Department for
Science, Innovation
& Technology

Analysis of the UK Extension to the EU-US Data Privacy Framework

September 2023

Any enquiries regarding this publication should be sent to us at:
alt.formats@dsit.gov.uk.

Contents

Introduction

Section 17A of the Data Protection Act 2018[1] ("DPA 2018") empowers the Secretary of State to make adequacy regulations (also known informally as "*data bridges*") to permit the free flow of personal data to another country[2] if the Secretary of State considers that the country provides an adequate level of protection for personal data. In accordance with Article 44 of the UK General Data Protection Regulation[3] ("UK GDPR"), when doing so the Secretary of State must be satisfied that the level of protection of personal data will not be undermined after the personal data is transferred to the third country. The Secretary of State can specify that an adequate level of protection is provided for all transfers to a country, or can limit the specification to certain transfers to that country. Article 45(2) of the UK GDPR sets out a list of particular matters which the Secretary of State must take into account when assessing whether a country provides the necessary level of protection.

Once a country is the subject of adequacy regulations, UK controllers and processors can make transfers of personal data that are within the scope of the regulations freely, without requiring additional safeguards such as standard contractual clauses. As such, adequacy regulations are the most straightforward mechanism for controllers and processors seeking to transfer personal data overseas.

A country's data protection regime does not need to provide a point-to-point replication of UK GDPR in order to provide an adequate level of protection. Rather, it is through a comprehensive assessment of the substance of data protection rights and their effective implementation, supervision and enforcement, as well as an assessment of related provisions, that the Department for Science, Innovation and Technology ("DSIT") determine whether the system in a country provides a sufficient level of protection for data subjects.

DSIT has therefore analysed the relevant legal framework and practice in the US in relation to the UK Extension to the EU-US Data Privacy Framework ("UK Extension") in order to determine whether it provides an adequate level of protection for personal data.

On the basis of the analysis set out below, DSIT considers that the provisions of the UK Extension and other relevant US laws and practices provide an adequate level of protection for UK personal data, and do not undermine the level of protection that UK data subjects enjoy under the UK GDPR, when that data is transferred to certified US organisations.

[1] https://www.legislation.gov.uk/ukpga/2018/12/section/17A

[2] The Secretary of State can also designate a territory or one or more sectors within a third country, or an international organisation. See Section 17A(1) UK DPA 2018.

[3] https://www.legislation.gov.uk/eur/2016/679/article/44

Context

DSIT has assessed the level of protection provided by the UK Extension. The EU-US Data Privacy Framework ("DPF") was set up and is administered by the US Department of Commerce ("DoC").[4] The DPF is a framework consisting of the Principles, Supplemental Principles and Annex I of the Principles ("the DPF Principles") which provides protections for personal data transferred from the EU to certified US organisations. The full text of the DPF is included at Annex A. In order to self-certify, eligible US organisations must agree to comply with the DPF Principles and make a public commitment to do so via a published privacy policy. The DPF is a voluntary self-certification framework that US organisations may choose to join. The DPF Principles take the form of requirements in relation to data protection and set out requirements on how an organisation collects, processes and discloses personal data.

The DoC has agreed to extend the DPF, and the protections that exist under it, to personal data transferred from the UK to certified US organisations, under the UK Extension.[5] Organisations may elect to utilise the DPF where they are acting as processors for UK organisations or where they have a controller-controller transfer relationship with a UK organisation.

Once organisations in the US have successfully self-certified to the DPF they are included on the Data Privacy Framework List[6] ("DPF List") on the Data Privacy Framework website ("DPF Website"). Organisations who have self-certified to the DPF (to receive personal data from the EU) may also elect to be certified under the UK Extension by making additional UK-specific commitments within their public commitments and indicating on their self-certification to the DoC that they are electing to participate in the UK Extension.[7] Though self-certification to the DPF is voluntary, once an organisation has made a public commitment,[8] any non-compliance with those commitments and the DPF Principles can be enforced under US law.[9]

The DPF List maintained by the DoC includes a specific programme filter for the UK Extension to enable UK businesses an easily accessible route to identify businesses in the US who are participating in the UK Extension, and therefore will be protecting UK personal data in line with the DPF Principles.

[4] The Privacy Shield framework was set up to replace the Safe Harbor programme in 2016 in the wake of the *Schrems I* judgment of the CJEU which invalidated the previous adequacy decision. The EU-US DPF now amends the Privacy Shield following the July 2020 *Schrems II* judgment which invalidated the adequacy decision enabling the transfer of personal data from the EU via the Privacy Shield framework.

[5] For the purposes of the UK Extension, references to the European Union ("EU"), European Commission, EU Data Protection Authorities (DPAs) and EU individuals, areare read in the context of transfers from the UK and Gibraltar to refer to the UK, UK government, the ICO and UK individuals, to refer to the UK, UK government, the ICO and UK individuals, reflective of the differences between the UK and Gibraltar, and the EU.

[6] https://www.dataprivacyframework.gov/s/participant-search

[7] https://www.dataprivacyframework.gov/s/article/How-to-Join-the-Data-Privacy-Framework-DPF-Program-part-1-dpf and https://www.dataprivacyframework.gov/s/article/FAQs-Privacy-Policy-1-5-dpf

[8] The requirements and procedure for self-certification can be found within DPF Supplemental Principle 6 and on the DPF Website (https://www.dataprivacyframework.gov/s/article/Self-Certification-Information-dpf).

[9] Section 5 of the FTC Act and 49 U.S.C. §41712.

This DPF is administered by the DPF Team in the International Trade Administration (the "ITA") of the DoC and enforced by the Federal Trade Commission ("FTC") and Department of Transportation ("DoT"). Only organisations that are under the regulatory remit of the FTC or DoT are eligible to join the DPF and confirming this eligibility is one aspect of the self-certification process (see section on 'Scope and Definitions').

To confirm the extension of the protections under the DPF to personal data transferred from the UK under the UK Extension, and to support the functioning of the UK Extension, the US government, the FTC and the DoT have shared letters with the DSIT Secretary of State outlining further commitments and reassurances concerning the administration, functioning and enforcement of the DPF. These letters are as follows:

- Department of Commerce letter from Secretary of Commerce Gina M. Raimondo, dated 14 July 2023 (Annex B)
- International Trade Administration (Department of Commerce) letter from Under-Secretary for International Trade Marisa Lago, dated 13 July 2023 (Annex C)
- Federal Trade Commission letter from Chair, Federal Trade Commision, Lina M. Khan, dated 13 July 2023, including Appendix A (*"Privacy Shield and Safe Harbor Enforcement"*) (Annex D-1 and D-2, as letter and appendix, respectively).
- Department of Transportation letter from Secretary of Transportation Pete Buttigieg, dated 14 July 2023 (Annex E)
- Department of Justice letter from Deputy Assistant Attorney General and Counselor for International Affairs Bruce C. Swartz, dated 14 July 2023 (Annex F).
- Office of General Counsel of the Office of the Director of National Intelligence, Christopher C. Fonzone to Leslie B. Kiernan, General Counsel of the U.S Department of Commerce, dated 9 December, 2022 (Annex G).

Legislative Framework and Commitment to Data Protection

Overview

The Data Protection Act 2018 empowers the Secretary of State to make regulations finding that a country, territory, sector, or international organisation ensures an adequate level of protection for personal data, pursuant to Article 45 of the UK GDPR. In assessing a country's level of protection, the Secretary of State must take into account the rule of law, respect for fundamental rights and freedoms, the existence of an effective and independent supervisory authority, and any relevant international commitments.[10]

As part of its assessment of the UK Extension, DSIT has conducted an analysis of the US with respect to the aforementioned areas. In assessing the rule of law and respect for human rights and fundamental freedoms[11] in the US, DSIT has taken into account the differences in legal and cultural traditions that exist in the UK and the US. DSIT's assessment does not directly compare the UK and US in this regard.

Constitutional and Legislative Framework

The US is a federal republic of states and non-state territories, which together form a political union administered and governed by a federal government in accordance with the US Constitution.

The US is a mature democracy, with established checks and balances on the exercise of political authority. The US Constitution enshrines the separation of powers of the executive, judiciary and legislature. The Constitution also divides political authority between the states and the federal government. Whilst states retain a number of powers and exclusive areas of jurisdiction, the Constitution restricts the ability of states to infringe on the fundamental rights of US persons established in the Constitution. The World Justice Project Rule of Law Index 2022 ranks the US 26th out of 140 countries worldwide, with the US consistently placing within the top 30 countries of the index since its inception in 2015.[12]

As the elected head of state, the US President has broad powers to manage national affairs and run the executive branch.[13]

The laws of the US are interpreted and applied by the US judiciary, whose independence is guaranteed under Article III of the Constitution. Legal jurisdiction is divided between federal and

[10] Sections 17A (and 74A) and 17B(12) and 74B of the UK DPA 2018.

[11] Article 4(28) of the UK GDPR.

[12] https://worldjusticeproject.org/rule-of-law-index/global/2022/United%20States/historical

[13] The legislative branch has the power to approve Presidential nominations, control the budget, and can impeach the President and remove him or her from office. There are limits on how long a President can serve: they are elected for a four-year term, with a two-term limit stated in the 22nd Amendment.

state courts, with the Constitution serving as supreme law in both systems. The federal government has jurisdiction over cases involving federal laws and statutes, treaties with foreign nations, and cases involving foreign governments. State jurisdiction applies in other areas such as contract and criminal law.

Article III of the Constitution governs the appointment, tenure, and payment of Supreme Court justices, and federal circuit and district judges. These judges, often referred to as "*Article III judges*," are nominated by the president and confirmed by the US Senate. In particular, judicial independence is ensured through:

- The independence of the judiciary is enshrined in Article III of the Constitution, and all other governmental branches are required to respect this. The judiciary has the power to decide on all matters in front of them, with complete authority to decide on the issues.
- Judges are bound by the Code of Conduct for US Judges.[14] In particular, this contains requirements for judges to carry out their roles impartially, fairly and with integrity, and to uphold the independence of judiciary.
- Article III states that these judges "*hold their office during good behaviour*," which means they have a lifetime appointment, except under very limited circumstances. Article III judges can be removed from office only through impeachment by the House of Representatives and conviction by the Senate. Article III judgeships are created by legislation enacted by Congress.
- The Constitution also provides that judges' salaries cannot be reduced while they are in office. Article III judicial salaries are not affected by geography or length of tenure.

The US Supreme Court is the highest federal court in the United States. Justices are appointed for life by the President, subject to a confirmation by the Senate. The Supreme Court hears cases from lower federal courts as the highest court of appeal, as well as cases that involve issues of federal law or the interpretation of the Constitution. The Court exercises its power of judicial review in hearing challenges on constitutional grounds to recent laws and the actions of the other branches.

This analysis shows that the US respects the rule of law and, in conjunction with the other parts of the analysis, demonstrates how the US provides an adequate level of protection for data subjects.

Human Rights and Fundamental Freedoms

The US has a history of respecting human rights and fundamental freedoms and promoting their expansion domestically and has publicly committed to supporting and strengthening rights and

[14] https://www.uscourts.gov/judges-judgeships/code-conduct-united-states-judges#:~:text=(1)%20A%20judge%20should%20be,decorum%20in%20all%20judicial%20proceedings

freedoms within the US.[15] The US is characterised by its protections for freedoms of expression and religious belief, and a wide array of other civil liberties, including freedom of appropriate conditions of confinement and protection from excessive force and unlawful intrusions into personal privacy.

The US does not currently have a comprehensive federal privacy statute, however there are numerous sector-specific privacy and data security laws that exist in federal law. State and local authorities have in many cases also implemented their own privacy and data protection laws.[16]

Whilst there exists no explicitly enumerated right to privacy in the Constitution, Supreme Court rulings have established the existence of a '*right to privacy*' read into the Constitution,'[17] as well as elaborating a legal doctrine of a reasonable '*expectation of privacy*'.[18]

The Constitution enumerates a number of rights and liberties[19] for US persons,[20] which may not be infringed upon by state or federal authorities, and are rigorously enforced by the judiciary. These rights in many instances coincide with human rights listed in the Universal Declaration of Human Rights ("UDHR"), including but not limited to the rights to freedom of the press, speech and religion, protections against cruel and unusual punishment and the right to due process before the courts. The US played a leading role in the creation of the UDHR.[21]

The Equal Protection[22] and Due Process clauses[23] in the Constitution guarantee equal treatment and protection before the law for all individuals. Individuals (including non-US persons) charged with a crime in US courts have a Fifth Amendment protection against unlawful seizures by the US government, and may exercise this right to exclude evidence obtained unlawfully.[24]

Discrimination on the basis of race, colour, religion, nationality and sex are prohibited by the Civil Rights Act of 1964, and illegal under the Equal Protection clause of the Constitution.[25] The US

[15] https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/08/fact-sheet-the-biden-harris-administration-is-taking-action-to-restore-and-strengthen-american-democracy/

[16] Examples include the California Consumer Protection Act 2018 and the California Privacy Rights Act 2020 ("CPRA"). A comprehensive evaluation of non-federal privacy laws is outside the scope of this analysis

[17] See *Griswold v. Connecticut, 381 US 479 (1965)* inferred the existence of a right to privacy as existing in the '*penumbras*' of the protections offered by the Bill of Rights in the 1st, 3rd, 4th, 5th and 9th Amendments https://supreme.justia.com/cases/federal/us/381/479/

[18] See *Katz v. United States, 389 US 347 (1967)* https://supreme.justia.com/cases/federal/us/389/347/

[19] 9th Amendment allows for US courts to identify and establish 'unenumerated' rights for US persons implicit in those specifically protected by the Constitution, such as the right to privacy.

[20] Collectively referred to as the *'Bill of Rights*'

[21] https://www.un.org/en/about-us/universal-declaration-of-human-rights

[22] US Constitution, 14th Amendment (https://www.law.cornell.edu/constitution/amendmentxiv)

[23] US Constitution, 5th Amendment (https://www.law.cornell.edu/constitution/fifth_amendment)

[24] Fifth Amendment protection against unlawful seizure is treated at great detail in the Law Enforcement section of this analysis

[25] See *Brown v. Board of Education of Topeka, 347 US 483 (1954)* ruled the existing practice at the time of racially segregating public schools to be unconstitutional under the Equal Protection Clause. https://supreme.justia.com/cases/federal/us/347/483/#tab-opinion-1940809

Commission on Civil Rights is a bipartisan and independent commission tasked with investigating civil rights violations within the US and reports to Congress.[26]

Whilst Civil Rights Act protections are limited to the characteristics listed above, further protections guaranteeing individuals the right to not be discriminated against exist in US statute and case law. The Americans with Disabilities Act of 1990 and the Rehabilitation Act of 1973 protect individuals with disabilities against discrimination by federal, state and local governments, and the Pregnancy Discrimination Act and the Equal Pay Act prohibits discrimination against women in the workplace.

The US Department of Justice enforces federal laws that prohibit discrimination on the basis of race, colour, national origin, sex, disability and religion. The DoJ is responsible for investigating and prosecuting cases of discrimination in areas such as voting rights, fair housing, education, employment, and access to public accommodations. It also works to ensure that law enforcement agencies comply with constitutional and federal statutory requirements, and it provides training and technical assistance to help prevent and address civil rights violations.

This analysis shows that the US respects human rights and fundamental freedoms[27] and, in conjunction with the other parts of the analysis, demonstrates how the US provides an adequate level of protection for data subjects.

International Commitments

The US has evidenced its respect for human rights on the international stage through its involvement in international agreements and treaties. The US is party to a number of international agreements and treaties which include commitments and guarantees concerning an individual's right to privacy and human rights more generally.

Treaties ratified by the US in this area include the International Covenant on Civil and Political Rights,[28] the International Convention on the Elimination of All Forms of Racial Discrimination[29] and the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.[30]

[26] An example of the work of the Committee can be found in its most recent report: https://www.usccr.gov/files/2022-09/2022-statutory-report-fema.pdf

[27] Article 4(28) of the UK GDPR

[28] International Covenant on Civil and Political Rights (ICCPR), (https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights)

[29] International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), (https://www.ohchr.org/en/instruments-mechanisms/instruments/international-convention-elimination-all-forms-racial)

[30] Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT),(https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-against-torture-and-other-cruel-inhuman-or-degrading)

The US is a signatory to the Convention on the Rights of Persons with Disabilities[31] the Convention on the Rights of the Child[32] and the International Covenant on Economic, Social and Cultural Rights,[33] all of which include some form of guarantees on individuals' right to privacy. The US is a participating member of the Budapest Convention on Cybercrime.[34]

The "*Agreement between the government of the United States of America and the government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime*"[35] is a bilateral agreement between the UK and the US. The agreement puts in place a mechanism by which authorities can request electronic data relevant to the investigation of a serious crime directly from a provider without going through the Mutual Legal Assistance Treaty ("MLAT") process and contains privacy protections in the form of several targeting and data minimisation procedures, as well as limitations on use and transfer and privacy safeguards.

