reference to CJEU cases *Schrems II*, paras. 175, 180 and 181, *EU-CAN PNR*, para. 139 (and further case-law cited there) and *PI*, paras. 65 and 68; and ECtHR cases *Liberty*, para. 63, *Weber and Saravia*, para. 95 and *Malone*, paras 65 – 66. The quote is from ECtHR judgment in *Zakharov*, para. 229.

5.2 ***Re* "law" (2):** The law "must itself define" the scope and application of the measure in question.

References: EEGs, para. 29, with reference to the CJEU *Schrems II* judgment, para. 175, repeated *verbatim* with a cross-reference in its *PI* judgment, para. 65, and in its *LQDN* judgment, para. 175. Cf. also its *DRI* judgment, para. 68 (*re* EU law). Repeated in EEGs, para. 36.

Note: In its *BBW* judgment, the ECtHR has outlined "six minimum requirements" that surveillance laws must meet in order to ensure that they are "sufficiently foreseeable to minimise the risk of abuses of power" and which can be said to also indicate the "defining" that the CJEU says should be enshrined in the law itself. These are (in summary):

- [the need for a specification of] the nature of offences which may give rise to an interception order;

- [the need for] a definition of the categories of people liable to have their communications intercepted;
- [the need for] a [stipulated] limit on the duration of interception;
- [the need for an appropriate] procedure to be followed for examining, using and storing the data obtained;
- [the need for appropriate] precautions to be taken when communicating the data to other parties; and
- [the need for limitations on] the circumstances in which intercepted data may or must be erased or destroyed

(*BBW* judgment, para. 423, summarising the more detailed overview of the six requirements in para. 307, with indents and words in square brackets added. See also the EEGs, para. 30).

The first two of these correspond to the CJEU requirement that there must be some reasonable link between the individuals whose data are collected and the offences or threats to national security in relation to which their data are collected. In other words: **the law itself should expressly preclude the collection of personal data (including metadata) on individuals who have no personal link, or some link in time or place, to the offences or threats in question. General, indiscriminate, "dragnet", bulk collection of personal data (including metadata) – collecting of the "hay" from a "haystack" in order to find a "needle" buried in it – is fundamentally incompatible with EU fundamental rights law; and the laws covering surveillance should themselves, explicitly make clear that such bulk collection is not permitted. This cannot be left to vague language such as instructing a government minister authorising surveillance to do so only in a "proportionate" manner.**

In section 3.2, we will show that this is an important specific issue of concern in relation to UK law.

5.3 ***Re* necessity and proportionality and respect for the essence of rights:** Rules that permit general and indiscriminate transmission of communications data, including metadata to – or access to such data by – national intelligence agencies, are inherently disproportionate and unnecessary, and incompatible with the EU Charter of Fundamental Rights. Rather, there must be some link, "even an indirect and remote one", between the individuals whose data are collected, or the time or place in relation to which the data are collected, and the serious crimes or threats to national security for which the data are collected.

References: EEGs, paras. 37 – 38. This is also explicitly stated in the CJEU's *DRI* judgment, paras. 34 – 35, and implicitly in paras. 58 – 59, with regard to data compulsorily retained for law enforcement purposes, and in para. 81 with regard to compulsory disclosure of traffic- and location data for those purposes. *Idem* in its *PI* judgment with regard to compulsory transmission of traffic- and location data to intelligence agencies for national security purposes (paras. 78 – 82, with references to its *DRI* and *Tele2* judgments). The principle clearly also applies to data that are actually collected by the intelligence agencies (e.g., by extracting them from Internet cables or by means of "back doors" from the systems of communication or Internet service providers) and retaining those data for subsequent analysis and access).

Notes:

(1) In its *DRI* judgment, the CJEU held that while general and indiscriminate transmission of metadata "constitutes a particularly serious interference with [the fundamental right to privacy and the other rights laid down in Article 7 of the Charter]", it "is not such as to adversely affect the essence of those rights given that … [the directive under which this happened, the Data Retention Directive] [did] not permit the acquisition of knowledge of the content of the electronic communications as such." (*DRI* judgment, para. 39). But in view of the fact that the Court has since held that metadata are "no less sensitive than the actual content of communications" (*Pi* judgment, para. 71, see the second indent, above), it is doubtful that this distinction still applies. If general and indiscriminate access to the contents of communications adversely affects the essence of the right to privacy, the general and indiscriminate access to the "no less sensitive" metadata must now also be considered as compromising

the essence of that right. This is especially the case given metadata, even more than content of communications, can be – and are – used to create profiles and label individuals as possible or probable targets for intrusive surveillance and other, even more intrusive or harmful measures (as noted in the final indent, below).

(2) The CJEU judgments focus on the need of there being some personal link between the individuals whose data are collected and the threat in question. In *LQDN*, the CJEU also mentioned exceptional circumstances in which there is **a "serious", "genuine and present or foreseeable" threat to "the essential functions of the State and the fundamental interests of society"** such as "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 paras. 135 – 137). In such extreme situations – comparable to those in which there is a "public emergency threatening the life of the nation" envisaged in Article 15 ECHR, in which many normal human rights guarantees including the right to privacy can be derogated from – the Charter "*does not, in principle, preclude a legislative measure which permits the competent authorities to order providers of electronic communications services to retain traffic and location data of all users of electronic communications systems for a limited period of time*" (para. 137). However, there must be "sufficiently solid grounds" for considering that such an extreme threat exists. In our opinion, this part of the judgment is clearly limited to "clear and present dangers" to the fundamental functions of the state and cannot be relied upon in relation to lesser threats including isolated acts of terrorism that, while an outrage to the human conscience and a serious threat to individuals, do not threaten those fundamental values or interests. Specifically, we read this as applying in particular to situations in which the authorities learn about a planned serious attack with some indication of the intended time and place – and in which they may therefore decide to indiscriminately monitor (and retain) all traffic and location data of all users of electronic communications systems in the relevant area (cf. para. 144), for a limited period of time relating to the expected attack. This exception for extreme threats to the foundations of the state and society cannot be relied upon for more general anti-terrorist surveillance. Otherwise, this exception would become the rule – and the Court stresses both earlier in the judgment and shortly after the above paragraphs that derogations from the rights to confidentiality of communication and privacy should never become the rule (see paras. 111 and 142).

5.4 ***Re* legitimacy of purpose:** surveillance laws must only be used to protect the state and its people from genuine, serious, real threats to national security – using such laws to obtain confidential, private or incriminating information for political purposes or to carry out industrial espionage is not a legitimate use of such laws and therefore also inherently disproportionate and unnecessary, and incompatible with the EU Charter of Fundamental Rights and the GDPR. The relevant law must therefore itself explicitly prohibit such abuse of its powers (see point 5.2, above).