The US is also an active participant in a number of international organisations focusing on facilitating international data transfers whilst maintaining data protection. In particular:

- As a member of the Organisation for Economic Co-operation and Development ("OECD"), the US has committed on the international stage to the standards set out in the OECD Privacy Framework, and played a key role in the drafting of the OECD's '*Declaration on Government Access to Personal Data held by Private Sector Entities*'.[36]
- The US participates in the Asia-Pacific Economic Cooperation ("APEC") Cross-Border Privacy Rules ("CBPR") System and is a member of the Global Cross Border Privacy Rules Forum, which was established to globalise the CBPR System.[37]

The US has been involved in efforts within the G7 to better define international standards on international data transfers, and contributed in this capacity to the G7 Data Protection and Privacy Authorities Roundtable's publication on '*Data Free Flow with Trust*' last year in September 2022.

DSIT considers that this analysis demonstrates that the US has entered into international commitments and, in conjunction with the other parts of the analysis, evidences how the US provides an adequate level of protection for data subjects.

[31] Convention on the Rights of Persons with Disabilities (CRPD), (https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities)
[32] Convention on the Rights of the Child (CRC), (https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child)
[33] International Covenant on Economic, Social and Cultural Rights (ICESCR), (https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights)
[34] https://rm.coe.int/1680081561
[35] https://www.justice.gov/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern
[36] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487
[37] For a more detailed treatment of the CBPRs and the onward transfer restrictions, please refer to the below section on the '*Focus On International and Onward Transfers*'.

Legislative Framework & Commitments Conclusion

On the basis of this analysis, DSIT considers that the US respects and maintains the rule of law in its constitutional and legislative framework, and that the US respects human rights and fundamental freedoms.

The UK Extension to the EU-US Data Privacy Framework

Framework Applying to the Processing of Personal Data

Scope and Definitions

Our assessment is limited solely to transfers of personal data which will be subject to the UK Extension, which explicitly excludes the transfer of journalistic data in accordance with Supplemental Principle 2 (Journalistic Exceptions).[38] Only personal data covered by the definitions and scope of the DPF may be transferred from the UK. Where US organisations wish to receive personal information collected in the context of an employment relationship (i.e., Human Resources ("HR") data), they may do so under the DPF. However, they are required to specifically notify the US DoC that they wish to do so under their certification and they are required to commit to cooperate with investigations and the advice of the UK Information Commissioner's Office ("ICO") (see the section on '*Redress*' regarding the UK Extension to the EU-US Data Privacy Framework below for further information).

Of note, there are various state and sectoral laws within the US that may provide additional protections for personal data and further mitigations to supplement the protections under the DPF. The DPF accounts for this in the Overview section, highlighting that where there are conflicts in requirements and where organisations have the option to do so, they are expected to opt for the higher level of protection. This may be beneficial in helping to bring in rights and protections which may not be evident under the DPF and provide further protections for UK data subjects whose personal data has been transferred under the DPF. However, the scope of our assessment is limited solely to transfers under the UK Extension, and the protections of the DPF itself. Though there may be additional protections from state or sectoral law, these should be taken as additional, rather than foundational. It is also important to consider the limitations of such protections, in that the level of protection may vary and may not be applicable to all data transferred, depending on the state or sector in which a US organisation resides.

As explained in this analysis, the DPF Principles are framed in EU terminology reflecting the EU-US negotiations to establish the DPF itself, and to reflect the EU's laws and practices in relation to data protection and privacy. However, the DoC (and other relevant authorities) have agreed to extend the protections of the DPF Principles and the DPF to personal data transferred from the UK, as set out in their letters.[39]

[38] This is defined as personal data that is collected for "*publication, broadcast or other forms of public communication of journalistic material and information in previous published material disseminated from media archives*".

[39] Annex B (DoC Letter) and Annex C (ITA Letter).

As such, in the ITA letter to the Secretary of State[40] certified US organisations participating in the UK Extension will be required to treat personal data shared under the UK Extension in accordance with DPF Principles. Additionally, the letters clarify that, where appropriate under the DPF, references to the EU (i.e., the European Commission, EU data subject, EU Data Protection Authorities ("DPAs"), etc) should be understood as referring to the UK and relevant UK bodies or data subjects. All references to the DPF through this assessment, should be read in line with this understanding.

Additionally, though the FTC and DoT have committed to enforcement of the UK Extension under their letters sent to the Secretary of State.[41] It is helpful to note that relevant laws (i.e., those enabling and regulating enforcement by the FTC and the DoT, e.g. Section 5 FTC Act) are written in plain terms and do not differentiate between nationalities or the origin of the data transferred to certified US organisations.

The key concepts and definitions of the DPF are based on (and, in some cases, directly reference) the definitions set out within the EU General Data Protection Regulation ("EU GDPR"). They are aligned with the UK's definitions and concepts in this area as set out in UK data protection legislation.

Personal Data is defined as any data about "*an identified or identifiable individual*" that is within the scope of the EU GDPR, which (in the context of the UK Extension) is received by a certified US organisation from the UK.[42]

- The DPF also defines '*Key-coded Data*' as a type of research data under Supplemental Principle 14(g).[43] Such data has been uniquely '*key-coded*' at its origin with the specific key-code only held by the principal researcher and not shared. Data encoded in this way, which is considered to be personal data under the UK GDPR would be covered by the DPF.
- HR data is defined under Supplemental Principle 9(a)(i) as personal information about employees (past or present) collected by an organisation in the context of the employment relationship.
- Public Record information,[44] defined within Supplemental Principle 15(a), is set out to mean records kept by government agencies or entities at any level that are open to consultation by the public in general. Such information is not subject to the Notice, Choice or Accountability for Onward Transfer Principles as long as i) it is not combined with non-public record information, and ii) any conditions for consultation established by the relevant jurisdiction are respected.
- Within Personal Data, some information may be considered of a more sensitive nature. Sensitive information is defined under the Choice Principle 2(c), as personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious

[40] Annex C (ITA Letter), footnote 3.

[41] See Annex D-1 (FTC Letter) and Annex E (DoT Letter).

[42] DPF Overview(8)(a).

[43] Key-coded data is a type of research data coded at their origin. When such data is shared the specific coding key is not shared and only held at the origin so that data can re-identified if needed. This is essentially a form of "*pseudonymisation*".

[44] Separate to "*personal data*" collected from publicly available sources.

or philosophical beliefs, trade union membership or information specifying the sex life of the individual, but the DPF goes on to clarify that certified US organisations should also treat as sensitive, personal information received from a third party where the third party itself treats the information as sensitive and has identified it as such.

Processing is defined as any operation or set of operations which is performed upon personal data, whether or not by automated means, "*such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction"*.[45] The list provided within the DPF, though not identical to the definition under the UK GDPR, is set out as a list of ways data could be processed. Ultimately, the definition includes "*any operation or set of operations*" performed upon personal data.

The DPF does not make a distinction between certified US organisations acting as controllers and those acting as processors for UK organisations with respect to DPF applicability. All certified US organisations are subject to the DPF Principles and requirements. In terms of onward transfers, a distinction is made between transfers from a certified US organisation to other parties acting as controllers, ("*a person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data*") and those to other parties acting as an '*agents*' ("*who perform task(s) on behalf of and under the instructions of the organisation*").[46]

The DPF does not contain a glossary of terms to define specific terms or uses throughout.The FTC's authority for enforcement of the DPF is broad, in reliance on their enforcement powers under the FTC Act. Though there may be some vagueness in some of the terms used, the FTC has shown itself to err on the side of higher individual protections when applying the terms of privacy frameworks in enforcement action.[47]

Sensitive data

The DPF specifically highlights sensitive information as information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual.[48] This list is somewhat analogous to the definition provided for special category data under the UK GDPR,[49] with the exception of biometric, genetic and sexual orientation personal data which are not included under the DPF list.

However, under the DPF, the list of sensitive information is set out as an example non-exhaustive list and requires that certified US organisations "*should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive*".

[45] DPF Overview(8)(b).

[46] '*Agents*' are comparable to the UK concept of "*processors*" under the UK GDPR. DPF Overview(8)(c) and Principles 2(b), 3(b), and 7(d).

[47] Evidenced by the language used in the FTC's mission statement - "*The FTC's mission is protecting the public from deceptive or unfair business practices…*" and the recent Flo Health complaint highlights the numerous violations identified and broad enforcement action taken by the FTC on behalf of consumer privacy and protection. (https://www.ftc.gov/system/files/documents/cases/flo_health_complaint.pdf).

[48] DPF Principle 2(c).

[49] Article 9(1) of the UK GDPR.

Thus, if UK organisations who are sending information to certified US organisations have highlighted specific personal data as being sensitive[50], this will require certified US organisations to treat it as such, as it will be covered by the '*sensitive data*' requirements of the DPF. This requirement provides a mitigation against the differing definitions of sensitive information and special category data under the DPF and UK GDPR, respectively. Additionally, under the UK GDPR[51] contracts with processors are required to stipulate the "*nature and purpose of the processing*" and the "*type of personal data and categories of data subjects*". This provides further basis for controllers highlighting where data in the UK is considered to be '*sensitive*' and therefore where US processors under the DPF would be required to meet the requirements of the Choice (2)(c) Principle.

Where onward transfers from certified US organisations to other processors and controllers are concerned the requirements under Supplemental Principle 10 apply, requiring contracts between controllers and processors to provide for the same level of protection as provided under the DPF. Furthermore, under Supplemental Principle 10(a)(ii)(3), the DPF specifies that contracts put in place between controllers and processors are for the purposes of ensuring the processor takes into account the nature of the processing - which would include whether the data is sensitive. Though risks may not be fully mitigated in fringe scenarios, DSIT will need to continue to monitor how such transfers take place and where risks to data subjects become apparent.

DSIT is aware that the Choice Principle does not include genetic and biometric data in the list provided of sensitive information. Notwithstanding the additional protections provided for under Choice 2(c) Principle relating to the specific highlighting of data which is considered sensitive by UK controllers, genetic and biometric data categories are an increasing focus of US privacy laws.[52] The US state privacy laws, such as the California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act, increasingly provide a definition of '*sensitive data*' which includes genetic and biometric data.[53] Additionally, some states have implemented biometric privacy laws[54] which regulate the collection and use of certain "*biometric identifiers*" and use of that information by privacy entities. In a recently-passed law in Washington state, the My Health My Data Act also provides increasing protections for consumers' health data which applies to health information that is not covered under other federal privacy laws, such as the Health Insurance Portability and Accountability Act (HIPAA).[55]

---

[50] Such as that which has been collected in accordance with Article 9 of the UK GDPR.

[51] Article 28(3) of the UK GDPR.

[52] Though the specific protections each of the above laws provide will vary depending on where US organisations are based and therefore the additional protections provided may be limited.

[53] The definition of "*sensitive data*" varies between states but generally includes data revealing racial or ethnic origin, religious beliefs, physical or mental health diagnosis, sexual orientation, citizenship or immigrant status, as well as genetic or biometric data processed for identification, precise geolocation, and personal data collected from a known child. The CCPA also includes data revealing Social Security, driver's licence, state identification card or passport numbers; account log-in, financial account, debit card or credit card numbers in combination with any required security or access code, password or credentials allowing access to an account; union membership; philosophical beliefs; contents of a consumer's mail, email, and text messages (unless the business is the intended recipient).

[54] Such as Illinois's Biometric Information Privacy Act (BIPA) and similar laws in Texas and Washington.

[55] HIPAA only covers certain specified entities, such as healthcare providers and health insurers, and their business associates/processors.

For sensitive information, certified US organisations must obtain affirmative express consent (opt in) from the data subject if the information will be (a) disclosed to a third party or (b) used for a purpose other than those for which it was originally collected for or authorised by the individual. As such, because of the need for affirmative authorisation for the disclosure and/or re-purposing of sensitive information, UK data subjects are able to retain greater control over their personal data. Additionally, while the Choice Principle does not start from a position of prohibiting processing of sensitive data (in the same way as Article 9 starts from a position of prohibiting processing of special category data under the UK GDPR, subject to various exceptions), the '*affirmative express consent*' is broadly similar to the explicit consent requirement under the UK GDPR as one of the exemptions to the processing of special category data. DSIT considers this requirement to be comparable to that under the UK GDPR, given the additional Notice (1.) and Data Integrity and Purpose Limitation (5.) DPF Principles, requirements and other considerations are discussed in the 'Principles underpinning the data protection regime' section below.

However, there are specific exemptions provided for under the DPF (Supplemental Principle 1.) that allow for the transfer of sensitive data without '*opt-in*' consent, though data is still required to be afforded protection provided by the rest of the DPF Principles. The exemptions are: (a) vital interests; (b) if it is necessary for the establishment of a legal claim or defence; (c) required for the provision of medical care/diagnosis; (d) use in the course of legitimate activities by a foundation or non-profit body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; (e) necessary for obligations under employment law; and (f) when related to data manifestly made public by the individual.

DSIT considers that these exemptions are comparable to exemptions provided for under Article 9(2) of the UK GDPR and do not pose a material risk to UK data subjects.Thus, DSIT considers that the DPF provides comparable protections and control over sensitive personal data for UK data subjects as would be received within the UK.

Human Resources (HR) Data

HR data transferred under the DPF is subject to the requirements set out within Supplemental Principle 9[56] and defined as personal information collected about employees (past or present) by an organisation in the context of the employment relationship. Where it is being transferred to the US under the UK Extension HR data will have initially been collected and processed subject to the UK's domestic laws and such laws and requirements must also be followed prior to a transfer taking place. Once transferred the personal data must be maintained according to the DPF Principles. However, for a certified US organisation to receive HR data under the DPF, they must notify the DoC when self-certifying[57] of their intention to transfer such data, and, to ensure that UK laws and requirements concerning the handling and use of HR data are maintained, certified US organisations must agree to comply with UK regulators where enforcement or redress is necessary.[58] This ensures that, where there are overlapping

[56] DPF Supplemental Principle 9.
[57] This is included as a separate filter and label on the DPF List.
[58] DPF Supplemental Principle 9(d).

requirements within the UK under data protection and employment laws, the data is treated in line with UK legal and regulatory requirements. DSIT concludes that this provides appropriate protections for the transfer of this specific type of data under the DPF.

There is an exemption under the Supplemental Principle on Human Resources data (e)(i), concerning the use of some data for occasional employment-related needs for transfers of data for short-term purposes including booking flights, hotel rooms, or insurance coverage. This exemption allows employers to conduct transfers for small numbers of employees to controllers outside of the usual restrictions of the Accountability for Onward Transfer Principle and without the application of the Access Principle. DSIT considers that the use of such an exemption for employment-related purposes on a small scale does not pose a considerable risk to UK data subjects, especially taking into account that certified US organisations are still required to comply with the Notice and Choice Principles. The application of these Principles still requires certified US organisations to have notified UK data subjects about the use and disclosure of their data (even occasional) for such purposes to third-parties and provide them with an opt-out/in as necessary under the Choice Principle where they may be utilising personal data for purposes incompatible with those for which the personal data was originally collected.

Personal data that relates to offenders or suspected offenders in the context of criminal activity, allegations, investigations and proceedings is provided additional protections under the UK GDPR. As well as complying with the general requirements under the UK GDPR, controllers can only process criminal offence data if they are doing so under the control of official authority or if authorised by another domestic law (meeting one of the conditions in Schedule 1 of the DPA 2018). In the majority of cases such data would be shared as part of HR data held by UK organisations and be protected as above in line with the requirements under Supplemental Principle 9. However, where there is the potential for HR data (such as criminal offence data) to be processed outside of a HR relationship,[59] protections afforded to this type of data could be encompassed under the Choice Principle if the transferring party identifies the data as '*sensitive*', therefore requiring the receiving party to treat it as '*sensitive*' under the DPF Principles.[60]

Supporting the protections under the DPF, within the US where criminal history information may be used for background check purposes (such as for employment or housing), the Fair Credit Reporting Act ("FCRA") and similar state laws may, where applicable, provide protections to information collected by consumer reporting agencies that include companies who assist in criminal background checks.[61] There are specific procedures required under the FCRA, including obtaining permission from individuals, notifying individuals how the report will be used, limiting any misuse, providing copies of any reports (if employers decide not to hire them) and allowing individuals to dispute information contained within the reports.

Therefore, DSIT does not think that the extra protections afforded to criminal offence data under the UK GDPR are likely to be undermined and such data will likely benefit from comparable

[59] For example, credit reports or background checks outside of the employer-employee relationship.

[60] In contrast, in the US, Criminal Offence data is generally considered to be public record (apart from juvenile cases and where records have been expunged), and would therefore not be subject to the Notice, Choice and Accountability for Onward Transfer Principles (unless combined with non-public record information). Transferring organisations can indicate that these principles should be applied as under supplemental principle 15(b).

[61] Noting the limitations of differing state jurisdictions that will not provide uniform protection to data from the UK.

protections under the DPF. However, DSIT will continue to monitor the sharing and use of this type of data and address challenges where there may be issues arising.

Principles underpinning the data protection regime

The DPF is based on a system of self-certification by which US organisations, eligible to join the DPF, publicly commit to the DPF Principles.[62] The DPF Principles are:

Notice principle[63]

Certified US organisations are required to provide certain information to data subjects in relation to the processing of their personal data. This includes the type of data collected, the purpose of processing, their right of access and choice (as discussed below), conditions for onward transfers and liability. Further, certified US organisations are required to make their privacy policies a public-facing document[64] and to provide links to the DoC's website (which includes information on self-certification, data subject rights and available redress mechanisms) and the DPF List, as well as information related to the independent dispute resolution body.

Data integrity and purpose limitation principle[65]

Certified US organisations are required to ensure that the processing of personal data is limited to information relevant for the purpose of the processing, reliable for its intended use, accurate, complete and current. Certified US organisations are prohibited from processing personal data in a way that is incompatible with the purpose for which it was originally collected or subsequently authorised by the relevant data subject. Further, certified US organisations are permitted to only retain any personal data in a form which can identify an individual for only as long as it serves the original purpose it was collected for.

Choice principle[66]

Where changed purposes are materially different but still compatible with the original purpose, the Choice Principle gives data subjects the right to object or opt out. This does not supersede the express prohibition on incompatible processing, under the Data Integrity and Purpose Limitation Principle. There are also additional rules which allow data subjects to opt out from the use of personal data for direct marketing at any time. For sensitive data, certified US organisations are generally required to obtain the data subject's express consent.[67]

[62] These principles are expanded upon and clarified through various supplemental principles which organisations are also required to implement and agree to.
[63] DPF Principle 1.
[64] DPF Supplemental Principle 6.
[65] DPF Principle 5.
[66] DPF Principle 2.
[67] DPF Supplemental Principle 1.

Security principle[68]

Certified US organisations creating, maintaining, using or disseminating personal data must take "*reasonable and appropriate*" security measures, taking into account the risks involved in the processing and the nature of the data. For sub-processing, certified US organisations must enter into a contract with the sub-processor guaranteeing the recipient shall provide the same level of protection as the Principles.[69]

Access principle[70]

Data subjects have the right to obtain confirmation on whether a certified US organisation is processing personal data related to them and have the data communicated to them within a reasonable time and subject to a nominal fee. Data subjects also have the right to correct, amend or delete their personal data where it is inaccurate or has been processed in breach of the DPF Principles. Additionally, the Supplemental Principle on Access confirms that certified US organisations "*should answer requests from an individual concerning the purposes of the processing, the categories of personal data concerned, and the recipients[71] or categories of recipients to whom the personal data is disclosed*", as well as have data communicated to individuals that allows them to verify the accuracy and confirm the lawfulness of the processing as part of access requests.[72] This additional information helps to provide individuals with greater knowledge and control over the use and disclosure of their personal data by organisations once it has been transferred outside of the UK.

Recourse, enforcement and liability principle[73]

Certified US organisations must implement robust mechanisms to assure compliance with the other DPF Principles, redress for data subjects whose personal data has been processed in a non-compliant manner, and consequences for the certified US organisation when the DPF Principles are not followed. Certified US organisations are required to have a readily available independent recourse mechanism by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual. Certified US organisations must also have follow-up procedures for verifying that the attestations and assertions they make about their privacy practices are true and that privacy practices have been implemented as presented. Mechanisms established or relied upon by organisations must also include an obligation to remedy problems arising out of failure to comply with the DPF Principles.

[68] DPF Principle 4.
[69] DPF Principle 3.
[70] DPF Principle 6.
[71] Recent judgments in the EU have highlighted their interpretation of the Right of Access under the EU GDPR as including the right to know who has been in receipt of personal data held and disclosed by an organisation.
[72] DPF Supplemental Principle 8(a)(i).
[73] DPF Principle 7.

Accountability for onward transfer principle[74]

To transfer personal information to a third party acting as a controller, certified US organisations must comply with the Notice and Choice Principles. Certified US organisations must also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the DPF Principles. To transfer personal data to a third party acting as an agent, certified US organisations must take a number of steps designed to protect the data, including transferring the data only for limited and specified purposes and taking reasonable and appropriate steps to ensure the agent effectively processes the personal data in a manner consistent with the certified US organisation's obligations under the DPF Principles.

Exemptions

Within the DPF Principles, there are various exemptions that certified US organisations can rely on if needed:

Choice

There are limited exemptions under the Choice Principle. The only pertinent exemption which may have an impact on protections for UK data subjects is that the requirements of the Choice Principle[75] do not apply when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the certified US organisation. In such situations, certified US organisations are required to adhere to the Accountability for Onward Transfer Principle and supplemental information in the Obligatory Contracts for Onward Transfers.

Data integrity and purpose limitation

Certified US organisations can continue to process personal data for longer periods if the time and the extent of such processing fulfils one of the following specific purposes: archiving in the public interest, journalism, literature and art, scientific and historical research and statistical analysis.[76] Importantly, according to Principle 5(b) "*such processing shall be subject to the other Principles and provisions of the [DPF]*," therefore ensuring that where such processing is continued for the aforementioned specific purposes it is still subject to the Choice and Notice Principles relating to opt-out, and the other DPF Principles relating to ensuring continued security and access rights for individuals.

Limitations on adherence to principles

Adherence to the DPF Principles may be limited (a) to the extent necessary to comply with a court order or meet national security, public interest or law enforcement requirements including where a statute or government regulation create conflicting obligations; (b) by statute,

[74] DPF Principle 3.
[75] DPF Principle 2(b) - To provide an opt-out.
[76] DPF Principle 5(b).

government regulation or court order that creates explicit authorisations; or (c) if the effect of the UK law is to allow exceptions or derogations.[77]

Access principle

The Access Principle does not apply to public record information[78] as long as it is not combined with other personal information (apart from limited information used to index or organise the public record information). The Access Principle is also limited where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of third-party individuals would be violated.[79] The Supplemental Principle on Access (8.) provides further information relating to the obligations on certified US organisations to balance restricting the right of access and paragraph 8(b) provides that this exemption can only be relied upon in "*exceptional circumstances*" and provides examples as to what would not be considered disproportionate in relation to the burden or expense of providing access. This section (8.(a)(iii) and (e)(i) and (ii)) also requires that where certified US organisations are restricting access and claiming an exemption they have "*the burden of demonstrating its necessity, and the reasons for restricting access and a contact point for further inquiries should be given to individuals.*" This provides UK data subjects with a route and information with which to raise issues with the certified US organisation in question and if still unsatisfied UK data subjects may utilise other redress mechanisms under the DPF to attempt to remedy any complaints.

Further mitigations

The DPF Principles broadly align to those under Article 5 of the UK GDPR with the exception of the Lawfulness Principle and Accountability Principle under the UK GDPR, where there are further mitigations and analysis to consider.

The Lawfulness Principle, as it relates to the establishment of a lawful basis under Article 6 or 9 of the UK GDPR is discussed below (in section '*Legal bases for processing*'). The overarching Lawfulness Principle under the UK GDPR relates primarily to the requirement that personal data is "*processed lawfully, fairly and in a transparent manner in relation to the data subject*".[80] DSIT is satisfied that the totality of the requirements under the DPF and the DPF Principles mean that certified US organisations who are processing personal data in compliance with the DPF will be processing data in a lawful, fair and transparent manner. UK data subjects can further confirm this through their Access rights. Under the Supplemental Principle on Access, 8(a)(i)(2), the Access Principle under the DPF allows for people to *"have communicated to them such data so that they could verify its accuracy and the lawfulness of the processing*". This is an important route for UK data subjects to verify the processing of their personal data is in compliance with the DPF Principles. Furthermore, UK data subjects can utilise the various redress mechanisms where they believe certified US organisations are in breach of the DPF Principles and any breach

[77] DPF Overview(5).
[78] Personal data collected from public records is defined under DPF Supplemental Principle 15(a) as "*records kept by government agencies or entities at any level that are open to consultation by the public in general*".
[79] DPF Supplemental Principles 8 and 15.
[80] Article 5(1)(a) of the UK GDPR.

of these requirement, or of any of the DPF Principles, would leave certified US organisations open to enforcement action by the appropriate supervisory authority through enforcement actions (set out below in the section on enforcement).

The Accountability Principle, though not explicitly covered in any particular section of the DPF, is covered by wider holistic requirements and obligations placed on certified US organisations[81], as well as the accountability and auditing actions of the DoC[82] (see the accountability section for further information on the role of the DoC in providing administration and oversight of the DPF).

Furthermore, certified US organisations are subject to the '*Notice*' Principle which requires that the purpose for the collection and processing of personal data must be communicated to data subjects. DSIT is content that ensuring that individuals understand the use of their personal data by certified US organisations and the fact that certified US organisations are limited in their lawful processing abilities through the Notice and Choice Principles (including providing individuals with opt-out/in requirements in specific contexts), reduces any additional risks to UK data subjects from the DPF not containing a specific '*fairness' or 'lawfulness*' principle.

Conclusion

DSIT considers that the DPF principles broadly align with those of the UK and provide comparable protections for UK data subjects and are mitigated where differences are apparent. There are also holistic and practical observations which contribute to the overall culture of privacy practices by organisations in the US, such as a general adoption of the highest international standards where organisations operate internationally. A good example of this is the US participation in the APEC CBPR System and the Global CBPR Forum, which provide a mechanism for US companies to certify compliance with international standards and facilitate transfer of data. Though not explicit across all organisations who would certify under the DPF, it does provide evidence as to the general privacy culture of larger multinational companies operating in the US.

Legal bases for processing

The DPF does not contain an explicit concept of 'permissible legal bases for processing' as under the UK GDPR under Article 6. However, some protection is provided by a combination of other mechanisms within the DPF.

Personal data will initially have been collected from UK data subjects in the UK in line with a permissible legal basis under the UK GDPR by a UK controller prior to any transfer to a certified US organisation.[83] Certified US organisations are required to comply with the Data Integrity and Purpose Limitation Principle (as set out earlier in this analysis). This ensures that certified US organisations may not process personal data in a way that is incompatible with the specific

[81] DPF Supplemental Principle 7.

[82] Annex C (ITA Letter).

[83] UK individuals would still have a right to withdraw consent from the original UK controller, where consent was the original legal basis, but would not have this right in relation to the DPF, given that the DPF does not require a legal basis such as consent.

purpose for which it was originally collected or subsequently authorised to be processed by the UK data subject, for which there will have been a legal basis established by the UK controller.

If certified US organisations wish to change how they are processing or sharing UK personal data received under the UK Extension for a purpose other than that for which it was collected or had previously been authorised by the data subject then the Choice Principle engages.[84]

Under the Choice Principle, individuals must be provided with the opportunity to opt-out[85] of whether their personal data is (a) disclosed to a third party or (b) if used for a purpose that is materially different to the purpose(s) for which it was originally collected or authorised by the individual. Individuals must be provided with this choice through a clear and readily available mechanism in order to exercise their right to opt out[86], this is in combination with the Notice Principle'[87]. It is our understanding that in practice individuals are informed via email or through the posting of updated privacy policies with instructions on how to exercise their opt-out. Although the DPF utilises an '*opt-out*', rather than '*opt-in*' approach, the requirement to notify individuals and the various redress mechanisms available mitigate the risks associated. Further, in circumstances where personal data is disclosed to a third party, in addition to the data subject having an opt-out under the Choice Principle, the Accountability for Onward Transfer Principle (discussed below in the section '*Focus On International and Onward Transfers*') requires safeguards to be contained in a contract between the transferring entity and the third party.

Though DSIT acknowledges that there may be a limitation in notification, such as where a privacy policy is merely posted online instead of directly shared with individuals, DSIT considers that the limitations on use of personal data for different purposes offers an initial protection to individuals. Additionally, in line with Article 14(5)(b) of the UK GDPR concerning disproportionate effort of notification, DSIT is satisfied that the provision of such a notification from a US organisation to a UK individual may involve disproportionate effort if organisations do not have readily available access to UK data subject contact information. Therefore, DSIT is content that the broader protections in place prior to the engaging of this Principle and the protections that exist for redress where individuals are displeased with how their data has been used present protections to mitigate this concern.

Conclusion

Overall, DSIT judges that the lack of an underlying requirement for a legal basis for processing in the DPF, is to some extent mitigated by the combination of the DPF Principles of Data Integrity and Purpose Limitation, and Choice, which limit how certified US organisations are able to process UK personal data. Where those organisations wish to undertake changes to the purpose

[84] DPF Principle 2.

[85] Or for sensitive personal data, the opportunity to "*opt-in*". See section above. on '*Sensitive Data*'.

[86] DPF Principle 2(a).

[87] The Notice Principle requires organisations provide individuals with a clear statement of information concerning, amongst other things, the reasons for their data being collected and processed, whether and to whom their personal data may be disclosed, their rights over their personal data, and the available recourse and redress mechanisms.

for which the personal data is being processed they are required to provide UK data subjects with a means to exercise control over their personal data through the Choice principle.

Exemptions

The DPF contains a general exemption[88] where certified US organisations may be limited in their following of the DPF Principles to "*the extent necessary to comply with a court order or meet public interest, law enforcement, or national security requirements, including where statute or government regulation creates conflicting obligations*",[89] which potentially limits the protections for personal data, should certified US organisations be required to comply with these obligations outside of the provisions of the DPF.[90] This is not considered to be a disproportionate provision for the reasons set out below. In the UK, exemptions from compliance with certain provisions of the UK GDPR can be applied for purposes including national security and the prevention of crime, amongst others.[91] While the exact limits of public interest exemptions are not detailed within the DPF, there are references within the Access Principle regarding the limits placed on such access related to the "*safeguarding of important countervailing public interests, such as national security; defense; or public security*".[92] Exemptions for various public interest purposes are commonplace in data protection legislation and the details of many are included within the UK DPA 2018.[93]

The DPF also accounts for areas where there may be conflicting government regulations or case law that creates explicit obligations that conflict with the DPF Principles[94]. This could include, for example, the US local laws to require the disclosure of personal data during audits or the requirement to meet more stringent data processing requirements under sector-specific laws. Where such conflicts arise, certified US organisations are required under the DPF to demonstrate that their non-compliance with the DPF is limited to the extent necessary to meet the legitimate interests of the laws involved.[95] Additionally, where organisational conflicts arise that are applicable in a data protection context, certified US organisations are expected to opt for the higher protections where possible, such as in relation to state data breach notification requirements[96] or where there is conflict with federal or state laws. Where certified US organisations are applying these exemptions, they should be able to justify their actions given the ability of the DoC, regulator (FTC or DoT) or independent redress mechanisms to request any and all records demonstrating a certified US organisation's implementation of their privacy policies.[97] Additionally, certified US organisations are required, under the Notice Principle, to

[88] DPF Overview(5).

[89] Though the concept of "*necessity*" is not a common one in US laws. This was recently raised again under EO 14086, demonstrating an increased use of such terms within the US system.

[90] In the US, access to personal data by public authorities for national security and law enforcement purposes is dealt with under separate legislation which form part of this assessment (see the government access to data sections below for further information).

[91] Section 26 of the DPA 2018 and Schedules 2-4 of the DPA 2018.

[92] DPF Supplemental Principle 8(e)(i).

[93] Schedules 2-4 of the DPA 2018.

[94] DPF Overview(5).

[95] DPF Overview(5).

[96] These are often managed at a State level through various State Data Breach Notification laws

[97] DPF Supplemental Principle 7(e).

provide information where there may be such exemptions relied upon, ensuring UK data subjects are informed as to the potential sharing of personal data outside of the DPF. DSIT considers this exemption to be proportionate to the local legislative context, and the added requirements in the DPF to maintain records for audit purposes strengthens the oversight and accountability of the use of such exemptions.

Additionally, where such personal data has been processed in accordance with exemptions to the DPF Principles, it would only be in accordance with other legal frameworks in the US, potentially including oversight and safeguards included in such laws as are being relied upon to make use of the exemption. However it should be highlighted that not all laws being relied upon may provide data protection requirements, but DSIT considers that where such an exemption is being utilised, the requirements on certified US organisations to continue to uphold their commitments under the DPF reduces the risks to data subjects. However, the DPF does state that certified US organisations are expected to opt for the higher level of protection where the option to do so is permitted under the DPF Principles and/or US law. In addition, multinational organisations who have a presence in both the US and UK are more likely to opt for higher protections across their organisation and have consistent compliance frameworks. This is beneficial to bring in other Principles and rights which may not be demonstrable under the DPF and help to mitigate risk for UK data subjects whose personal data has been collected and processed.[98]

Under the Verification Supplemental Principle, certified US organisations are required to maintain and provide follow-up procedures for verifying the assertions made about their privacy practices under the DPF, and must maintain records of such implementation of their privacy practices.[99] This provides a measure of accountability and oversight that also provides potential routes for enforcement against certified US organisations that misuse exemptions and notification policies (either via the DoC taking action directly, or via a regulator). This requirement for certified US organisations to maintain and demonstrate compliance (if necessary), is also aligned with the Accountability Principle under the UK GDPR (see section on '*Principles underpinning the data protection regime*' above).

Information that is available publicly and as part of public record[100] may be collected by certified US organisations under the DPF but they are exempt from the requirements to apply the Notice, Choice, Access[101] or Accountability for Onward Transfer Principles. However, they are still required to maintain the Principles of Security, Data Integrity and Purpose Limitation, and Recourse, Enforcement and Liability. In the UK, information collected from open sources should be clearly set out within privacy notices in line with the right to be informed. However, under the DPF this is not the case as this type of information is exempt from the Notice Principle. That said, the Data Integrity and Purpose Limitation still applies however, and therefore limits the use of any personal data for purposes incompatible with which it was originally collected. Additionally,

[98] Though we should point out the limitations of relying on such non-DPF federal, state or sectoral laws in this assessment. They are welcome additions but the exact nature of each law cannot be reasonably investigated and set out within this analysis, and therefore may provide only limited benefit and protections in some situations.