References: Both the CJEU and ECtHR stress, in all the judgments mentioned, that surveillance powers must only be used when strictly necessary to prevent serious crimes or to counter serious threats to national security. Thus, only "the objectives of combating serious crime, preventing serious attacks on public security and, a fortiori, safeguarding national security are capable of justifying … the particularly serious interference entailed by the targeted retention of traffic and location data" (*LQDN*, para. 146) – and the same applies to the transmission of such data to, or the collecting of such data by, the intelligence agencies. Surveillance powers should not be used – and surveillance laws should not allow or facilitate – the collection of information that is merely "relevant" to national security, let alone salacious private information for use in power games (see section 2.2.2.i, above). In terms of the GDPR, the collection of such information does not serve a "legitimate purpose" and is therefore in violation of Article 5(1)(b) of the Regulation. If the law of a third country nevertheless does allow for the collection of such data – and of course especially if there is evidence that such data are in fact collected under the third country's surveillance laws – then the transfer of data to that country would undermine the

protection to such data accorded by the Charter and the GDPR, and that stands in the way of a positive adequacy decision for the third country in question.[110]

6. Any interference with the right to privacy and data protection, and therefore also any collection and further processing of personal data by intelligence agencies, should be subject to an effective, independent and impartial oversight system that must be provided for either by a judge or by another independent body.

References: EEGs, paras. 39 – 42, with reference to ECtHR judgment *Klass*, paras. 17 and 51, CJEU judgment *Schrems II*, paras. 179 and 183

6.1 ***Re* scope of the oversight: "**The aim of that review is to verify that a situation justifying the measure exists and the conditions and safeguards that must be laid down are observed. For real-time collection of traffic and location data, the review should allow to check ex ante, inter alia, whether it is authorised only within the limits of what is strictly necessary. In cases of duly justified urgency, the measures may take place without such prior review; however, the Court still requires that the subsequent review takes place within a short time."

References: EEGs, para. 41, with references to CJEU judgment *LQDN*, paras. 168 and 189.

6.2 ***Re* independence of the oversight body:** This should preferably be a judge but could also be another body "as long as it is sufficiently independent from the executive" and "of the authorities carrying out the surveillance, and [is] vested with sufficient powers and competence to exercise an effective and continuous control". The supervisory body must have access to all relevant documents, including closed materials and its activities should be open to public scrutiny (e.g., through the body issuing public reports).

References: EEGs, para. 42, quoting ECtHR judgment in *Zakharov*, paras. 258, 278, 281 and 283, and other ECtHR judgments.

7. Individuals whose data have been collected by the intelligence agencies must be notified of this as soon as the notification no longer jeopardizes the tasks for which those authorities are responsible, and must have access to effective remedies before a judicial or quasi-judicial body if they believe their rights have not been respected.

(Article 13 ECHR; Article 47 CFR)

References: EEGs, paras. 43 – 47, quoting ECtHR judgment in *Zakharov*, paras. 258, 278, 281 and 283, and other ECtHR judgments.

7.1 *Re* notification: Both the ECHR and the CJEU stress that in principle individuals whose communications have been intercepted should be informed of this as soon as possible, while accepting that this may not be possible if notification "jeopardizes the tasks for which those authorities are responsible". But in that case, any person who suspects that his or her communications are being or have been intercepted should be able to apply to the courts, and the courts must then review the matter with full access to all materials (see point 7.3, below).

References: EEGs, paras. 44 – 45, quoting ECtHR judgments in *Zakharov*, para. 234, and *Kennedy*, para. 190.

---

[110] See the discussion of the requirements for a positive adequacy decision in Part One, section 2.1.4, of our submission.

7.2 ***Re* the nature of the remedial body:** The body should preferably be a judicial one (i.e., a judge or court) but if not, it should have the essential attributes of a judicial body in terms of its independence and qualifications.

References: EEGs, para. 47, quoting ECtHR judgment in *Klass*, para. 67, and CJEU judgment in *Schrems II*, paras. 194, 195 and 197. Cf. the ECtHR case-law on the attributes of the "national authority" referred to in Article 13 ECHR. The EDPB notes that Article 47 CFR uses the word "tribunal" in its English version, but "court" in other languages (German "Gericht"; Dutch "gerecht").

7.3 ***Re* the powers of the remedial body:** The body must have access to all relevant information including closed materials, and it must have the power to remedy non-compliance with the law (or the above-mentioned standards), i.e., to order remedial action.

References: EEGs, para. 45, with reference to the Council of Europe Commissioner for Human Rights view that the so-called "third parties" rule – under which intelligence agencies in one country that provide data to intelligence agencies in another country can impose a duty on the receiving agencies to not disclose the transferred data to any third party – should not apply to oversight bodies in order not to undermine the possibility of an effective remedy (Issue Paper on Democratic and effective oversight of national security services) and to the ECtHR judgment in *Kennedy*, para. 167.

8. If the intelligence agencies in a third country share data – including data that may have been transferred from the EU or directly obtained from the EU (e.g., from communication cables that run from the EU to that third country) – with sister agencies in other third countries, then this amounts to "onward transfers" of those data to that other third country. If that other third country does not provide adequate/essentially equivalent protection to those data this data sharing/onward transfers undermines the protection accorded to the data by EU law.

Note:

This issue is not addressed in the EDPB's European Essential Guarantees. However, data sharing regimes – and indeed joint operations – are common among intelligence agencies of different countries, be that between the "5EYES" countries (USA, UK, Canada, Australia and New Zealand)[111] or within the "Club of Berne"/CTG,[112] or between CIS countries.[113] If under such arrangements data can also be shared between the parties concerned that were transferred to the first party from the EU, this would constitute "onward transfers" of the EU data – and the GDPR specifically stipulates that such onward transfers must be assessed in the context of an adequacy decision to ensure that the protection accorded to the data under the GDPR is not undermined by the transfer. If data transferred from the EU to a third country ended up with the intelligence agencies in that third country, and were then likely to be shared by the intelligence agencies of that third country with the agencies of another third country that would not provide adequate/essentially equivalent protection to the data as is accorded under the GDPR – then that would clearly undermine that protection, and stand in the way of a positive adequacy decision in relation to the first third country.