[99] DPF Supplemental Principle 7(a) and (e).

[100] DPF Supplemental Principle 15.

[101] Though if combined with other personal data then it may become eligible for the Access Principle again.

the purposes and notification of which would have been provided at the original point of collection by a UK organisation in full compliance with the UK GDPR and UK data protection framework. DSIT does not therefore believe that this exemption for publicly available information demonstrates a material risk for the transfer of personal data from the UK under the UK Extension.

Security

Under the Security Principle,[102] certified US organisations creating, maintaining, using or disseminating personal data are required to implement *"reasonable and appropriate*" security measures to protect it from loss, misuse and unauthorised access, disclosure, alteration and destruction, taking into account the risks involved in the processing and the nature of the data. Where certified US organisations appoint third-parties to process personal data on their behalf (sub-processors), the certified US organisations must enter into a contract with a sub-processor which requires the same level of protection as provided by the DPF principles and ensures steps are taken to ensure its proper implementation. While the application of the Security Principle is not specifically expressed to apply to '*processing*' but rather to "*creating, maintaining, using or disseminating personal information*", DSIT does not consider that there is a material different in practice given that the matters listed arguably cover all forms of processing, and the Security Principle references the more comprehensive definition of '*processing*' as part of setting out how the Security Principle should be applied.[103]

With regard to publicly available information, certified US organisations must apply the Security Principle to personal data from publicly available sources including personal data collected from public records, i.e., records kept by government agencies or entities at any level that are open to consultation by the public.

The Security Principle broadly reflects the wording of the UK GDPR's '*Security Principle*' as set out in Article 5(1)(f) and Article 32 of the UK GDPR, ensuring the level of protection offered is broadly aligned. Additionally, there are no specific exemptions relating to the Security Principle, and exemptions are only allowable in places where certified US organisations would be exempted from all DPF Principles (i.e., to meet national security, public interest or law enforcement requirements).

The UK GDPR's security requirements go beyond the wording highlighted within the Security Principle of the DPF. Article 32(1) UK GDPR requires organisations to take into account certain specific factors - such as the state of the art, the costs of implementation and the nature of processing as well as the varying likelihood and severity for the rights and freedoms of data subjects – when determining what constitutes appropriate security measures. No such factors are explicitly prescribed under the Security Principle, however the Principle does reference the "*risks involved in the processing*" as requiring consideration. This may provide an additional measure of protection for certain data which may need to be protected to a higher standard or which is classed as sensitive. Furthermore, the UK GDPR separates security measures into two

[102] DPF Principle 4.

[103] DPF Principle 4(a) - "*taking into due account the risks involved in the **processing** and nature of the personal data".* [Emphasis added]

categories (i) technical measures and (ii) organisational measures, a level of detail which is not captured within the DPF. However, one such area that may benefit from increased protections in the security and management of personal data is the use of data concerning children. In the US, there is federal law that may place additional requirements on organisations (regardless of their certification to the DPF) under the Children's Online Privacy Protection Act (COPPA), which is also regulated by the FTC. This law applies to any collection of personal information concerning children under 13 years of age (including children outside of the US) and details of what must be included in privacy policies, when and how to seek consent and the responsibilities that must be placed on organisations to protect children's privacy and safety online. This is a strong example of federal law in the US which supplements and places further protection on personal data within the US outside of the remit of the DPF and helps to ensure personal data is safeguarded when transferred from the UK.

There are, however, no explicit requirements within the DPF relating to data breach notification. However, there are many factors across the US legislative space that may serve to mitigate this gap (and potentially provide mitigations and protections complementary to the DPF).Importantly though this is dependent on whether the particular organisation is subject to the relevant legislation, rather than explicit requirements under the DPF. For instance, many: (i) sector-specific, federal privacy laws; and (ii) '*general application*' state data security or privacy laws, contain requirements that either (a) mandate the reporting of data security breaches and create potential liability for such breaches (thereby creating an incentive to implement robust security measures); and in some cases (b) expressly require the implementation of appropriate/minimum security measures. For example:

- All 50 US states, Washington DC, and most US territories (including, Puerto Rico, Guam and the Virgin Islands) have passed data breach notification laws that require notifying state residents, and in some cases a regulator such as the state Attorney General ("AG"), of a security breach involving more sensitive categories of information as defined by each jurisdiction, such as Social Security numbers and other government identifiers, credit card and financial account numbers, health or medical information, insurance ID, tax ID, birthdate, as well as online account credentials, digital signatures and/or biometrics.
- The CCPA provides a private right of action to individuals for certain breaches of unencrypted personal information, which increases class action risks posed by data breaches.
- The New York "*SHIELD Act"* sets forth minimum security obligations for safeguarding private information.
- The New York Department of Financial Services (NYDFS) regulations impose extensive cybersecurity and data security requirements on licensees of the NYDFS, which includes financial services and insurance companies, and the Federal Gramm-Leach-Bliley Act and implementing regulations require financial institutions to implement reasonable security measures.[104]
- The HIPAA Security Rule requires covered entities (e.g. healthcare providers, health plans) and their service providers to protect patients' electronically stored, protected

[104] Financial services companies are not FTC regulated and therefore are not eligible to be certified organisations under Privacy Shield. However, they may act as onward recipients of data transferred under the DPF.

> health information (known as "ePHI") by using appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of this information.[105]

Outside of '*hard law*' requirements, there are also a number of '*best practice*' technical standards for data security (the most common of which are ISO 27001 and National Institute of Standards and Technology (NIST) Cybersecurity Framework)[106] which many US organisations will adhere to or be certified under (though there are no explicit requirements to do so under the DPF). US organisations may comply with these standards for a number of reasons, including: (i) as a '*quality hallmark*' to help differentiate their service offering to customers;[107] (ii) to mitigate the risks of a cybersecurity attack, thereby reducing their exposure to operational disruption and financial losses; and (iii) to demonstrate robust governance of information security to the market or to private investors. The FTC also has published a Data Breach Response guide for businesses[108] which outlines the steps businesses should take and consider when they learn there has been a data breach. This includes a multitude of information and suggestions, including suggesting the notification of other businesses of the breach if the organisation holds or collects personal data on behalf of other businesses.

Broadly speaking, and based on the information above, DSIT does not consider the gap between the UK GDPR and the Security Principle to be significant. For instance, the factors listed in Article 32 are broad considerations that a controller or processor is only required to "*take into account*", and they therefore do not translate into specific security controls that organisations are mandated to implement as part of their security programme.

Conclusion

Therefore DSIT considers that, though there are differences in the detail and language between the two Principles of the UK GDPR and the DPF, DSIT this does not undermine the protections afforded to UK personal data and there are mitigations available that enable comparable protections. DSIT will continue to monitor potential impacts of any gaps on UK data subjects.

Accountability

Under the UK GDPR[109] organisations are required to be able to demonstrate compliance with the Principles set out within Article 5(1). Under the DPF, no such explicit Principle to enforce accountability or compliance exists, but the structure of the DPF itself and other requirements of the DPF requires companies to demonstrate accountability[110].

---

[105] As with financial services, most healthcare providers will not be FTC regulated, although may be onward recipients. Service providers to healthcare providers ('*business associates*') may be FTC regulated (for example, a technology company that hosts healthcare data on behalf of a healthcare provider).

[106] The NIST compliance framework was created to provide a uniform set of cybersecurity rules, guidelines, and standards across industries (https://www.nist.gov/cyberframework).

[107] This is particularly relevant for the many technology service providers that are certified US organisations under the DPF.

[108] https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business.

[109] Article 5(2) of the UK GDPR.

[110] DPF Supplemental Principles 6 and 7.

The DPF is a '*self-certification*' system which places the onus on certified US organisations to verify that they are complying with the requirements of the DPF when completing their certification and annual renewals. The Verification Supplemental Principle (7) sets out how certified US organisations can make attestations regarding their compliance with the DPF, through the '*self-assessment*' approach or '*outside compliance review*'[111]. Both approaches require certified US organisations to produce attestations signed by a corporate officer or designate (or outside reviewer), which must be renewed annually. Under this Supplemental Principle (7(e)), certified US organisations are required to maintain records of their implementation of the DPF Principles and privacy policies, which they must make available when necessary, as a result of investigations or complaints, or to the DoC in response to inquiries or requests for information.

A failure of certified US organisations to be able to effectively respond to requests from regulators and consumers regarding their privacy practices, responses to complaints or when consumers attempt to utilise their data rights, would open them up to enforcement and redress action. This is a key oversight element that certified US organisations would need to be able to withstand if they wished to continue collecting and utilising personal data transferred under any adequacy regulations for the DPF.

Role of the Department of Commerce

The DPF is administered by the DoC. In order to ensure that organisations meet the requirements to join the DPF, the DoC has committed[112] to verify and provide accountability for multiple aspects of certifications, including ensuring that organisations have published the correct information in their public-facing privacy policy before certifications are finalised and organisations are added to the DPF List on the website.[113]

The DPF Principles apply only to US organisations who have self-certified to the DoC that they meet the requirements set out. In order to self-certify to the DPF, an organisation must certify that they are subject to the investigatory and enforcement powers of either the FTC or the DoT,[114,115] certify that they comply with the DPF Principles, make a public commitment through a privacy notice (which includes a specific commitment to protect personal data received from the UK under the DPF), and have paid the annual certification fee. Once the DoC has determined

[111] The DPF, under the DPF Supplemental principle (7(d)) states that "*The methods of review may include, without limitation, auditing, random reviews, use of "decoys", or use of technology tools as appropriate. A statement verifying that an outside compliance review has been successfully completed must be signed either by the reviewer or by the corporate officer or other authorized representative of the organization at least once a year and made available upon request by individuals or in the context of an investigation or a complaint about compliance*."

[112] Annex C (ITA Letter).

[113] This also includes when organisations are undertaking their annual recertifications.

[114] Or other statutory enforcement body. However, at this time no other such enforcement bodies have been recognised under the DPF. The Framework notes "*other US statutory bodies recognized by the EU may be included as an annex in the future*" (DPF Overview (2)).

[115] This generally covers most US organisations, but generally excludes most depository institutions (banks, federal credit unions, and savings & loan institutions), telecommunications and interstate transportation common carrier activities, labour associations, most non-profit organisations, and most packer and stockyard activities. The scope of the FTC's regulatory remit is set out under the FTC Act 15 U.S.C. §45 (a)(2).

that the self-certification is accurate and complete for the receipt of UK personal data,[116] they place the organisation on the publicly available DPF List on the DPF website and indicate on the DPF List that they are participating in the UK Extension to acknowledge that organisations have made UK-specific changes to their self-certification[117]. Once businesses are placed upon the DPF List, they are considered to be "*active*" participants to the DPF and required to comply with the DPF principles.

Certified US organisations can also be removed from the list: between 2016 and 2020, the DoC moved approximately 732[118] organisations from the "*active*" to "*inactive*" list due to organisations withdrawing from the previous Privacy Shield framework or allowing their annual certification to lapse, which DSIT is satisfied evidences oversight from the DoC. If an organisation is removed from the '*active*' DPF List, they are unable to continue to receive personal data through any UK adequacy regulations for the DPF. However, once removed, if they choose to keep the data received under the DPF, whilst they were '*active*', they are still required to treat data acquired under the DPF in line with the DPF Principles, or else they are required to delete or return the personal data.[119] The DoC has also committed to annually monitor such '*inactive*' organisations where they have chosen to retain personal data obtained under the DPF, to ensure continued application of the DPF Principles or that adequate protection by other authorised means is being provided.[120]

The DoC also has a role during the self-certification process and overall administration of the DPF to monitor Alternative Dispute Resolution Bodies relied upon by certified US organisations. The DoC has committed to verify that such bodies meet the minimum requirements set out under the DPF[121] and ensure that such bodies are notified regarding material changes to the DoC's administration of the DPF, as well as provide guidance where necessary to support such bodies roles under the DPF.[122]

The DoC has also committed to a robust process of conducting proactive *ex officio* compliance reviews to ensure certified US organisations are complying with the requirements under the DPF, which includes following up on complaints that are not frivolous or vexatious, and monitoring news sites for potential non-compliance, random selection of certified US organisations for compliance reviews.

---

[116] The ITA has committed to this role in the letter issued setting out their administration of the Framework (Annex C).

[117] These changes include, but not limited to, updating their public privacy notices and agreeing to accept the ICO as the designated local independent data protection authority for investigations, if requested (mandatory where UK human resources data is concerned). The Website contains information on how to self-certify including what information is required for the general process (https://www.dataprivacyframework.gov/s/article/How-to-Join-the-Data-Privacy-Framework-DPF-Program-part-1-dpf)].

[118] As of 31st July, 2020.

[119] See DPF Supplemental Principle 6(f) and https://www.dataprivacyframework.gov/s/article/Withdrawal-under-the-Data-Privacy-Framework-DPF-Program-dpf which provides detailed information on the process, including a questionnaire that the DoC requires organisations to complete and an annual affirmation of its protections and/or desire to retain/delete the personal data it holds.

[120] Annex C (ITA Letter).

[121] DPF Supplemental Principle 11(d)(ii).

[122] Annex C (ITA Letter).

The DoC has committed to review and address specific complaints and claims of non-compliance by certified or non-certified organisations (including those received from individuals, national DPAs, independent redress bodies, UK businesses or other interested third parties), including where certified US organisations fail compliance reviews or who are unwilling/unable to take advised corrective action. The DoC has committed[123] to taking appropriate corrective action as necessary, such as removal of certified US organisations from the DPF List on the website, referring organisations to the relevant regulatory authority and/or taking action based on the False Statements Act (18 U.S.C. §1001), where organisations have made misrepresentations to the Department. Furthermore, organisations can be delisted from the list of certified US organisations, which means they can no longer receive data through relevant adequacy regulations that utilise the DPF programme that they have been delisted from. Additionally, the DoC can refer such an organisation to the FTC or DoT, dependent on the organisational jurisdiction, for investigation and potential enforcement.

Under the DPF, organisations are required to self-certify (and annually re-certify) that they meet the necessary requirements of the DPF regarding their protection of personal data. The DoC has committed to and actively engages in '*false claims monitoring*' to identify organisations making false claims of participating in the DPF,[124] including to target organisations who have never participated in or began but did not complete the self-certification process for the DPF. These include *ad hoc* methods, which in the past have included practices such as third-party contracting with a '*web crawling*' service provider to identify such non-compliance.

The DoC has also committed to provide tailored information to relevant audiences in the US and UK on the DPF website. This information is expected to facilitate transparency, ensure individuals are aware of their rights and certified US organisations understand their obligations, and provide further information about the functioning and administration of the DPF. The DoC has also confirmed their role in managing the functioning of the Arbitration mechanism under Annex I of the DPF Principles and in cooperating in periodic discussions with the UK, as appropriate, related to the "*functioning, implementation, supervision, and enforcement*" of the DPF.[125]

Other accountability and requirements

This risk of potential enforcement by the FTC or DoT (aided by their history of effective enforcement action against US organisations who conduct '*deceptive*' trade practices)[126] helps to drive '*good privacy behaviour*' amongst US businesses[127]. The FTC specifically may use a Civil Investigative Demand to investigate possible compliance violations, which is a type of subpoena that seeks documents or other information related to an FTC investigation. US organisations would need to be able to present evidence of their compliance in order to avoid further enforcement action.

[123] Annex C (ITALetter).
[124] Annex C (ITA Letter).
[125] Annex C (ITA Letter).
[126] [See Annex D-1 (FTC Letter) and Annex E (DoT Letter)].
[127] DPF Overview(2) and Annex D-1 (FTC Letter) and/or Annex E (DoT Letter).

The Recourse, Enforcement and Liability Principle also requires that certified US organisations implement robust mechanisms for assuring compliance with the DPF Principles, including procedures for verifying that the attestations and assertions they make are true and that privacy practices have been implemented as presented.

Conclusion

Thus, it is DSIT's position that there are multiple layers of accountability that contribute to an environment that ensures organisations remain compliant with the DPF Principles. Combined with the commitments made by the DoC to take a proactive stance on compliance review, the absence of a specific Accountability Principle within the DPF does not undermine the protections of UK data subjects and is comparable to the requirements of accountability found within the UK GDPR.

Individual rights

Within the UK legislative framework, data subject rights are set out under Articles 15-22 of the UK GDPR, with associated exemptions under Schedule 2-4 of the DPA 2018. Though not explicitly set out separately, under the DPF data subject rights are included throughout the DPF Principles and Supplemental Principles.

Under the DPF data subjects are broadly afforded the same rights as they are offered under the UK GDPR and DPA 2018, with data subjects having the right to **correct**, **amend**, **delete** or **object to the processing** of their personal data where it is inaccurate or has been processed in violation of the DPF Principles.

- The Access Principle of the DPF provides individuals with several rights, including the right of access to data and the right to have data corrected and erased. This is built on further under the Supplemental Principle on Access that requires certified US organisations to provide data subjects who make access requests, with confirmation as to whether an organisation is processing their personal data and should be able to have that data communicated to them within a reasonable time for individuals to verify its accuracy, lawfulness of the processing, type of data being processed and to whom the data has been disclosed.[128] The Principle also requires certified US organisations to respond to requests within a reasonable period of time and, where necessary, such as to mitigate the challenges of requests that are manifestly excessive or repetitive, allows certified US organisations to charge a non-excessive fee[129]. The limits of when certified US organisations can charge a fee or when they can be justified are set out within the Supplemental Principle on Access[130]. Moreover businesses may not refuse an access request on cost grounds, if individuals offer to pay the necessary costs. Where individuals may disagree with the approach or application of these Principles (including

[128] There is no specific requirement on organisations to provide verification or identity check requirements where access requests have been made. However, the Security principle requires organisations to protect against "*misuse and unauthorised access*". Breaching this principle by providing unverified access to data would leave organisations open to enforcement as having violated the DPF.
[129] DPF Supplemental Principle 8(f)
[130] DPF Supplemental Principle 8(f)(i-iii).

"*reasonableness*" and "*nominal fees*") by certified US organisations, they can raise complaints and utilise the redress mechanisms available under the DPF, which DSIT judges to appropriately serve this purpose.[131]

- Though there is no explicit right or route for individuals to exercise deletion of their personal data under the DPF, many US state laws, also include a right for individuals to have their personal data deleted, subject to certain exemptions[132]. Though these exemptions are broader than those under the UK GDPR, they are more comprehensive than under the DPF and may provide a limited mitigation for some circumstances that could arise for UK individuals.
- Where automated processing of personal data to make decisions affecting an individual is used, automated processing is covered under the definition of '*processing*' and this data is provided the same rights as under the other DPF Principles (i.e., Access). Therefore, individuals have the right to be informed of the specific reasons underlying the processing and to dispute incomplete or inaccurate information and are able to seek redress through the usual routes under the DPF. The EU conducted limited exploration of this point during the first Annual Joint Review of the Privacy Shield,[133] finding that automated processing was more relevant for processing by companies that were EU-facing and where data was collected directly from EU individuals, rather than transferred under the Privacy Shield. Furthermore, where data is transferred under the DPF in many cases there may be a controller-processor relationship in place between the UK and certified US organisations; UK organisations are required to set parameters for any processing (including automated decision-making) and be responsible under UK legislation for that processing.[134] Therefore, though the DPF does not specifically address automated processing, in our opinion there is a low chance of a material impact on UK data subjects and, in addition, where issues do arise, there is access to multiple redress mechanisms under the DPF. This is one area in particular, given the increased use of AI and automated approaches to data processing, that will continue to be monitored.
- In the US, there are also limited protections provided under US state consumer privacy laws. The majority of the currently-enacted[135] laws provide individuals rights regarding the opting out of the processing of their personal information for purposes of profiling and where automated processing is being used to make decisions that affect individuals (i.e., credit lending, mortgage offers, employment, insurance, etc).[136] The FTC has also started

[131] The FTC have set out their understanding of '*reasonableness*' in the 1983 Policy Statement on Deception (https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf)

[132] Such as completing the initial transaction for which the personal information was originally collected, complying with certain laws and/or legal obligations, enabling solely internal uses that are reasonably aligned with the expectations of the consumer, exercising free speech and/or ensuring the right of another consumer to exercise that free speech or another right provided for by law.

[133] Paragraph 4.1.5, SWD (2017) 344 final - https://ec.europa.eu/newsroom/document.cfm?doc_id=47799.

[134] This approach and view is supported by findings from the EU Commission's 2018 Second Annual Review of the functioning of the Privacy Shield. This found that there was no evidence that automated decision making was normally being conducted by businesses on personal data transferred under the Privacy Shield framework.

[135] As of 20 May 2023, which include the Fair Credit Reporting Act ("FCRA"), Equal Credit Opportunity Act ("ECOA"), Fair Housing Act, Health Insurance Portability and Accountability Act ("HIPAA") as examples.

[136] The definitions differ slightly across the laws, but "*profiling*" is the term generally used and refers to automated processing performed on personal data to evaluate, analyse, or predict personal aspects related to an identified or

to take a more active role in managing AI and automated processes which suggests the potential of an increasing regulatory and enforcement environment.[137]

- Individuals, under the Choice - Timing of Opt - Out Supplemental Principle (12.), have the right to opt-out at any time of the use of their personal data for any direct marketing purposes, which can be related to the absolute right to object under the UK GDPR. This is in addition to the ability to '*opt-out*' of processing, in situations where personal data would be processed for purposes materially different (but compatible) to which had been originally set out to individuals at the point of personal data being collected under the Notice Principle of the DPF and/or the Notification obligation under Article 13 of the UK GDPR (further information is covered above in sections on '*Principles underpinning the data protection regime*' and '*Legal bases for processing*')
- Though there is no specific "*right to restrict processing*" as it exists under the UK GDPR, similar goals may be achieved by individuals through access and erasure rights under the Access Principle, to obtain control over their personal data. Additionally, where controllers for the personal data are UK based (using US organisations as processors or secondary processors), individuals can exercise their rights under the UK GDPR directly with UK organisations, whose responsibility it is to ensure that individuals data rights are adhered to by joint controllers and processors, in compliance with (most notably) Articles 24, 26 and 28 of the UK GDPR. Individuals can also exercise specific opt-out and opt-in control through the Choice Principle, especially where sensitive personal data is concerned (within the circumstances set out in the above section on '*Sensitive Data*').

There are also a number of exemptions, beyond those general exemptions to the DPF Principles, to the rights provided under the Access Principle that can be used in limited circumstances, and need to be necessary and justified, with the certified US organisation bearing the burden of demonstrating that these requirements are fulfilled.[138] These exemptions are broadly consistent with, and in general not more permissive than equivalent exemptions within the UK data protection framework. Additionally, where certified US organisations are claiming to rely on one of the exceptions, they shoulder the burden of being able to demonstrate its necessity and should provide individuals the reasons for restricting access and a contact point or further enquiries.[139]

The Right to Data Portability, is not outlined specifically in the DPF, nor are there specific provisions for it under other DPF Principles. However, the way that the DPF functions, as a self-certification framework for certified US organisations to receive data from UK organisations rather than as controllers or processors who have the direct relationship with individuals, reduces the importance of this right being included. DSIT considers it more likely that UK data subjects would want to change from one service provider within a UK domestic context. Further, UK data subjects are likely to be requesting data portability from UK based controllers who provide the service for UK data subjects, and not from US based processors who have had such data shared with them. Where UK data subjects rights to data portability are impacted concerning personal

identifiable individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.

[137] The FTC has recently issued various blog posts warning businesses to avoid unfair or deceptive practices, including "*Keep your AI claims in check*" and "*Chatbots, deep fakes, and voice clones: AI deception for sale*."

[138] DPF Supplemental Principle 8(e)(ii).

[139] DPF Supplemental Principle 8(e)(ii).

data that has been transferred to the US under the DPF, the provision of rights to access, erase and rectification provide sufficient ability for individuals to exercise such control over their personal data as they may wish to under Data Portability, including utilising the Choice Principle and redress mechanisms to opt-out or request specific action be taken with respect to their personal data. DSIT does not believe this represents a barrier or significant reduction in protection for UK data subjects, especially with reference to UK controllers maintaining overall responsibility and control over personal data that is being processed by certified US organisations.

Conclusion

It is our opinion that the areas where there is no direct alignment and areas where protections may be impacted are not significant, and compensated as set out above. Additionally, privacy rights are increasingly prevalent under state privacy laws and all currently-enacted state privacy laws[140] contain some form of consumer privacy rights, with the most common being a right of access.[141]

Therefore, DSIT considers that there are adequate protections with regards to the available rights for UK data subjects under the DPF.

Redress

Certified US organisations have to agree to the Recourse, Enforcement and Liability Principle (7.) of the DPF which sets out the requirement to "*include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed*". Minimum requirements under this Principle include:

- readily available independent redress mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the DPF Principles, and damages awarded where the applicable law or private-sector initiatives so provide;
- follow-up procedures for verifying that the attestations and assertions that certified US organisations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and
- obligations to remedy problems arising out of failure to comply with the DPF Principles by organisations announcing their adherence to them and consequences for such organisations. Sanctions must be sufficiently rigorous to ensure compliance by organisations.

There are numerous routes available to data subjects for redress against certified US organisations who have breached their obligations under the DPF or failed to satisfactorily

[140] As of 25th May 2022.

[141] The more closely aligned with and inspired by the EU GDPR (i.e., the California Consumer Privacy Act and California Privacy Rights Act or the (in draft) Massachusetts Information Privacy Act), the more likely they are to contain equivalent rights.

respond to a request or complaint.[142] A failure to comply with the redress requirements is itself a breach of the DPF Principles, which could result in FTC or DoT investigations and/or removal from the DPF List by the DoC. However, it should be noted that to date no certified US organisation has ever been removed for a persistent failure to comply with the commitments of the DPF. The routes available to UK data subjects are:

Complaints

Certified US organisations are required to take steps to remedy problems arising out of their failure to comply with the DPF Principles. In broad terms, this presents a broad obligation to take whatever steps can be mutually agreed between certified US organisations and complainants. Only when a resolution cannot be agreed would the next logical step be to move to the next redress route. Certified US organisations are required to respond to complaints by individuals within 45 days[143], with information on how they will rectify issues.[144] This is similar to the initial advice that the ICO provides in a UK context.[145]

Independent Dispute Resolution Body

Certified US organisations are required to sign-up to and agree to the directions and decisions of independent dispute resolution bodies.[146] The DPF does not specify the requirements of redress provided by such bodies, allowing for a broad discretion in determining remedies and sanctions. However, remedies under the DPF must ensure that the effects of non-compliance are reversed or corrected, ensure future processing is in conformity with the DPF Principles, and where appropriate, ceasing the processing of personal data of individuals who have brought complaints.[147] In this way, certified US organisations need to ensure that when signing up to use a particular body they meet the requirements of the Recourse, Enforcement and Liability Principle of the DPF.[148] Compliance with the decisions and orders of an independent dispute resolution body is a requirement of the DPF, failure to do so would be considered a violation of the DPF Principles. The DoC has committed[149] to work with independent dispute resolution bodies to verify that they include information on their websites regarding the DPF Principles and the services they provide is accurate.

[142] DPF Principle 7, Supplemental Principle 11 and Annex 1: Arbitral Model.
[143] DPF Supplemental Principle 11(d)(i).
[144] DPF Supplemental Principle 11(c).
[145] https://ico.org.uk/your-data-matters/how-to-make-a-data-protection-complaint/
[146] Three of the most popular service providers for independent dispute resolution bodies based on the most participants are TRUSTe, JAMS and BBB National Programmes. Each of these offer similar but different approaches to fulfilling the requirements under the DPF.
[147] DPF Supplemental Principle 11.
[148] The requirements of what such bodies must provide is set out under DPF Supplemental Principle 11 (d)(i-iii). Failure to utilise a body that meets such requirements would constitute a violation of the Framework Principles.
[149] Annex C (ITA Letter) - Facilitate Cooperation with Alternative Dispute Resolution Bodies That Provide Principles-Related Services.

UK ICO

Under the DPF, certified US organisations may elect to cooperate with the ICO[150] instead of an independent dispute resolution body (where certified US organisations are receiving HR data, they are required to cooperate with the ICO). Such US organisations must certify they will cooperate with the ICO in investigations and resolution of complaints and comply with any advice given by the ICO. Though the precise nature of how investigations and resolution of complaints is not set out, the implication under the Supplemental Principle (5.) '*The Role of the Data Protection Authorities*' requires certified US organisations to cooperate with investigations and decisions of national DPAs, which implies that DPAs are free to determine whatever measures and remedies they deem necessary, in line with their normal investigative procedures. Additionally, UK data subjects may complain to the ICO and "*organisations must respond expeditiously to complaints regarding their compliance with the Principles referred through the Department by DPA*s". A failure of certified US organisations to follow the advice and direction of the DPAs would be considered an act of non-compliance under the DPF.[151]

The ability of the DPAs to provide advice is without prejudice to their role in enforcing the extra-territorial scope of the UK GDPR or when issuing remedies and sanctions under Article 58 of the UK GDPR against data exporting organisations within the UK.

FTC/DoT

Individuals can file complaints with the FTC through the Consumer Sentinel database.[152] Additionally, the FTC and the DoT have both committed to reviewing, on a priority basis, referrals alleging non-compliance with the DPF received from the ICO or DoC.[153] Though the FTC and DoT do not generally act upon individual complaints, they can open investigations into organisational non-compliance and systemic issues related to the DPF. Both the FTC and DoT have investigatory powers which enables them to demand reports and subpoena witnesses and issue binding orders and enforcement under their respective acts and enforcement powers.[154] Orders issued by the FTC or DoT can be enforced by either agency/department in a federal court.

As such, individuals do not generally have routes available to them to challenge the decisions or raise complaints about the FTC or DoT's enforcement activities. However, some decisions of the FTC are published online for independent review and public comment prior to being finalised, providing individuals the opportunity to object to agreements. Broadly however, where individuals have specific complaints, they can utilise each additional stage of redress from initial complaints to organisations through to binding arbitration to seek resolution.

[150] Annex C (ITA Letter) sets out that in the UK context the ICO is the national DPA for the purposes of the Framework.
[151] Annex C (ITA Letter) sets out that the UK Information Commissioner is the national or UK Data Protection Authority (or DPA) for purposes of the DPF.
[152] This is highlighted in footnote 14 of Annex D-1 (FTC Letter) (https://reportfraud.ftc.gov/).
[153] Annex D-1 (FTC Letter) and Annex E (DoT Letter).
[154] S.5 of the FTC Act and 49 U.S.C. §41712.

DPF Arbitration Panel

Annex I to the DPF sets out the Arbitration Mechanism, which was designed as a redress mechanism of '*last resort*' for residual claims that have not been resolved under the previous mechanisms set out above. It can be utilised where a violation of the DPF occurs - that is, where individuals believe certified US organisations have misapplied or breached the DPF Principles. It is also important to bear in mind that individuals are required to follow the other redress steps before invoking binding arbitration which may resolve complaints from individuals before this stage. The mechanism service itself is managed by the International Centre for Dispute Resolution (ICDR), which is the international division of the American Arbitration Association (AAA), who are responsible for managing the arbitration mechanism fund, as well as setting out and administering the rules for arbitration.[155] Certified US organisations are required to make a contribution to the fund for the arbitration mechanism. This fund cannot be used by individuals or organisations for attorney fees, if individuals desire to utilise their services. However, attorneys are not necessary to make use of the arbitration panel or mechanism, and therefore DSIT does not consider this to present an unreasonable barrier to individuals accessing the Arbitration mechanism. Arbiters are selected from a list of independent experts selected by the US and EU for the DPF. All panellists are selected for their independence, integrity, as well as experience in US privacy. Individuals are also selected based on their experience in EU privacy law. UK data protection law is currently closely aligned with the EU data protection framework. Additionally, the arbitration panel is designed to provide arbitration on issues arising from the application of the DPF, which is based within the US system and under US laws and practices. DSIT therefore does not believe it is necessary for panellists to have expertise in UK law, but this will be monitored going forward.

The Arbitration panel can impose equitable remedies as necessary in each case but cannot impose fines or award compensation. Decisions are binding on all parties and individuals (inc. UK data subjects) can seek judicial review and enforcement of a decision through a US Court under the Federal Arbitration Act - a judicial means to enforce the terms of the DPF. This route avoids the usual issues of demonstrating '*standing*' to bring a court action as individuals or organisations are utilising the statutory standing of the Federal Arbitration Act to enforce the decision of the arbitration panel.[156]

Department of Commerce (DoC)

Though not a mechanism for individuals to obtain redress under the DPF, the DoC has the ability to remove certified US organisations from the DPF for persistent failures to comply with the DPF Principles; such removal would include them returning or deleting personal data received through the DPF.[157] The requirements for "*persistent failure*" are set out under Supplemental

[155] https://go.adr.org/eu-us_dpf_annexi.html

[156] Individuals are required to establish "*standing*" in US courts when determining whether they are entitled to have a court decide the merits of a dispute or issue. In the US, there are three requirements for '*standing*', including demonstration that they have suffered an "*injury in fact*", demonstration of a causal link between such an '*injury*' and the complaint, and a demonstration that a favourable court decision would address the '*injury*'. Demonstrating an injury in fact may not always be possible where no material damage has been suffered by the data subject.

[157] After providing organisations 30 days to make representations prior to their removal.

Principle 11(g) of Dispute Resolution and Enforcement. The role of the DoC in facilitating cooperation with the national DPAs is further clarified within the ITA within the DoC letter to the Secretary of State concerning their role in administering the DPF.[158] This includes liaising between the ICO and certified-businesses where a complaint has been received or where the ICO has raised a question over a certified US organisation's compliance.

Each of the approaches and mechanisms set out above are specific to,[159] and set out within the DPF, and access is not restricted for UK data subjects under the UK Extension.