9. Laws that allow for the taking of decisions on individuals that produce legal effects concerning those individuals or that otherwise "significantly affect" them, "based solely on automated processing, including profiling", must contain "suitable

---

111 See section 2.4, above.

112 See Matthias Monroy, *Schlagwort: Club of Berne – Bundestag report finds flaws in the oversight of European intelligence services in The Hague*, 14 June 2017, available at: https://digit.site36.net/tag/club-of-berne/
Also: *Schlagwort: CTG – German proposal: Prohibited EU secret service cooperation through the back door*, 20 October 2020, available at: https://digit.site36.net/tag/ctg/

113 Cf. *[President of Russia] Meeting with heads of CIS member states' security and intelligence agencies*, 19 December 2017, available at: http://en.kremlin.ru/events/president/news/56414

measures to safeguard the data subject's rights and freedoms and legitimate interests". If special categories of personal data are used in this (i.e., data on or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or sexual orientation, or genetic or biometric data), the laws must contain "suitable and specific measures" to safeguard their fundamental rights and interests.

(Article 22(2)(b) and (4), read with Article 9(2)(g) GDPR)

Note:

This issue too is not addressed in the EDPB's European Essential Guarantees. However, given that one main aim of bulk data collection by intelligence agencies (including the UK ones)[114] is to enable data mining and profiling, the above general requirements of the GDPR should be taken into account in any assessment of the adequacy of a third country's surveillance laws and practices. Specifically, the absence of any suitable (or suitable and specific) safeguards from the law of any third country that allows for the carrying out of bulk data collection, data mining and profiling, also of personal data transferred from the EU (or extracted from communication cables from the EU), as part of its intelligence/national security activities, would clearly undermine the protection accorded to those data by the GDPR. That, too, would stand in the way of a positive adequacy decision.

In section 3.2, we will assess the UK's surveillance laws and practices in the light of the above standards. First, however, we should discuss two further issues, already noted in the introduction.

3.1.3 Two further issues

i. If the UK is not held to provide adequate protection, does its extraction of data on EU communications amount to a personal data breach on the part of EU controllers and processors responsible for those data?

Article 4(12) GDPR defines a "personal data breach" as follows:

> 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Failure to protect against a personal data breach, or transferring personal data to a recipient in a third country in violation of the rules on such transfers, constitute serious infringements of the GDPR (see Articles 35ff and 83).

Some at least of the data that are extracted by the UK (and US) intelligence agencies from the underseas communications cables in bulk will relate to communications of individuals in the EU, routed into those cables by communication and Internet service providers (CSPs and ISPs) in the EU – and that extraction of and access to those data takes place (a) without the consent of the data subjects; (b) is, presumably, not "authorised" by the EU-based CSPs and ISPs in question (see below); and (c) is, since Brexit and certainly after the post-Brexit transition period, not based on "Union or Member State law".

There are two possibilities here. First of all, perhaps some UK bulk interception warrants are served on such EU-based CSPs and ISPs, or on their mother or partner companies in the UK – and the EU companies then facilitate (or passively allow) such access on the basis of that warrant. However, that would be in breach of Article 48 GDPR that stipulates that:

---

114 See section 2.3, above.

> Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

A bulk interception warrant issued under the UK Investigatory Powers Act constitutes precisely such a "decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data". And therefore, unless the UK were to seek to enforce such a warrant through some existing Mutual Legal Assistance Treaty, the EU CSPs and ISPs will be in breach of the GDPR if they comply with such a UK order (at least from 1 January 2021). The disclosure would be unlawful.

Alternatively, perhaps the EU CSPs and ISPs are not, themselves, directly involved or approached at all in relation to the extraction of the data. But in that case the disclosure of the data to, and the access to the data by, the UK intelligence agencies is still clearly "unauthorised". Moreover, to the extent that UK-based (or USA-based) companies are in physical control of the infrastructure through which the communications travel at the time of extraction, they must be seen as processors acting for the EU-based CSPs and ISPs (who are the controllers of the processing). In that case, the EU-based companies are in breach of their duty to:

> take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law. (Article 32(4) GDPR)

The EDPB, in its very recently issued recommendations on supplementary measures that may be required for transfers to third countries that indulge in mass surveillance,[115] strongly emphasises that it is the duty of the EU data exporter – i.e., *in casu*, the EU-based CSPs and ISPs – to take measures such as very strong encryption to ensure that the data are really, effectively protected against undue access to the exported data by third country authorities, stressing that they are responsible for assessing both the risks of such access and the effectiveness of any supplementary measures they could adopt:[116]

> You should conduct [the assessment of the law and practice of the third country] with due diligence and document it thoroughly, as **you will be held accountable to the decision you may take on that basis**.
>
> …
>
> You will be responsible for assessing [the adopted supplementary measures'] effectiveness in the context of the transfer, and in light of the third country law and the transfer tool you are relying on and **you will be held accountable for the decision you take**.

---

115 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, adopted on 10 November 2020, available at: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

116 *Idem*, Executive Summary, p. 3, emphasis added.

In this, they should also:[117]

> **not forget to also take into account onward transfers**, for instance whether your processors outside the EEA transfer the personal data you entrusted to them to a sub-processor in another third country or in the same third country –

stressing, in a footnote, that in any case the data controller/data exporter must grant "prior specific or general written authorisation" for such onward transfers.[118]

In our opinion, **the direct access to and extraction of communications data (be that content or metadata) by the UK intelligence agencies, from communications infrastructure used by EU-based providers**, constitutes a **personal data breach** on the part of those EU-based providers, means that any instruments they used in relation to the transfers of the data involved (such as SCCs) were insufficient and therefore **did not provide "appropriate safeguards"**, and **poses obvious "risk[s] to the rights and freedoms of natural persons"**, i.e., of their EU customers (generally, but also more specifically to the rights of persons such as EU Member State and EU officials, politicians including MEPs, journalists or activists using their services, to whom the confidentiality of their data is especially important).

This means that the data breach and transfer breach must be reported to the relevant EU Member State supervisory authority/ies (Article 33 GDPR) and that the data subjects – in particular the special categories in data subjects just mentioned, for whom the breach constitutes a "high risk" – must be informed (Article 34). Moreover, the EU-based CSPs and ISPs are liable for any material and immaterial damage caused by the breach (i.e., by the undue access to the data by the UK (and US) intelligence agencies.

We discuss the implications in section 4.4.2, below.

ii. Do the activities of the UK (and US) intelligence agencies constitute "monitoring of the behaviour of individuals in the EU"?

Finally, it is difficult to see how the surveillance activities of the UK (and U.S) intelligence services, where directed (also) at individuals in the EU can be said to not constitute "monitoring of [the] behaviour [of data subjects in the EU] as far as their behaviour takes place within the Union".

That means, on the face of it, *all* of the GDPR applies to those activities under Article 3(2)(b) GDPR, which stipulates:

> **This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:**
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such **data subjects in the Union**; or
>
> (b) **the monitoring of their behaviour as far as their behaviour takes place within the Union.**

Specifically, as the CJEU expressly clarified in *Schrems II*, activities by third country intelligence and national security agencies are not covered by the provision in the EU Treaties, in

117 *Idem*, para. 10, on p. 9.
118 *Idem*, footnote 25.

particular Article 4 TEU, that excludes the activities of the Member States in the area of national security from EU law (including the Charter and the GDPR):[119]

> [I]t should be made clear at the outset that the rule in Article 4(2) TEU, according to which, within the European Union, national security remains the sole responsibility of each Member State, concerns Member States of the European Union only. That rule is therefore irrelevant, in the present case, for the purposes of interpreting [various articles of] the GDPR.

It would of course be difficult to enforce the GDPR against the activities of a third country's intelligence agencies. However, the very fact that on the face of it GCHQ (and the US NSA) are subject to the EU rules should give some pause for thought. We will note this again in section 4.1.

3.2 Assessment

Having clarified the issues to be addressed and the standards to be applied, we can now proceed with the assessment of whether the UK surveillance laws and practices are compatible with those standards, or whether they are not – which would mean that the European Commission cannot lawfully issue a positive adequacy decision on the country. We have limited this assessment to what we believe are the main nine issues.

1. Are metadata subject to UK data protection law protections?

Metadata including traffic and location data are regarded as personal data in UK law and their processing is therefore subject to UK data protection law including (from 1 January 2021) the "UK GDPR", but also the Privacy and Electronic Communications Regulations, PECR (in the latest version of 2019) that implement the EU e-Privacy Directive and that will (for the time being) continue to apply.

However, the PECR contain a **sweeping exemption**, in Regulation 28. This exempts communications providers from any of the rules in PECR if that exemption is required for the purpose of safeguarding national security. Moreover, as the UK data protection authority, the ICO, explains:[120]

> A Minister of the Crown can issue a certificate stating that an exemption was, is or will be required in certain circumstances for national security reasons. A ministerial certificate is conclusive proof that the exemption applies in those circumstances. Any person directly affected by a ministerial certificate may appeal against it to the Information Rights Tribunal.

This means that **in effect all processing of traffic and communications data purportedly to safeguard national security can be deprived of any and all protection on the say-so of a government minister**. This in itself raises serious questions about the compatibility of the UK data protection regime with EU law and the EU Charter of Fundamental Rights.

Furthermore, under paragraph 253 of the Investigatory Powers Act, telecommunications companies can be served with a so-called **technical capability notice** that requires them to provide and maintain a continuous capability to carry out interception – i.e., to build a **"back**

---

119 *Schrems II*, para. 81.

120 ICO, *Guide to PECR – Exemptions*, available at: https://ico.org.uk/for-organisations/guide-to-pecr/exemptions/

door" into their systems through which the intelligence agencies can gain direct, indiscriminate access to all communications data (metadata and content).

And as we have shown in section 2.2.2.i, above, under **bulk interception warrants**, GCHQ also **taps directly into the underseas communication cables** to gain access to selected "bearers" within those cables, and extracts (at least) all metadata that flows through those selected bearers indiscriminately, in bulk.

Whatever the UK authorities may claim, **such bulk, indiscriminate extractions of data – at least of metadata – undoubtedly constitute serious breaches of the rights of data subjects in terms of EU data protection and Charter law, even if the data are not immediately (or in many cases, ever) directly accessed or inspected by a human being. Indeed, in our opinion, this bulk extraction in and by itself compromises the very essence of the rights to privacy, confidentiality of communications, and data protection**.[121] **These violations are further seriously aggravated if after extraction the bulk data are mined and analysed and used to create profiles in order to "identify" previously unknown threats or "persons of interest" (see below, point 9).**

In sum: Even now, but also under the "UK GDPR", metadata are not meaningfully protected against undue access and bulk collection by the UK intelligence agencies at all.

2. Is the bulk collection of communications data, in particular metadata, based on "law"?

The direct collection/extraction of communications data, including the bulk extraction of metadata from the communication bearers, is based on the Investigatory Powers Act 2016. The question is whether this Act of Parliament constitutes "law" in the ECHR/CFR sense. As noted at 3.1.2, above, at 5.1 and 5.2, for this to be the case the law must be accessible (i.e., published), legally binding, clear, precise, foreseeable in its application, and "itself define" the scope and application of the interception powers.

The Act is published and legally binding, also on the intelligence agencies – the (bad) old days of the "clandestine" agencies operating outside the law has ended.[122] And the Act, although complex, is as such reasonably clear and precise – although, as noted next, not really foreseeable in its application.

However, as explained at 2.2.2, above, **the Act does not itself define the scope and application of its powers** beyond the broad parameter that they may be used in the interest of matters "relevant to the interests of national security". Within that – in our view, and we believe in the light of EU law – excessively broad phrase, **the specific scope and limit of any specific bulk data interception authorisation is set out in "operational purposes" that are secret**.

In other words, as Graham Smith observes, while the CJEU requires "*clear and precise conditions set out in the legislation itself*", the UK legislator has instead chosen "*an approach based primarily on safeguards and oversight of a broad discretionary power*".[123] He wonders whether this is compatible with EU law.

---

121 See section 3.1.2, Note (1) under point 5.3, above.

122 Cf. section 2.2.1, above.

123 Graham Smith, *Hard questions about soft limits* (footnote 106, above).

We would put it more strongly: in our opinion, the UK Investigatory Powers Act clearly does not "itself define" the scope and limitations of the use of the powers it grants the intelligence agencies, in particular in relation to direct access to the systems of communication and Internet service providers, or to direct tapping into the underseas cables. The IPA therefore does not meet the requirements set by the CJEU in *Schrems II*.

3. Does the law allow for general, indiscriminate access to personal data and for its collection/extraction in bulk?

As we have shown in section 2.2.2, above, the IPA allows for **the extraction, in bulk, of at least all the metadata of all communications that flow through a selected bearer**. The only "targeting" that occurs in that regard is the selection of the bearer – there is no attempt to limit the extraction to communications of persons who are linked (even if perhaps only in an indirect and remote way) to serious crimes or serious threats to national security, or to times or places where a serious, imminent threat is clearly indicated.

This is not remedied by the fact that most of the content data are filtered out after extraction: **the metadata are extracted and retained for some time, indiscriminately**.