Individuals are free to pursue any of the mechanisms available to them under the DPF and there is no '*formal*' hierarchy associated with them. The exception to this is the arbitration mechanism, which requires that individuals seek to resolve their complaints through other mechanisms before it can be invoked.

The range of redress mechanisms available under the DPF means that UK data subjects can use a range and blend of remedies to enforce their data subject rights, ensuring that their rights are not undermined. The type of redress available also increases in formality from dispute resolution directly with a certified US organisation, through to routes for judicial redress following Arbitration (under the Federal Arbitration Act, following the convening of the Arbitration panel under the DPF).

Enforcement of Data Subject Rights

Both the UK GDPR and the DPF provide for mechanisms to enforce compliance with data subject rights (e.g. of access, erasure, correction etc.) and to otherwise secure orders for data to be deleted in cases of non-compliant processing.

Under the DPF, this begins with a request/complaint to the company in question. The DPF requires that certified US organisations provide a response to any complaints within a period of 45 days.[160]

Where a certified US organisation fails to comply with the data subject's request, the data subject can escalate their complaint. Under the DPF this would, in the first instance, be to the designated independent recourse mechanism, decisions of which certified US organisations are required to comply. Further up the chain, similar orders can be made by the national DPA, the FTC/DoT and the Arbitration Panel.

DSIT considers that these points evidence the suitability of the redress mechanisms available to the enforcement of data subject rights and provide comparable protections for UK data subjects as under the UK GDPR.

[158] Annex C (ITA Letter).

[159] With the exception of general enforcement powers of the FTC and DoT, though their specific roles and enforcement under the DPF is set out within the framework documentation and principles.

[160] DPF Supplemental Principle 11(d)(i).

Compensation and Fines

Both the UK GDPR/DPA 2018 and the DPF redress mechanisms provide, to differing extents, for rights to receive individual monetary compensation if a data subject suffers non-compliant processing of their personal data.

The route for a data subject to claim compensation under the UK GDPR is clear, albeit it involves the data subject going directly to court (individual compensation cannot be awarded by any intermediary body, such as the ICO). Under Article 82 of the UK GDPR, a data subject has an unconditional right to obtain compensation if a controller's infringement of the UK GDPR has resulted in material or non-material damage for the data subject.

Under the DPF, compensation to individuals may be ordered as a remedy by the independent dispute resolution body (however, it is important to note that not all such bodies offer this as a remedy.[161] Further, the FTC, following a final order, can utilise Section 19 of the FTC Act to sue a certified US organisation for consumer redress, although there is no explicit requirement under the DPF or FTC Act for them to do so.

Though there are limited routes to receive compensation specifically through the DPF, individuals do have the option to attempt to obtain compensation via bringing a suit pursuant to a tort within a US court (for example claiming *'invasion of privacy*' or '*injury in fact'*). However, individuals are required to establish "*standing*" and demonstrate that they have suffered an "*injury in fact*", which raises the bar on individuals pursuing these methods, but does not completely exclude the possibility[162]. Furthermore, State laws, including state Unfair and Deceptive Acts and Practices laws, can also offer private rights of action[163]. DSIT recognises that this is a general point of difference between the legal systems and routes available in the US and that which is available within the UK. As such, our analysis of redress primarily focuses on the routes available provided for under the DPF.

DSIT acknowledges that there may be some shortfall between the extent of the compensation right under the UK GDPR and the position under the DPF. However, UK data subjects may be able to claim, as above, to obtain enforcement of their data protection rights or obtain remedies over the use of their data which amount to significant redress for individuals, through other routes and laws.

With respect to fines for non-compliance, these may, and routinely are, imposed by the FTC as one of the relevant regulators of certified US organisations under the DPF, albeit normally through the mechanism of a consent decree under which the company does not admit liability

[161] Supplemental Principle 11. (e)(i) includes that compensation as a sanction that could result from a complaint to an independent dispute resolution body.

[162] A recent US Supreme Court decision in *TransUnion LLC v. Ramirez* does address the issue of "*standing*" relating to class-action suits against private defendants. This was primarily focused on the FCRA and the Supreme Court ruled that only individuals who can show concrete harm could seek damages. Specifically, that "*in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as a concrete harm*". However, courts are interpreting this case in different ways and how this will play out in the long-term within US litigation is still difficult to predict.

[163] https://www.nclc.org/images/pdf/udap/udap-report.pdf; all offer the ability for individuals to enforce the provisions of such acts in court, though the ability for individuals to challenge organisations vary from state-to-state.

but agrees to pay a penalty to settle the matter.[164] In a UK GDPR context, they are imposed by the ICO pursuant to Section 155 DPA 2018/Article 83 UK GDPR.

There is ample evidence that the FTC has enforced against Privacy Shield non-compliance in practice.[165] For example, in March 2022, the FTC settled privacy and security allegations with Residual Pumpkin Entity, LLC and PlanetArt, LLC for $500,000 and an agreement to an extensive compliance program. The FTC's complaint alleged that Residual Pumpkin Entity represented that it adhered to the EU-US and Swiss-US Privacy Shield Frameworks, but did not in fact adhere to the DPF Principles of Choice, Security, and Access, and thus the representations were false or misleading. The complaint alleged additional privacy and data security deficiencies, including that the respondents failed to properly disclose a data breach and failed to maintain reasonable data security practices.

Conclusion

Overall, there is a multi-layered process of redress available to UK data subjects. Though there are some areas which do not map directly across to UK GDPR, the options available, including the arbitration panel, allow UK data subjects to exercise these rights and enforce them as necessary (including ultimately through a judicial decision), and provide comparable protections for UK data subjects.

Focus on International and Onward Transfers

Principles accounting for onward transfers

The DPF does not set out any specific requirements for the **international** transfer of data by controllers or processors who have transferred personal data from the UK. However, the Accountability for Onward Transfers Principle (3.) and Obligatory Contracts for Onwards Transfers (10.) Supplemental Principle does apply for **all** transfers of personal data from certified US organisations who have received and/or transferred personal data under the DPF to organisations both within and outside of the US.[166]

Under the Accountability for Onward Transfers Principle, if certified US organisations wish to share or transfer personal data with other **controllers** or **processors** they must enter into a contract which requires that:

- Such data may only be processed for limited and specific purposes consistent with the original purposes or consent provided by the individual;

[164] The investigations and decisions of the FTC in relation to the Privacy Shield and Safe Harbor can be found in Annex D-2 (Appendix A of the FTC Letter).
[165] Annex D-2 (FTC Letter).
[166] All personal data received from the UK under adequacy regulations by Framework certified organisations would have been subject to requirements under UK GDPR and data protection legislation for international transfers between controllers and processors.

- The recipient of any transfer must continue to provide the same level of protection as would be found under the DPF and notify the original certified US organisation if it makes a determination that it can no longer meet such an obligation; and,
- If such a determination is made, the third-party will cease processing or take other steps to remedy the situation.[167]

The Onward Transfer Principles (as highlighted above) are considered in combination with the Data Integrity and Purpose Limitation, Notice, and Choice Principles.[168] Taken together in consideration, these Principles ensure that transfers that are for purposes incompatible with those originally set out to individuals should not take place.[169] The result being that where certified US organisations do want to share personal data with third parties, they meet the requirements under the Choice Principle, or have taken account of the Notice Principle and informed individuals of the transfer and identity of the third party and provided individuals with the chance to opt-out of such a transfer.[170] Additionally, the requirement within any onward transfer contacts, for the recipient of any transfer to provide the same level of protection as would be found under the DPF is key to ensuring that personal data is protected to the same standards when shared. If requested, certified US organisations under the DPF are required to provide a summary/representative copy of the privacy provisions of contracts to the DoC.[171]

Where recipient organisations are no longer able to meet such obligations set out under the contracts put in place, the contracts require that recipients to notify the transferring certified US organisation of such a determination. Contracts must provide that where such a determination is made, the third-party controller ceases the processing or takes other reasonable steps to remediate the deficiencies.

Where transfers take place with a third party acting as a processor (or agent), the responsibility for ensuring the personal data is protected in line with a certified US organisation's obligations under the Principles rests with the certified US organisation. To ensure compliance, the contract that organisations are required to put in place may be required to be shared with the DoC to check adherence to the Principles.[172] Additionally, though receiving controllers are not required to be participants of the DPF or have independent redress mechanisms, they are required to make available an equivalent mechanism.[173]

[167] The steps are slightly different depending on if the recipient is a controller or processor (or agent). If a controller, the contract must provide that the recipient controller will take reasonable steps to remedy the situation themselves. If a processor (or agent), then the responsibility sits with the certified-organisation under the framework to take appropriate action.

[168] The Accountability for Onward Transfers Principle specifically highlights the Notice (1.) and Choice (2.) Principles that certified-organisations transferring personal data (to third parties acting as controllers) should comply with.

[169] Under the Data Integrity and Purpose Limitation 5.(a) and Choice 2.(a) Principles.

[170] Or in the case of sensitive personal data, where individuals have to provide '*opt-in'* consent.

[171] DPF Principle 3(b).

[172] DPF Principle 3(b)(vi).

[173] DPF Supplemental Principle 10(c).

Outside of the DPF

Outside of the DPF, the US in general has no overarching laws[174] that set out how data may be shared or transferred internationally. However, the US participates in the APEC CBPR System and the Global CBPR Forum which provides a framework for organisations to certify compliance with government-backed data privacy and protection standards. An organisation that has committed to comply with the DPF Principles, is subject to the requirements of the Accountability for Onward Transfers Principle even if it is also certified to the CBPR system.

Where there are organisations who have a controller-controller or controller-processor relationship with a certified US organisation and who themselves are not certified US organisations, they may wish to make use of the CBPR framework for international transfers of personal data received originally through the DPF from UK data subjects. In these cases certified US organisations would be expected to have put in place contractual requirements under the Accountability for Onward Transfers Principle (3.) and Obligatory Contracts for Onwards Transfers (10.) Supplemental Principle to ensure that third-parties provide the same level of protection as is available under the DPF, including the requirement for contracts for any onward transfers of personal data.

Conclusion

DSIT views that the requirements under the DPF provide adequate protection for the onward transfer of personal data from certified US organisations and ensure that any onward transfers result in the flowing of protections alongside the personal data in question.

Enforcement and Supervisory Authority

The Federal Trade Commission (FTC)

The US does not have federal privacy legislation and therefore there is no singularly established Data Protection authority. However, the FTC is one of the most established and powerful regulators within the US and is the US's *de facto* privacy enforcement agency, and it is responsible for the enforcement of the DPF for the majority of organisations that self-certify. The FTC is also a member of a number of international privacy and data protection fora, such as the Global Privacy Assembly, the Global Privacy Enforcement Network, the International Consumer Protection and Enforcement Network, the International Conference of Data Protection and Privacy Commissioners, the Asia Pacific Privacy Authorities Forum, and the APEC Cross Border Privacy Enforcement Arrangement, in order to promote the international discussion of privacy and data protection. The FTC has also signed multiple Memoranda of Understanding with data protection authorities internationally, including the UK ICO, to support their role in investigating, enforcing and educating on privacy and data protection.

The FTC is a bipartisan independent federal agency, whose remit, jurisdiction and powers are clearly set out under the FTC Act. The FTC is led by 5 Commissioners, one of whom is selected to be Chairman by the President of the United States. Commissioners serve the FTC for a period

[174] However various sectoral legislation may provide specific requirements that must be followed.

of seven years. New Commissioners are selected by the President and confirmed by the Senate. At any one time no more than 3 Commissioners may be of the same political party. As an independent agency of the US government, Commissioners may not be arbitrarily dismissed by the President (or others) without cause.

The FTC is fully funded annually from appropriations from the federal government. In 2021 this budget was $351,000,000 with 1,123 full-time equivalent employees. The majority of these employees are public sector civil servants who have robust employment protections and are not subject to political appointment. Given the wide range of the FTC's jurisdiction over a large part of the US consumer sector, the branch that is dedicated to deceptions and unfair business practices in the marketplace (where enforcement for the Privacy Shield sits) had a budget of $186,198,000 with 612 full time equivalent employees.

The FTC's legislative authority that allows for the enforcement of the DPF is under Section 5 of the FTC Act ("s.5 FTC Act"). This section specifically allows the FTC to investigate (under s.5(b)) and take action against businesses under their authority provided in s.5(a) for "*unfair or deceptive acts or practices that affect consumers*".[175] The failure of certified US organisations to uphold their publicly stated commitment to follow the DPF Principles leaves them open to enforcement under this section of the FTC Act.

The FTC is able to open investigations based on directly received complaints, news reports, complaints from other businesses, referrals from the DoC and ICO or from internal research.The Recourse, Enforcement and Liability Principle of the DPF states that the FTC will give priority consideration to referrals of non-compliance with the DPF Principles from the DoC and national DPAs.[176]

The FTC's powers of investigation are detailed under the FTC Act and provide it with robust and broad investigatory powers to conduct thorough investigations.[177] If an organisation is found to have breached s.5, it can agree to a settlement with the FTC or to contest the complaint. If it chooses to contest the complaint, the FTC involves an FTC Administrative Law Judge ("ALJ") in a trial-type proceeding who finds for either the FTC (by issuing a *'cease and desist order'*) or for the organisations (by dismissing the complaint).[178] Once all judicial review of its order is complete, the FTC can then utilise Section 19 of the FTC Act to sue the organisation for consumer redress. If an organisation violates a final order, it is liable for a civil penalty for each

[175] The FTC issued a policy statement in November 2022 (https://www.ftc.gov/system/files/ftc_gov/pdf/P221202Section5PolicyStatement.pdf) setting out advisory guidance on the scope and meaning of unfair methods of competition under Section 5 of the FTC and issued a policy statement on deception under Section 5 of the FTC in 1983 (https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf).

[176] Further committed to by the FTC and DoT in their respective letters (Annexes D-1 and E) to the Secretary of State.

[177] Annex D-1 (FTC Letter) further details their investigative approach and sets out the commitments made to enforcing compliance by certified-organisations under the Framework.

[178] This decision may be appealed to the FTC Commissioners sitting as an adjudicative body. The Commission's final decision is then appealable by any respondent against which an order is issued; the respondent may file a petition for review with any United States court of appeals with jurisdiction.

violation pursuant to s.5(l) FTC Act.[179] The penalty is assessed by a federal district court in a suit brought to enforce the FTC's order, and the court may also issue "*mandatory injunctions*" and "*such other and further equitable relief*" as is deemed appropriate.

ALJs are judges under Article I of the US Constitution,[180] and the Supreme Court has recognised that the role of ALJs is "*functionally comparable*" to that of an Article III judge. Their independence and protection from unfair dismissal is ensured under the Administrative Procedure Act of 1946.[181] This provides an additional measure of independence, requiring that there be an evidentiary hearing in situations where organisations disagree with the enforcement action decided upon by the FTC and pass the decision to an independent ALJ for the final determination.

ALJs may only be removed from their roles by the agency that appoints them (in this case, the FTC) for '*good cause*'. This cause must be established and determined by the Merit Systems Protection Board following a hearing before the Board itself. The Merit Systems Protection Board is an independent agency established by the Reorganisation Plan No. 2 of 1978 and is a successor agency to the US Civil Service Commission. The Board consists of 3 members, who decide on the outcomes of hearings.

The FTC has a strong role in both enforcement and education, and regularly produces advisory opinions, reports and studies which help to clarify FTC rules and decisions.[182] The FTC also maintains a database on their website of all their cases, settlements and press releases which include those actions against organisations who have violated the DPF Principles or misrepresented their participation.

The FTC have recently posted multiple high value fines against organisations who have breached s.5 of the FTC Act, including $5 billion for Facebook[183] and at least $575 million for Equifax,[184] and a recent proceeding against Flo Health,[185] demonstrating the FTC's active enforcement of this section of the FTC Act upon organisations for privacy and data related breaches outside of the Privacy Shield. Such orders are intended to remain in place for 20 years, where any violations will result in court action for monetary damages, requiring structural changes to how these organisations handle personal data and manage the privacy of their customers.

[179] Violations of the FTC's administrative orders can lead to civil penalties of up to $ 50,120 per violation, or $50,120 per day for a continuing violation (15 U.S.C. § 45 (m); 16 C.F.R. § 1.98). This amount is periodically adjusted for inflation.

[180] Rather than Article III judges who are within the Judicial branch of the US government system.

[181] ALJs may only be dismissed for good cause, are assigned cases in a rotating schedule, may not perform roles and duties that are inconsistent with their role as an ALJ, are not subject to the authority of the individual investigative teams within the DoT and are required to conduct their activities impartially.

[182] Annex D-1 (FTC Letter).

[183] https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

[184] https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related

[185] https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc

Including the above high value fines, the FTC undertakes numerous investigations and sanctions against organisations who violate s.5 of the FTC Act. Since 2002 they have brought forward more than 70 cases against organisations under this section that have involved personal data and 21 of these have involved the former Privacy Shield framework. Though this number of investigations undertaken could be considered low by some for the time period, taken with DoC commitments[186] and processes to internally review and audit organisations on their compliance with the principles of the former Privacy Shield and DPF, DSIT concludes that this demonstrates a robust system of accountability and, where necessary, enforcement.