The UK IPA rules that allow for the extraction, in bulk, of at least all the metadata of all communications that flow through a selected bearer, are clearly incompatible with the standards set out in a range of CJEU judgments and arguably (given the now-recognised inherent sensitivity of metadata) compromises the very essence of the rights to privacy, confidentiality of communications and data protection.[124]

4. Is the law only used to counter genuine serious threats to national security?

There have been extensive reports of abuse of surveillance powers by the US NSA, to spy on political and industrial targets and non-violent activists.[125] There is less information on whether the UK agencies have similarly abused their powers under the IPA. However, it has become clear that the authorities in the UK have for many years spied on domestic activists, including through undercover agents, leading to the establishment of an official inquiry into the matter[126] – and it would be surprising if the same authorities that authorised this domestic abuse had not also spied on political and other targets abroad, including by spying on their communications. Moreover, as we have seen, the UK agencies work hand-in-glove with the U.S. ones.

The point to be made here is that, as explained in sections 2.2 and 2.3, above, the law allows for broadly phrased bulk interception warrants and for vague search criteria applied to stored data; the law itself does little to preclude targeting of improper targets. Rather, almost

---

124 See section 3.1.2, Note (1) under point 5.3.

125 See section 2.2.2, above, and in particular the reports referenced in footnotes 23 – 26, above.

126 Undercover Policing Inquiry, see: https://www.ucpi.org.uk/
See also the website of the Police Spies Out of Lives (PSOOL) campaigning support group, at: https://policespiesoutoflives.org.uk/home/
BBC page: https://www.bbc.co.uk/news/topics/cg1ln7gm46et/undercover-policing-inquiry
For newspaper reports see, e.g., *Officer wasted her time spying on group pushing for equal pay, inquiry told. Ex-police officer tells inquiry she infiltrated lawful meetings of as few as two activists*, Guardian, 18 November 2020, available at: https://www.theguardian.com/uk-news/2020/nov/18/undercover-police-officer-spied-on-womens-rights-group-inquiry-told

complete reliance is placed on the institutional oversight of the use of the powers.[127] As already noted at 2, above, this too is at odds with the EU requirements.

5. Is there an effective, independent and impartial oversight system over all aspects and phases of the surveillance/bulk data collection?

The European Court of Human Rights, in its *Big Brother Watch* judgment, found that several aspects of the Regulation of Investigatory Powers Act 2000 (RIPA), in force at the time of the violations alleged by the applicants in that case, violated the European Convention on Human Rights. This included:[128]

- A lack of robust end to end oversight of bulk interception acquisition, selection and searching processes; and
- Lack of controls on the use of communications data acquired from bulk interception.

RIPA was replaced by the Investigatory Powers Act 2016. As reported to the EU Fundamental Rights Agency:[129]

> The IPA largely replicates and expands the Regulation of Investigatory Powers Act 2000 (RIPA). It sets out a new oversight regime, the Investigatory Powers Commissioner, which [replaces] the existing regime, namely the Interception of Communications Commissioner, the Intelligence Services Commissioner and the Surveillance Commissioners. The Commissioner [is] supported by a number of Judicial Commissioners undertaking either authorisation or oversight and inspection functions. The Commissioner [is] also in charge of informing individuals about errors and their right to apply to the Investigatory Powers Tribunal.

Some of the changes were, however, less than explicit. Graham Smith discusses whether these have remedied the defects in RIPA as follows:[130]

> [The Investigatory Powers Act] introduces independent approval of warrants by Judicial Commissioners, but does it create the robust oversight of the end to end process, particularly of selectors and search criteria, that the Strasbourg Court requires?
>
> **The March 2015 ISC Report recommended that the oversight body be given express authority to review the selection of bearers, the application of simple selectors and initial**

---

127 See the quote from Graham Smith at point 2, above.

128 See Graham Smith, *What will be in Investigatory Powers Act Version 1.2?*, 30 October 2018, available at: https://www.cyberleagle.com/2018/10/what-will-be-in-investigatory-powers.html
The Court also found a violation in relation to the lack of safeguards on access to journalistically privileged material (as also discussed by Smith), which we will not address in this submission.

129 An Cuypers and David Harris, *Monthly report on reform of intelligence legislation in the EU Member States*, submitted by the Human Rights Law Centre of University of Nottingham to the FRA in the context of its project on National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies, covering the period January – April 2017, footnotes omitted, available at: https://fra.europa.eu/sites/default/files/fra_uploads/united-kingdom-study-data-surveillance-ii-monthly-data-collection-uk.pdf
The text has been changed to the present tense (as indicated in square brackets).

130 Graham Smith, Tuesday, *What will be in Investigatory Powers Act Version 1.2?*, 30 October 2018, available at:
https://www.cyberleagle.com/2018/10/what-will-be-in-investigatory-powers.html (emphases added)
Much more detailed descriptions and analyses of the relevant powers can be found in the upcoming 5th edition of Smith's book, Internet Law & Regulation, Chapter 8, *Lawful Access and Data Retetion*, in particular paras. 8-006 to 8-016.

search criteria, and the complex searches which determine which communications are read. David Anderson Q.C.'s (now Lord Anderson) Bulk Powers Review[131] records (para 2.26(g)) an assurance given by the Home Office that that authority is inherent in clauses 205 and 211 of the Bill (now sections 229 and 235 of the IP Act).

Beyond that, under the IP Act the Judicial Commissioners have to consider at the warrant approval stage the necessity and proportionality of conduct authorised by a bulk warrant. Arguably that includes all four stages identified by the Strasbourg Court ... If that is right, **the RIPA gap may have been partially filled**.

However, the IP Act does not specify in terms that selectors and search criteria have to be reviewed. Moreover, focusing on those particular techniques already seems faintly old-fashioned. The Bulk Powers Review reveals the extent to which more sophisticated analytical techniques such as anomaly detection and pattern analysis are brought to bear on intercepted material, particularly communications data. Robust end to end oversight ought to cover these techniques as well as use of selectors and automated queries.

The remainder of the gap could perhaps be filled by an explanation of how closely the Judicial Commissioners oversee the various selection, searching and other analytical processes.

Filling this gap may not necessarily require amendment of the IP Act, although it would be preferable if it were set out in black and white. It could perhaps be filled by an IPCO advisory notice: first as to its understanding of the relevant requirements of the Act; and second explaining how that translates into practical oversight, as part of bulk warrant approval or otherwise, of the end to end stages involved in bulk interception (and indeed the other bulk powers).

In other words, rather than oversight over "the selection of bearers, the application of simple selectors and initial search criteria, and the complex searches which determine which communications are read" being clearly and expressly provided for in the law (i.e., in the IPA), the issue has been left to an "assurance" from the Home Office to the Independent Reviewer of Terrorism Legislation that such oversight is "inherent" in various clauses in the Act. That is hardly a hard-and-fast legal assurance; the assurance was not even made by a minister in Parliament.

The situation in relation to oversight over complex selectors and search criteria is still unclear, while oversight over the much more sophisticated data mining analyses appears to not have been addressed.

In our opinion, this means the situation in this regard, too, clearly does not (yet) meet the EU standards as set out, in particular, in the CJEU *LQDN* judgment, referenced in this regard in the EEGs.

(We do not believe that this can be resolved by an "explanation" or an "IPCO advisory notice". Rather, we believe that the EU requirement that limits on surveillance must be set out in the law itself means that the situation will not be in accordance with the EU standards until the IPA itself is appropriately amended.)

131 Report of the Bulk Powers Review by David Anderson Q.C., Independent Reviewer of Terrorism Legislation, August 2016, available at: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf

6. Must individuals be notified that they have been under surveillance (unless that jeopardises the agencies' tasks)?

Section 231(1) IPA provides as follows:

> (1) The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person of which the Commissioner is aware if the Commissioner considers that—
>
> (a) the error is a serious error, and
>
> (b) it is in the public interest for the person to be informed of the error.
>
> (2) In making a decision under subsection (1)(a), the Investigatory Powers Commissioner may not decide that an error is a serious error unless the Commissioner considers that the error has caused significant prejudice or harm to the person concerned.
>
> (3) Accordingly, the fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

Indeed:

> The Investigatory Powers Commissioner may not inform the person to whom it relates of a relevant error except as provided by this section (para. (7))

In other words, there is no general duty on the part of the authorities to notify individuals whose data have been intercepted and analysed of that interference with their fundamental rights – not even if this informing can be done without jeopardising the tasks of the intelligence agencies, and indeed not even if it is clear that the interference amounted to a violation of their rights under the UK Human Rights Act, which transposed the ECHR into domestic law. Individuals must only be informed if there was a "serious error". This is manifestly deficient in terms of ECtHR case-law and the European Essential Guarantees for surveillance.[132]

Moreover, the Human Rights Act and the full application of the ECHR, and powers of judicial review, are generally under threat from the UK Government, which feels that these impose undue restrictions on the – in their view, unfetterable – sovereignty of the nation state, and the UK Parliament in particular.[133]

---

132 See section 3.1.2, point 7.1, above.

133 A letter from the UK Attorney-General to the Government dated 2 September 2020 about the question of whether Parliament (the UK legislator) was bound by international law was quoted in the press as saying that "*parliament is sovereign as a matter of domestic law and can pass any legislation it sees fit, including legislation which results in the UK contravening its international obligations under treaties or customary, international law*"; and that "*parliamentary sovereignty*" trumps all other legal matters. It concludes that:

> "*All law officers agree that it is an established principle of international law that a state, acting through its executive government, is obliged to discharge its treaty obligations in good faith. This is, and ought to remain, the key principle in informing the UK's approach to international relations.*
> *However, in the difficult circumstances in which we find ourselves, the attorney general and solicitor general consider it is important to remember that an established principle of international law is subordinate to the much more fundamental principle of parliamentary sovereignty.*"

7. Do individuals whose rights may have been unduly interfered with have access to an effective remedy to rectify any breach of their rights?

The remedy in question is the right that individuals have to apply to the Investigatory Powers Tribunal (IPT). In its *Kennedy* and *BBW* judgments, the ECtHR held that the Tribunal in principle fulfilled the requirements of an "independent tribunal" (court) in terms of Article 6 ECHR,[134] and that "*an examination of the IPT's extensive post-Kennedy case-law demonstrates the important role that it can and does play in analysing and elucidating the general operation of secret surveillance regimes*".[135] Indeed, the Court concluded that:[136]

> the IPT can – and regularly does – elucidate the general operation of surveillance regimes, including in cases where such elucidation is considered necessary to ensure the regime's Convention compliance.

There are two important issues in this regard. First, the above mainly applies in relation to the *exercise* of surveillance powers under the law.[137] In *Kennedy*, the Court had held that the IPT was not an effective remedy when it came to a challenge to the legal regime as such, partly because the IPT could not issue a "Declaration of Incompatibility" of the law with the Human Rights Act (i.e., in effect, with the ECHR).[138] Without endorsing the system of such declarations,[139] the Court found that:[140]

> as a general rule the IPT has shown itself to be a remedy, available in theory and practice, which is capable of offering redress to applicants complaining of both specific incidences of surveillance and the general Convention compliance of surveillance regimes.

Brexit advice: are ministers obliged to comply with international law?, Guardian, 10 September 2020, available at:
https://www.theguardian.com/politics/2020/sep/10/brexit-letter-are-mps-obliged-to-comply-with-international-law

On the intention to review judicial review in order to limit the powers of judges, see the Government Press Release of 31 July 2020, *Government launches independent panel to look at judicial review*, available at:
https://www.gov.uk/government/news/government-launches-independent-panel-to-look-at-judicial-review
This follows on from a pledge in the Conservative Party election manifesto to ensure judicial review is "not abused to conduct politics by another means or to create endless delays". As the Law Society Gazette points out, "*[t]he terms of reference [of the review panel] make it clear that the review aims to consider whether judicial review has encroached too far into the work of the executive branch of government.*" See *Government announces independent review of judicial review*, Law Society Gazette, 6 August 2020, available at:
https://www.lawgazette.co.uk/legal-updates/government-announces-independent-review-of-judicial-review/5105287.article

134 See *BBW* judgment, para.

135 *Idem*, para. 255.

136 *Idem*, para. 257.

137 See in particular the examples in the *BBW* judgment of the IPT's order for the destruction of email communications of Amnesty International which had been intercepted and accessed "lawfully and proportionately" in terms of domestic law but retained for longer than permitted under GCHQ's internal policies (para. 258, with reference to para. 54); and the finding of the IPT that for a period "the regime for the interception, obtaining, analysis, use, disclosure and destruction of legally privileged material had not been in accordance with the law for the purposes of Article 8 § 2 of the Convention and was accordingly unlawful" also under UK law (*Belhadi* case, para. 259, with reference to para. 93).