Conclusion

The reach and robustness of the actions and investigatory powers of the FTC is well known and demonstrated through their transparency and large cases that they have concluded. DSIT takes this to demonstrate that they are an effective and competent regulator that is well placed to service the enforcement requirements of the DPF.

The Department of Transportation (DoT)

The DoT is a department within the Executive branch of the US government, headed by the Secretary of Transportation, a Cabinet level politically appointed position. The DoT may take action against a US or foreign air carrier or ticket agent to abide by its public commitment to implement the DPF under 49 U.S.C. § 41712, which prohibits engaging in "*an unfair or deceptive practice*" in the sale of air transportation that results in or is likely to result in consumer harm. Violations of § 41712 can result in the issuance of cease and desist orders and the imposition of civil penalties of up to $34,377 (~£26,700) for each violation. This acts in the same way as s.5 of the FTC act and allows the investigation of certified US organisations who violate the DPF via their published privacy notices.[187]

Enforcement of s.41712 within the DoT is handled within their Office of Aviation Consumer Protection ("OACP"), who undertake investigation and prosecution of organisations found to have breached Section 41712. The OACP largely starts investigations through direct complaints, referrals from the DoC and other US agencies, and through their own volition.[188]

Though the Department and OACP sit within a federal Department headed by a political official, the final decisions on administrative and enforcement action, where investigators cannot come to an agreement with organisations over violations, are made by an ALJ. They have the authority, following an evidentiary hearing, to issue cease and desist orders, administrative orders and civil penalties following the investigation by the OACP. Though the DoT does not have the power to force the awarding of damages to individual complainants, it can approve settlements from organisations following investigations by the OACP that directly benefit consumers (eg. provision

[186] Annex C (ITA Letter).

[187] The exact definitions of "*unfair and deceptive practices*" used by the DoT were addressed in the "*Guidance Regarding interpretation of the Unfair and Deceptive Practices*" (https://www.transportation.gov/sites/dot.gov/files/2022-08/2022-18170_0.pdf) and are substantially based on the interpretation of such definitions as used by the FTC in their enforcement activities.

[188] The DoT have committed to prioritising investigations of violations, addressing false or deceptive claims of participation in the Framework, working with national DPAs and monitoring and making public enforcement orders where necessary. These were shared in Annex E (DoT Letter).

of cash or vouchers) which can offset monetary penalties which would otherwise be payable to the US government.[189] The DoT also has the power to revoke an airline's economic operating authority in the case of repeated non-compliance or egregious situations.

As above, ALJs are judges under Article I of the US Constitution, and the Supreme Court has recognised that the role of ALJs is "*functionally comparable*" to that of an Article III judge. Their independence and protection from unfair dismissal is protected under the Administrative Procedure Act of 1946.[190] This provides increased independence of the decisions that emerge from the DoT and requires an evidentiary hearing before an independent Judge for the final determination. This helps to ensure that any directions and decisions taken by the DoT against organisations are appropriately evidenced and taken with just cause, as well as to help individuals see breaches by organisations dealt with appropriately and independently.

The DoT as a whole had a 2019 budget of $86.4bn with 54,522 employees. While no specific information is available as to the breakdown of the OACP, the DoT and this office in particular have their own website where they publish the results of their investigations, as well as guidance relating to their enforcement of the DPF.[191]

Conclusion

Overall, the bodies within the US responsible for the enforcement of the DPF are robust and have a demonstrated history of enforcement which provides reassurances as to the effectiveness of their enforcement and accountability for certified US organisations who violate the DPF Principles

Data Privacy Framework Conclusion

On the basis of the above analysis, DSIT considers that the level of protection under the UK GDPR is not undermined when UK data subjects' personal data is transferred from the UK under the UK Extension to certified organisations in the US.

[189] Annex E (DoT Letter) under 'Enforcement Practices'.

[190] ALJs may only be dismissed for good cause, are assigned cases in a rotating schedule, may not perform roles and duties that are inconsistent with their role as an ALJ, are not subject to the authority of the individual investigative teams within the DoT and are required to conduct their activities impartially. See the section on '*Enforcement and Supervisory authority*' for further information on protections related to dismissal of ALJs within the US government.

[191] https://www.transportation.gov/individuals/aviation-consumer-protection/privacy

Government Access to Personal Data - An Overview

DSIT has assessed the framework under which US public authorities are able to access personal data after it has been transferred to the US for matters in the public interest, in particular for criminal law enforcement and national security purposes (referred to in this analysis as "*government access*"). Such access has the potential to undermine the level of protection afforded to UK data subjects after their data is transferred to certified US organisations.

DSIT recognises the responsibility of states for protecting the safety of their citizens and acknowledges that this may require interference with privacy rights for the purposes of meeting that responsibility. Such interference can be justified and still maintain the necessary level of data protection, if undertaken in accordance with certain principles, which is an important part of building trust.

When assessing the US public authorities' ability to access personal data from certified US organisations DSIT has taken into account information relating to the following principles:

- Any interference with the right to privacy by government access should be provided for by law.
- Interferences should be subjected to limitations and safeguards which ensure that access is necessary and proportionate in the pursuit of legitimate aims, to mitigate the potential for abuse.
- There should be effective redress and routes to rectify unlawful interference.

National Security

Introduction

DSIT has assessed the legal basis, oversight, and safeguards, in relation to the collection and the use of personal data transferred to the US under the UK Extension by US public authorities, for the purposes of national security. This assessment primarily considered the powers available under the Foreign Intelligence Surveillance Act ("FISA") and the safeguards, oversight, and redress provided by Executive Order ("EO") 14086.

Personal data transferred to certified US organisations, including under the UK Extension, may receive requests from the US government for data in their possession based on national security, subject to specific safeguards and conditions. The DPF explicitly recognises this possibility and that the company may be bound to comply with that request and disclose personal data transferred under the DPF to meet their legal duties in the US.

Authorisations under FISA and statutes authorising the use of National Security Letters ("NSL") provide the primary legal bases under which personal data transferred to the US may be accessed by US authorities for national security purposes. These legal bases contain additional safeguards and protections, supplemented by other legislation and EOs 14086 and 12333. DSIT has also assessed the underlying protections that apply to UK data subjects in the US system to ensure there is appropriate oversight and a system of checks and balances in circumstances where UK personal data may be accessed.

Overall, where the US government may access UK personal data for national security purposes, DSIT considers there to be appropriate limitations, safeguards, redress mechanisms and oversight; and any such interferences in UK individuals right to privacy is in accordance with the law and can be considered necessary in a democratic society in the interests of national security.[192]

Background

In the judgment of the *Schrems II* case in July 2020, the Court of Justice of the European Union ("CJEU") struck down the EU's adequacy decision for the predecessor framework to the DPF, the Privacy Shield. This meant that transfers from the UK to the US could also no longer be made in reliance on the Privacy Shield framework.[193] In the judgment the CJEU concluded that public authority access to personal data for national security purposes in the US was not subject to sufficient limitations and did not provide for effective redress for EU data subjects.

[192] As set out under the European Convention on Human Rights (Article 8).

[193] The transition period was ongoing at the time the *Schrems II* judgment was handed down, so it applied in the UK.

Following the *Schrems II* judgment, the US has introduced new rules and practices relating to government access to data for national security purposes, specifically designed to address the issues raised in that judgment. These include further privacy safeguards, strengthened oversight and a new redress mechanism by which UK data subjects will be able to challenge the unlawful signals intelligence collection and use of their data by the US government.

Specifically, on 7 October 2022 the US President issued a new EO 14086 on Enhancing Safeguards for United States Signals Intelligence Activities ("EO 14086"), which imposes further limitations and safeguards that govern all US signals intelligence activities. With respect to personal data transmitted to the US, the requirements of EO 14086 apply to any signals intelligence activities the US conducts, regardless of the type or source of data that is being collected.

Lawful basis for public authority access

Rules governing public authority access

Data transferred to the US and held by US organisations can be accessed by the US government for the purposes of national security only when authorised by statute or Presidential authorisation, and undertaken in compliance with US law, including the Constitution.[194] The President has inherent authority under Article II of the Constitution to protect the national security of the United States, which includes the collection of intelligence.[195] This power is not unlimited and it can be impacted by congressional action. The Congress has authorised certain surveillance regimes,[196] and supported the President's use of the orders and directives to impose safeguards and limits on intelligence activities.

The US government have confirmed that personal data that has been transferred to the US and held by US organisations can only be accessed for national security purposes under statutory authorisation, specifically either the requirements of FISA[197] - both Section 702 and other alternative FISA bases[198] - or under statutory provisions authorising access through NSLs.[199]

[194] S.2(a)(i) EO 14086.

[195] There are 18 organisations that make up the US Intelligence Community ("USIC"), see https://www.intelligence.gov/how-the-ic-works. They are constrained by rules adopted to regulate their functions (see https://www.intelligence.gov/mission/our-values/336-ethics), as well as specific Intelligence Community Directives that prescribe the manner in which they can act (see https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives).

[196] In particular, FISA, the NSL statutes, the Wiretap Act and the Stored Communications Act. See the following link for the letter from the Department of Justice seeking approval from Congress to reauthorise FISA s.702: https://www.justice.gov/oip/page/file/1570411/download

[197] FISA contains several bases for the accessing of personal data: s.105 FISA, s.302 FISA. s.402 FISA, s.502 FISA and s.702 FISA.

[198] Collectively FISA s.105, s.302, s.402 and s.502 are referred to throughout this analysis as "*alternative FISA bases*".

[199] 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; and 18 U.S.C. § 2709.

Foreign Intelligence Surveillance Act (FISA)

FISA is the main statutory authority for carrying out the collection of foreign intelligence (including signals intelligence referred to as "SIGINT" throughout[200]) information within the US. FISA has been amended by the USA Patriot Act of 2001, the FISA Amendments Act of 2008, the FISA Amendments Reauthorization Act of 2017, and the USA Freedom Act of 2015. FISA is an Act of Congress (i.e., a statute passed by the legislative branch and promulgated by the executive), and therefore clearly constitutes an identifiable law. To date, FISA Title VII provisions have been passed subject to a sunset clause, meaning that there are periodic re-evaluations of those provisions by the legislative branch, which has an opportunity not to extend or to amend the provisions if it believes they are being abused.

FISA contains several bases for the accessing of personal data:

- Section 105 FISA Title I, Subchapter I, which concerns traditional individualised electronic surveillance;[201]
- Section 302 FISA Title III, Subchapter III, which concerns physical searches for foreign intelligence purposes;[202]
- Section 402 FISA Title IV, Subchapter III, which concerns the installation of pen registers or trap-and-trace devices;[203]
- Section 502 FISA Title V, Subchapter IV, which permits the Federal Bureau of Investigation ("FBI") to submit "*an application for an order authorising a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility to release records in its possession for an investigation to gather foreign intelligence information or an investigation concerning international terrorism;*"[204] and
- s.702 FISA Title VII, in particular which allows US Intelligence Community ("USIC") elements to seek access to information, including the content of internet communications, from US companies, targeting non-US persons who are reasonably believed to be located outside the US with the legally compelled assistance of electronic communication providers.[205] This relates to the interception of communications of a non-US person located outside the US but where the communication itself is acquired in the US due to the architecture of the internet itself.[206]

[200] The description on the website of the ODNI CLPO sets out SIGINT as "*Signals intelligence is derived from signal intercepts comprising -- however transmitted -- either individually or in combination: all communications intelligence (COMINT), electronic intelligence (ELINT) and foreign instrumentation signals intelligence (FISINT). The National Security Agency is responsible for collecting, processing, and reporting SIGINT. The National SIGINT Committee within NSA advises the Director, NSA, and the DNI on SIGINT policy issues and manages the SIGINT requirements system.*"

[201] 50 U.S.C. § 1804.

[202] 50 U.S.C. §1822.

[203] 50 U.S.C. § 1842 with § 1841(2) and S.3127 of Title 18.

[204] 0 U.S.C. § 1861.

[205] 50 U.S.C. § 1881a.

[206] PCLOB, in its review of the s.702 programme, set out that s.702 surveillance "*consists entirely of targeting specific [non-U.S.] persons about whom an individualised determination has been made*" (Privacy and Civil Liberties Oversight Board, Report on the Surveillance Programme Operated Pursuant to s.702 if the Foreign Intelligence Surveillance Act, 2 July 2014, s.702 Report, p. 111). See also NSA CLPO, NSA's Implementation of

With respect to alternative FISA bases, these operate upon an individualised, targeted and warranted/court order-based system which is a robust safeguard that provides significant levels of certainty about the use of such surveillance routes. Throughout this analysis DSIT has highlighted protections pertaining to s.702 FISA, and have drawn upon safeguards in relation to alternative bases where applicable and in specific cases.

Executive Order 14086

EO 14086, "*Enhancing Safeguards for United States Signals Intelligence Activities*", introduced and further strengthens privacy and civil liberties safeguards as they relate to US SIGINT activities, as well as creating a new method of redress for persons whose personal data is transferred from countries that have been designated by the US.

The specific safeguards and redress mechanisms provided for under EO 14086 apply solely to SIGINT activities, which includes, as implemented, EO12333 and s.702 FISA (but excludes other alternative FISA bases and NSLs). Therefore (as highlighted below in '*Alternative FISA Bases and NSLs*'), whilst DSIT has conducted an analysis focusing on all the surveillance routes available under FISA, there is greater consideration of those areas (i.e. s.702 FISA and EO 14086) which DSIT believes warrant further examination as a result of recent legal challenges and subsequent case law in order to ensure UK data subjects rights and protections are not undermined when their personal data is transferred to the US.[207]

EOs are signed, written, and published directives from the President. They have the status of an identifiable law and are codified under Title III of the Code of Federal Regulations, which is the formal collection of the rules and regulations issued by the executive branch and other federal agencies. EOs are not legislation (they do not require approval from the Congress, and the Congress cannot simply overturn them). The President uses EOs to delegate his authority to relevant Executive agencies and direct their activities. As an instruction from the head of the executive branch, EO 14086 is binding, with the force of law, on the executive branch agencies (including the DoJ), on the intelligence community and within the military, including for military personnel in the National Security Agency ("NSA"). The DoJ has confirmed that compliance with the terms of the EO is mandatory. As set out in this analysis, the new redress mechanism can be used to invoke the protections contained in the EO, as well as violations of EO 12333 and FISA. In addition, the Foreign Intelligence Surveillance Court ("FISC")[208] further provides oversight and scrutiny of the requirements contained within FISA.

EO 14086 is a public document that is placed on the Federal Register so revocation or amendment will be made public.[209] The revocation of the EO would require the same public

Foreign Intelligence Act s.702, 16 April 2014. The term '*electronic communication service provider*' is defined in 50 U.S.C. § 1881 (a)(4).

[207] See *Schrems I* and *Schrems II* judgments of the CJEU.

[208] The role, composition and statutory footing of the FISC is set out further below in this analysis in the oversight section

[209] The daily journal of the federal government that is published to inform the public about federal regulations and actions.

procedural steps as enacting it in the first place. This would provide notification to the UK of revocation of the regulation.

Executive Order 12333

The USIC also has authority to conduct Signals Intelligence ("SIGINT") activities outside of the US, under EO 12333. However, the application of EO 12333 is largely outside the scope of our adequacy assessment and not directly relevant to it, as it is concerned primarily with extraterritorial evidence gathering, and not protections for personal data within the US which is the focus of our adequacy assessment under the UK GDPR. Where EO 12333 does provide safeguards for access within the US, these have been considered as part of the assessment and referred to where appropriate within this analysis. Furthermore, S.2(c)(ii) of EO 14086 includes requirements that specifically relate to bulk collection that is carried out under EO 12333. As collection within the US is always targeted, these provisions are not directly related to our assessment. However, DSIT still considers that the contents are indicative of the US' attitude towards data protection, and the safeguards that they apply to SIGINT generally.

Applicability of the rules to UK data subjects

Generally, the US system in some places makes distinction between US and non-US persons. The focus s.702 FISA is the collection of personal data of non-US persons, located outside the US, which could include the UK data subjects.

Under the Fourth Amendment of the US Constitution, US persons and persons located in the US enjoy an overarching right to non-intrusion by authorities in their private properties.[210] This has been interpreted to include information and data privacy. As such, the Fourth Amendment is baseline in US law regarding search warrants, wiretaps, and other forms of search and seizure. These constitutional protections apply to searches of US persons including those conducted in the US (and including searches conducted on data transferred to the US).[211] The Supreme Court has not directly ruled on the applicability of the Fourth Amendment to intelligence activities concerning non-US persons' data where the data is located in the US.[212]

Non-US persons who are located outside the US would generally not be able enforce Fourth Amendment rights in a US court, and US courts are generally not required to take into account Fourth Amendment rights when conducting judicial oversight of surveillance programmes

[210] Fourth Amendment to the US Constitution - "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*."

[211] These protections would be applicable where authorisations are being issued under FISA and through NSLs.