138 Under the HRA, because of the doctrine of absolute Parliamentary sovereignty (cf. footnote 133, above), the UK courts cannot declare an Act of Parliament to be invalid or void because it is incompatible with the HRA (i.e., with the ECHR). Instead, if they find that there is such a conflict, the must issue a "Declaration of Incompatibility", and it is then up to the Government and Parliament to remedy the situation.

139 *BBW* judgment, para. 264.

140 *Idem*, para. 265.

However, second, it should be noted that the Strasbourg Court took into account the fact that, at the time of its judgment, the UK was a Member State of the EU and that it, and the IPT, were therefore bound by directly applicable EU law including the Charter of Fundamental Rights:[141]

> The Court observes that [the main UK legal regime for surveillance examined by the Court in the case] has a clear basis in both section 22 of RIPA and the ACD Code [the then-applicable rules]. However, as a Member State of the European Union, the Community legal order is integrated into that of the United Kingdom and, where there is a conflict between domestic and law and EU law, the latter has primacy.

In the case at hand, the Government had conceded that the relevant legal regime was incompatible with EU law, and "[f]ollowing this concession, the High Court ordered that the relevant provisions of the IPA should be amended" by a specified date.[142] Because this had not yet been done at the time of the judgment, the Strasbourg Court found there was, at that time, still a violation of the Convention.[143]

In other words, the remedies accorded by the IPT were essentially held to be effective in terms of the ECHR, partly because the Tribunal was clearly independent and impartial, and issued strong rulings in appropriate cases – but also because in its rulings it had the power and the duty to ensure that both practice and the law were compliant with EU law including the Charter of Fundamental Rights.

But of course, this will fundamentally change from 1 January 2021, when the IPT will no longer be able to rely on EU law (including the Charter) in assessing the validity of various elements of the UK surveillance regime – which we have found to be deficient in several respects.

In our opinion, this raises serious doubts as to whether, at least in relation to the compatibility of the legal regime as such with European fundamental rights standards, the IPT will still be able to provide a judicial remedy in terms of Article 6 ECHR, or even an "effective remedy" in terms of Article 13 ECHR, or an "effective remedy before a tribunal" in terms of Article 47 of the Charter (to which much attention was given by the CJEU in its *Schrems II* judgment).

8. If the UK were to be granted a positive adequacy decision, would the protection of the GDPR and Article 8 of the Charter be undermined by the arrangements for data sharing between the UK and the US intelligence agencies?

We established in section 2.4, above, that the UK shares most if not all of the data it collects in bulk from the underseas cables, and the results of its "simple", "complex" and even more sophisticated, algorithm/AI-based analyses, with the US NSA (and the other "5EYES" agencies). Indeed, as shown there, to a large extent those activities are carried out jointly by the UK GCHQ and the US NSA.

We also already concluded there that in terms of the GDPR, this sharing will, at least from 1 January 2021, involve the "onward transfer" of the data on individuals in the EU from the UK to the USA.

Article 45 GDPR expressly notes that the GDPR conditions for transfer of personal data from the EU to a third country must be complied with both in relation to the direct transfer from

141 *Idem*, para. 466.
142 *Idem*.
143 *Idem*, para. 268.

the EU to the relevant third country, and in relation to onward transfers from the third country to another third country. This is also affirmed in the EDPB-endorsed "Adequacy Referential"[144] and in the draft new standard contract clauses (SCCs) for transferring personal data to non-EU countries, issued by the European Commission on 12 November 2020[145]

The EDPB, in its very recently issued recommendations on supplementary measures that may be required for transfers to third countries that indulge in mass surveillance,[146] emphasises that the EU-based data exporter and the third country data importer should, in this, "not forget to also take into account onward transfers."[147]

In our opinion, the fact that data on individuals in the EU, extracted in bulk from the underseas cables by GCHQ, and the results of the analyses of those data, will be shared with the USA – which has been specifically held to not provide "adequate"/"essentially equivalent" protection to personal data in *Schrems II* – clearly stands in the way of the granting of an positive adequacy decision to the UK. Such a decision should not – in our opinion, legally may not – be granted unless and until the UK amends its intelligence data sharing agreement (i.e., the UKUSA Agreement) to limit the intelligence data sharing in a way that is compatible with European fundamental rights law.

9. Does data-mining by GCHQ involve the taking of fully-automated decisions on the individuals concerned, based on profiling?

In section 2.3.3, above, we have concluded that GCHQ, like the US NSA – indeed, it would again appear, jointly with the NSA – carries out in-depth profiling and algorithmic/AI-based analyses of the bulk data it extracts from the underseas cables, and of the other bulk personal datasets to which it has access (which all together create Big Data datasets); that this algorithmic datamining results in individuals being "identified" (read: labelled) as "Subjects of Interest" and then placed under further, intrusive surveillance; and that this activity suffers from in-built and largely unavoidable problematic features: the "base-rate fallacy" that inescapably leads to excessive "false positives" or "false negatives" (or both); conscious or unconscious biases; and (because of the complexity of self-learning algorithms) unchallengeability.[148]

The "identification" (labelling) of an individual as a "Subject of Interest" can have serious repercussions, e.g., in relation to job prospects, access to education, travel (including bans on access to certain countries) – and in some cases, arrest and detention.

In our opinion, any decision in relation to an individual based on the algorithmic analyses carried out by GCHQ (together with the US NSA) constitutes a "decision based solely on automated processing, including profiling, which produces legal effects concerning [that individual] or similarly significantly affects him or her". In the EU, the taking of such a decision

144 See Part One, section 2.1.

145 The draft new clauses and the implementing decision covering them are available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries

146 EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, (footnote 115, above).

147 *Idem*, para. 10, on p. 9.

148 For brief details and further references, see section 2.3.3, under the heading "*Identifying new threats and previously unknown persons 'of interest' through more sophisticated data mining*".

is in principle prohibited, subject to very limited exceptions (Article 22(1) GDPR). Even when authorised by EU or EU Member State law, the law in question must "lay[ ] down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests" (Article 22(2)(b)).

Leaving aside the question of whether it can be argued that GCHQ is itself directly subject to the GDPR because, although it is a third country entity, it "monitors the behaviour of individuals in the EU",[149] if personal data that are transferred from the EU to a third country can, in that third country, after transfer, be subjected to processing that does not meet the requirements of Article 22 GDPR, then it follows that that third country does, in this respect at least, not ensure "adequate"/ "essentially equivalent" protection to that accorded in the EU under the GDPR.

In our opinion, the carrying out of automated profiling by GCHQ (in cooperation with the US NSA), and the taking of decisions about individuals – including EU individuals – on the basis of the (secret) results of that profiling, does not meet the requirements of Article 22 GDPR – and this deficiency in UK law and practice, too, stands in the way of a positive adequacy decision on the UK.

3.3 Conclusions

In summary, our conclusions are as follows:

As to the UK surveillance practices:

- The UK, working jointly with the US NSA, taps into a large number of Internet communications links (especially but not only the undersea cables), including cables through which most of the communications of EU individuals, institutions and officials travel (in particular, most EU – UK – USA communications). These communications include not only emails and social media exchanges, but also frequently the data flows between EU users of US-based cloud services and the relevant US cloud servers.
- Very large amounts of data – including all communications metadata (including traffic and location data) are extracted by the UK from all selected bearers indiscriminately, in bulk, and retained for some time.
- The metadata are highly revealing of the lives of the tens or hundreds of thousands of individuals to which they may relate, but the vast majority of data subjects to which the metadata relate – which for many bearers will include large numbers of EU persons – will have no links with terrorism, threats to national security or serious crime.
- While much of the other data are filtered out fairly quickly through "simple" or "complex" queries, the metadata are retained for longer, to allow for their use in algorithmic analyses and profiling.
- At least some of the data including content data will be filtered out for further inspection for purposes that are not aimed at countering serious threats to national

[149] See section 3.1.3, at ii, above. We address the implications briefly in section 4.4.2 of the Executive Summary.

security, but rather, to gain some politically or economically advantageous insights into actions of adversaries and allies alike.

- The not-filtered-out data, including all metadata, are subject to automatic analyses by means of self-learning (AI-based) algorithmic datamining, to "identify" (i.e., label) or link individuals as/to "Subjects of Interest" ("SoI") – but this processing suffers from major, unavoidable defects: built-in biases, mathematically unavoidable excessive numbers of "false positives" or "false negatives" (or both), and the fact that because of their complexity they become effectively unchallengeable. It is unavoidable that many individuals who are labelled or linked to "SoI" are innocent and have no links to serious crime or terrorism.

As to the law:

- Under the "UK GDPR" that will apply from 1 January 2020, metadata are not meaningfully protected against undue access and bulk collection by the UK intelligence agencies.
- The UK Investigatory Powers Act clearly does not "itself define" the scope and limitations of the use of the powers it grants the intelligence agencies, in particular in relation to direct access to the systems of communication and Internet service providers, or to direct tapping into the underseas cables. The IPA therefore does not meet the requirement set in that regard by the CJEU in *Schrems II*.
- The UK IPA rules that allow for the extraction, in bulk, of at least all the metadata of all communications that flow through a selected bearer, are clearly incompatible with the standards set out in a range of CJEU judgments and arguably (given the now-recognised inherent sensitivity of metadata) compromises the very essence of the rights to privacy, confidentiality of communications and data protection.
- UK law allows for broadly phrased bulk interception warrants and for vague search criteria applied to stored data; the law itself does little to preclude targeting of improper targets. Rather, almost complete reliance is placed on the institutional oversight of the use of the powers. This too is at odds with the EU requirements.
- Rather than oversight over "the selection of bearers, the application of simple selectors and initial search criteria, and the complex searches which determine which communications are read" being clearly and expressly provided for in the law (i.e., in the IPA), the issue has been left to an "assurance" from the Home Office to the Independent Reviewer of Terrorism Legislation that such oversight is "inherent" in various clauses in the Act. That is hardly a hard-and-fast legal assurance; the assurance was not even made by a minister in Parliament.

  The situation in relation to oversight over complex selectors and search criteria is still unclear, while oversight over the much more sophisticated data mining analyses appears to not have been addressed.

  This means the situation in this regard, too, clearly does not (yet) meet the EU standards as set out, in particular, in the CJEU *LQDN* judgment, referenced in this regard in the EEGs.
- The Human Rights Act and the full application of the ECHR, and powers of judicial review, are generally under threat from the UK Government which feels that these

impose undue restrictions on the – in their view, unfetterable – sovereignty of the nation state, and the UK Parliament in particular.

- The remedies accorded by the IPT were essentially held to be effective in terms of the ECHR, partly because the Tribunal was clearly independent and impartial, and issued strong rulings in appropriate cases – but also because in its rulings it had the power and the duty to ensure that both practice and the law were compliant with EU law including the Charter of Fundamental Rights.

  But of course, this will fundamentally change from 1 January 2021, when the IPT will no longer be able to rely on EU law (including the Charter) in assessing the validity of various elements of the UK surveillance regime – which are deficient in several respects.

  This raises serious doubts as to whether, at least in relation to the compatibility of the legal regime as such with European fundamental rights standards, the IPT will still be able to provide a judicial remedy in terms of Article 6 ECHR, or even an "effective remedy" in terms of Article 13 ECHR, or an "effective remedy before a tribunal" in terms of Article 47 of the Charter (to which much attention was given by the CJEU in its *Schrems II* judgment).

- The fact that data on individuals in the EU, extracted in bulk from the underseas cables by GCHQ, and the results of the analyses of those data, will be shared with the USA – which has been specifically held to not provide "adequate"/"essentially equivalent" protection to personal data in *Schrems II* – clearly stands in the way of the granting of an positive adequacy decision to the UK. Such a decision should not – in our opinion, legally may not – be granted unless and until the UK amends its intelligence data sharing agreement (i.e., the UKUSA Agreement) to limit the intelligence data sharing in a way that is compatible with European fundamental rights law.

- The carrying out of automated profiling by GCHQ (in cooperation with the US NSA), and the taking of decisions about individuals – including EU individuals – on the basis of the (secret) results of that profiling, does not meet the requirements of Article 22 GDPR – and this deficiency in UK law and practice, too, stands in the way of a positive adequacy decision on the UK.

OVERALL CONCLUSION:

In our opinion, it is highly doubtful whether the processing of personal data by UK intelligence agencies, especially its bulk collection of communication data, is in line with the EU Charter of Fundamental Rights. In particular, its indiscriminate bulk collection of communications metadata ("related communications data") from selected "bearers" in the underseas communication cables would appear to be contrary to principles established by the European Court of Human Rights (*Big Brother Watch v. the UK*) and the CJEU (*Tele2/Watson*, *Digital Rights*, *Schrems II*, *Privacy International* and *La Quadrature du Net*), as reflected in the recent EDPB's "European Essential Guarantees for Surveillance Measures".

In our opinion, the UK can therefore not be granted a positive adequacy decision under Article 46 GDPR.

We briefly discuss some of the implications in the section of implications that is part of the Executive Summary of our submission, provided separately.

- o – O – o -