[212] Another relevant section of the US Constitution is the First Amendment, which has been interpreted by the courts to strictly protect the rights of the US press report on national security issues, including surveillance. It also protects against the overuse of defamation and libel claims to prevent such reporting, with strict requirements for proof of "*actual malice*" in any such suit - see *New York Times v. Sullivan, 376 US 254, 727 (1964)*. The First Amendment has also been interpreted to provide protections against the prior restraint of speech, including the censorship of any articles (see *New York Times Co v. US, 403 US, 713, 717 (1971)*) and enabling the publication of confidential information, even if obtained / shared with the journalist unlawfully (*see Bartnicki v. Vopper, 532 US, 514, 535 (2001)*).

impacting non-US persons located outside the US.[213] However, any surveillance that is carried out will still be subject to safeguards contained in FISA, other relevant legislation and EOs and implementing procedures, including EO 14086 where s.702 FISA has been relied upon, to ensure the protection of privacy and civil liberties, and with redress available under the routes discussed in 'Available Routes for Redress' section below.

EO 14086 applies to all US SIGINT activities in relation to all persons. It sets out that the "*United States recognizes that signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside.*"[214]

In relation to s.702 FISA, EO 14086 ensures that sufficient safeguards will underpin US signals intelligence activities in relation to the UK data subjects and the '*designation of a qualifying state*' requirement (in this case the UK), allows UK data subjects to access appropriate redress mechanisms provided for within the EO.

EO 14086 sets out explicitly that:

- signals intelligence activities can only be conducted in a manner "*proportionate to the validated intelligence priority [...] with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside*."[215]
- The policies and procedures designed to minimise the dissemination and retention of personal information collected through signals intelligence must ensure that there are equivalent protections for non-US persons as there are for US persons.[216]
- Signals intelligence collection priorities can only be validated "*after appropriate consideration for the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside*."[217]

Conclusion

DSIT considers that the bases for access are clearly set out in the body of legislation (e.g. FISA) and other enforceable directives (e.g. EO 14086) which are applicable to UK data subjects and provide the legal basis for government authority access to personal data.

[213] With respect to the Fourth Amendment, arguments have been advanced that non-US persons benefit indirectly from its protections. This is on the basis that all searches and seizures carried out by the US government on US soil (including on data transferred to the US from overseas) must meet Fourth Amendment standards, insofar as such searches and seizures must meet a reasonableness standard. However, this apparent protection, claimed by Swire and others, must be reconciled with the fact that: (i) the minimisation procedures under FISA, which the FISC considers in the light of the Fourth Amendment when approving programmes of searches on US soil under s.702, only apply to US persons; and (ii) EO 14086, as the primary source of protection for non-US persons, does not expressly deal with the Fourth Amendment or the concept of '*reasonable searches and seizures*'.

[214] S.1 EO 14086.

[215] S.(a)(ii)(B) EO 14086.

[216] S. 2(c)(iii)(A) EO 14086.

[217] S.2(b)(iii)(A)(3) EO 14086.

Nature and source of the requirement on private organisations to disclose the data

Alternative FISA bases and NSLs

FISA Title I s.105, and FISA Title III s.302 are known in the US as "*probable cause authorities*"[218] and require individualised warrant/court orders being authorised by the FISC on the basis of a probable cause finding[219] in order to exercise the authorisation provided by each section of FISA.

For FISA Title IV s.402, and FISA Title V s.502, neither of these allow the bulk collection of personal data. In the case of s.402 FISA, no contents of communications may be collected, instead focusing on phone numbers, dates and lengths of calls. s.502 FISA is focused on the collection of '*any tangible thing*'.[220] Both require an application[221] to the FISC to obtain authorisation (or a US Magistrate Judge).

In general however, the alternative FISA bases are specifically prohibited from the collection of bulk data under s.402 FISA, instead relying on and requiring the use of specific "*selection terms*".[222]

This individualised system is also the basis for NSLs. Compliance with an NSL is mandatory for organisations, and federal courts have the jurisdiction to review and enforce NSL requests when petitioned by recipients. Recipients may petition and be granted an order modifying, or setting aside an NSL, if the court finds that compliance would be unreasonable, oppressive, or otherwise unlawful. The standard is similar to the one that is used for subpoenas issued under the Federal Rules of Criminal Procedure (FRCP) (as set out in the Law Enforcement analysis below).

Conclusion

DSIT considers that the individualised and probable cause-based system of access to personal data through the above bases states how such powers are utilised and ensures UK data subjects' personal data is not unlawfully accessed without due cause by public authorities. This system is considered to be robust and is further explored below in the law enforcement analysis which has historically relied upon warrants, court orders and subpoenas as a lawful basis for conducting searches and surveillance.

[218] https://www.intelligence.gov/assets/documents/702%20Documents/statistical-transparency-report/2023_ASTR_for_CY2022.pdf

[219] This is based on a factual statement, in the application to the court that (i) the target is a foreign power or an agent of a foreign power, as defined by FISA, and (ii) the facility being targeted for electronic surveillance is used by or about to be used by, or the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power.

[220] These include books, records (e.g. electronic communications transactional records), papers, documents, and other items.

[221] The process for applications involves an assessment by court legal staff, clarificatory discussions with the requesting government department or agency, and finally a judge will ultimately decide whether to approve. The judge may also issue a Supplemental Order, attaching some form of reporting requirement to the request. More information is available at https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court

[222] 50 U.S.C. §1842 (c)(3).

S.702 FISA

Companies that are subject to s.702 FISA are required to comply with a Directive issued under s.702 FISA.[223] The US system contains specific requirements that must be satisfied before directives under s.702 FISA may be issued against telecommunications carriers, electronic communication service providers ("ECSPs"), and remote computing service providers.[224]

Once a directive has been received, an electronic communication service provider may decide to:

- Comply with the directive by immediately providing the US government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition, whilst minimising interference with the service being provided to the target of the interception. US ECSPs are not required to proactively disclose data, nor grant US intelligence agencies general access to the stored data itself; or
- Challenge the directive by application to the FISC on the grounds of unlawfulness[225].

Many major US tech companies have set out that they will, as a matter of course, challenge any requests that come through. If the company decides to challenge the directive, and then loses in court, a court order compelling compliance may be issued accordingly. Similarly, if the company merely refuses to comply from the outset, the AG can bring an action in the FISCt and, from there, the AG may obtain an order compelling compliance. In both cases, failure to comply is punishable by contempt which, in turn, is designed to compel compliance with an order through imposing fines and other remedies.

As referenced in *Schrems II*, certain programmes have been operating under FISA: for example, PRISM and UPSTREAM.[226] The same safeguards and limitations, including those set out in EO

[223] Only an electronic communication service provider can be issued with a FISA directive. Encompassing telecommunications carriers (under 47 U.S.C. § 153(51)), providers of electronic communications services (under 18 U.S.C. § 2510(15)), providers of remote computing services (under 18 U.S.C. § 2711(2)), any other communication service provider who has access to wire or electronic communications, and an officer, employee, or agent of any of these entities.

[224] Under s.702, the US AG and DNI may issue directives compelling US electronic communication service providers (ECSPs) to provide such information. An ECSP is defined as any service which provides to users the ability to send or receive wire or electronic communications. This would include companies that provide, for example, internal communication systems (eg, corporate email or messaging systems) or computer terminals running an electronic reservations system. An ECSP need not provide services to the public; giving any users the ability to send or receive communications is sufficient. This is consistent with both the US Department of Justice's published guidance as well as our interpretation, particularly in light of the broad definition and courts' willingness to apply it in a number of contexts. A business may qualify as an ECSP based upon only a small quantity of activity, even if that activity is unrelated to its primary function, such a distinction would not matter in the context of s.702's applicability – once a company meets the definition of an ECSP, it would need to provide all communications or data being sought that are within the scope of an authorised directive. See: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf

[225] 50 U.S.C. § 1881a(i)(4).

[226] Both PRISM and UPSTREAM were mentioned in the *Schrems II* judgment as programmes run under s.702 FISA, although the *Schrems II* judgment contained some inaccuracies as to the detail of the programmes. PRISM involves the direct '*downstream*' collection of communications by the NSA through the compelled assistance of electronic communications service providers. UPSTREAM involves the indirect '*upstream*' collection of communications through the compelled assistance of telecommunications providers that provide the backbone of the internet. This still requires the use of specific selectors. Only the NSA can collect data from the Upstream

14086 that limit the collection to ensure the protection of privacy rights apply regardless of the programme used.

Both the US and the UK have agreed to the OECD Trusted Government Access ("TGA") principles[227] which includes legal basis and transparency as two of the underlying principles.

The requirements and opportunity for challenge in the issuing of directives under s.702 FISA are clearly set out within the law and provide a transparent understanding of who and how these can be issued. On this basis and the above information, DSIT considers there to be a comprehensive and transparent body of laws, directives and rules which underpins US government access to UK personal data where it has been transferred to the US.

Limitations on access to data by public authorities

Purpose(s) for which the US public authorities can access personal data

The Director of National Intelligence ("DNI") is required to establish objectives, priorities, and guidance to the Intelligence Community for the collection, processing, analysis, and dissemination of intelligence: the National Intelligence Priorities Framework (NIPF).[228] Under the requirements of Intelligence Community Directive 204,[229] the President annually sets the nation's highest priorities for foreign intelligence collection after an extensive, formal interagency process.[230] The DNI then translates the intelligence priorities for the next 12-18 months into the NIPF. This is a classified document, which sets out high level priorities. These priorities address a diverse range of threats, and a description of these threats is published by the DNI in the annual public release of the Worldwide Threat Assessment.

The NIPF priorities are then translated into actual signals intelligence requirements managed by the National Signals Intelligence Committee ("SIGCOM").[231] SIGCOM is made up of

programme. The Upstream programme functions by filtering internet transactions to eliminate potential domestic transactions, then these are screened to only capture the communications linked to the specific selector. Only the communications that make it through both filters are stored for access by the NSA. The PCLOB concluded after its extensive review of the s.702 programme that it "*consists entirely of targeting individual persons and acquiring communications associated with those persons, from whom the government has reason to expect it will obtain certain types of foreign intelligence. The program does not operate by collecting communications in bulk*". PCLOB 702 Report at 103.

[227] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

[228] S.102A(f) of the National Security Act.

[229] https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf

[230] Cabinet officials are required to validate their signals intelligence requirements each year.

[231] SIGCOM was established in 1962 line with S.102, the National Security Act 1947 and EO 12333 to "*advise and assist the Director of Central Intelligence ("DCI") and the Director, National Security Agency (DIRNSA) in the discharge of their duties and responsibilities with respect to Signals Intelligence as specified in EO 12333, to monitor and assist in coordinating within the Intelligence Community the accomplishment of objectives established by the DCI, and to promote the effective use of Intelligence Community SIGINT resources*". See *DCID No. 6/1 SIGINT Committee*, https://www.hsdl.org/?abstract&did=441007. This Directive has since been superseded by S.1.3(b)12(A)(i) of EO12333, with the DIRNSA now leading the SIGCOM https://www.dni.gov/files/documents/ICD/ICD_113.pdf

representatives of all departments and agencies with a policy interest in signals intelligence, designated by heads of agencies of the USIC.[232]

Under EO 14086, there are additional requirements in relation to the development of the NIPF to ensure that privacy and civil liberties are considered in its development. Before presenting the NIPF to the President, the DNI must obtain from the Office of the Director of National Intelligence ("ODNI") Civil Liberties Privacy Officer ("CLPO")[233] an assessment of whether each of the intelligence priorities: advances one or more of the legitimate objectives (set out below); does not contravene the prohibited objectives (set out below); and was established after appropriate consideration for the privacy and civil liberties of *all* persons. In the case of disagreement between the ODNI CLPO and DNI, both sets of views must be presented to the President, who has the Constitutional authority to direct intelligence activities.

In a narrow set of circumstances (particularly the need to address a new or evolving intelligence requirement) such priorities can be set directly by the President or the head of an agency in the USIC, who in principle have to apply the same criteria as the ones described in s.2(b)(iii)(A)(1)-(3), see s.4(n) EO 14086.[234] However, this is not a unilateral process and still involves an authoritative inter-agency process, requiring the review and assessment of the ODNI CLPO prior to any amendments to the NIPF being presented to the President for final decision.

This system ensures that the consideration of privacy and civil liberties is at the heart of the setting of US signals intelligence priorities. The ODNI CLPO's views are given the same weight as that of the DNI, and will play a part in the Presidential authority to determine. This is of particular importance to s.702 FISA activities as these priorities represent the foundations of the programme and these intelligence priorities set the direction for US SIGINT collection in general.

The above and the role of the DNI in this overall process, apply to the collection of all intelligence under s.702 FISA. The FISA statute also specifies the purposes for which the US can collect "*foreign intelligence information*" through the various sections of FISA.[235] The US cannot collect information purely because the intended target is a non-US person.

The definition of '*Foreign intelligence information*' is primarily focused on matters such as: attacks against the US; sabotage; terrorism; and clandestine intelligence activities of foreign powers, all which align with national security considerations for the state. An exception to this is '*the conduct of the foreign affairs of the United States*', which may well encompass broader aims, such as diplomacy and international relations. The requirements under FISA, in particular because of the nature of the President's wide authority, and the definitions used in FISA, are

[232] https://www.hsdl.org/?abstract&did=441007

[233] CLPOs have a variety of roles to ensure protection of privacy and civil liberties within intelligence gathering and serve as the principal advisors in this regard to various departments, agencies, and elements that make up USIC. The position and role of the ODNI CLPO is the principle of these within the USIC. The overall role is discussed further below in section on '*CLPOs*'.

[234] DSIT notes that in these narrow circumstances, the decisions will be taken at the highest level of government, demonstrating the level of seniority under which these decisions will be taken. It is not for USIC to internally decide and authorise new intelligence priorities.

[235] Foreign intelligence information is set out in 50 U.S.C. § 1801 (e).

drafted in a broad but not unlimited manner, supplemented by binding policies and procedures that govern day to day activities.[236]

EO 14086 specifically delineates the overarching parameters for all signals intelligence activities, including those carried out under s.702 FISA:

- EO 14086 introduces a specific list of legitimate objectives that can be pursued by signals intelligence collection.[237] The list is exhaustive. In the case that a new security threat emerges, the President has the ability to update the list. Any updates must be released to the public, except in cases where the President determines that to do so would pose a risk to the national security of the US.[238]
- EO 14086 also sets out specific prohibited objectives that can never be pursued through signals intelligence activities: suppressing or burdening criticism, dissent, or the free expression of ideas or political opinions by individuals or the press; suppressing or restricting legitimate privacy interests; suppressing or restricting a right to legal counsel; or disadvantaging persons based on their ethnicity, race, gender, gender identity, sexual orientation, or religion; or to use foreign private commercial information / trade secrets to afford a competitive advantage to US companies.[239] The protections under EO 14086 mitigate against the broad scope of the definitions used for s.702 FISA purposes.

The legitimate objectives cannot be used by the intelligence agencies as the sole basis for US intelligence collection. The relevant operational sections of the USIC are required to further substantiate more concrete and specific priorities for which signals intelligence may be collected, as set out in the NIPF.

A s.702 FISA certification authorising the targeting of non-US persons located outside the US must attest that "*a significant purpose of the acquisition is to obtain foreign intelligence information*" and requires individual targeting determinations that the target is a non-US person who is reasonably believed to be located outside the US; and who has or is expected to communicate or receive foreign intelligence information.

Conclusion

The requirement for collection to be in "*the pursuit of specified and legitimate aims*"[240] is a principle under the OECD TGA. DSIT considers that the process for setting the purposes of collection of foreign intelligence information under FISA, and as otherwise set out in this analysis, is limited to collection for legitimate aims and purposes. Overall, the above information sets out a robust and balanced process for setting collection purposes involving due regard for privacy

[236] S.702 of FISA is concerned with the gathering of "*foreign intelligence information*". "*Foreign intelligence information" is broadly defined, and encompasses information that has a relationship with open-ended concepts such as "the national defence or security of the United States*". This is not unique to US law, for example the Investigatory Powers Act in the UK authorises the acquisition of data including in bulk for purposes relating to the protection of "*national security*".

[237] S.2(b)(i) EO 14086.

[238] S.2(b)(i)(B) EO 14086.

[239] S.2(b)(ii) EO 14086.

[240] OECD TGA principles, II Legitimate Aims.

and civil liberties, under EO 14086, whereby the ODNI CLPO's views in this area are given the same weight as those of the DNI.

The limitations and conditions under which interference with privacy can occur

Alternative FISA bases

The alternative bases under FISA allow for different sorts of access to data. The requirements for each are based on (a) the techniques that are used for each sort of access; and (b) the expectation of privacy in relation to the data sought. Electronic surveillance under FISA[241] is generally conducted under a FISC order unless the surveillance fits within one of three statutory exceptions.[242] Importantly, the alternative FISA bases require individualised court orders and/or warrants to proceed, which in itself provides a greater level of protection and oversight (by FISC and/or the judiciary) in the applications for and approval of the use of these surveillance routes.

FISA Title I, Subchapter I, s.105: In order to carry out individualised surveillance under s.105 FISA, an application for a court order authorising electronic surveillance for foreign intelligence purposes must be made by a federal officer in writing to an FISC judge. The application would have to contain, *inter alia*, a statement of the facts and circumstances that have been relied on to justify their belief that there is probable cause that the facility is used or about to be used by a foreign power or an agent of a foreign power,[243] as well as information as to the information and procedures that will be used.[244]

The application must be approved by the FISC based upon a finding that the relevant criteria and requirements have been met on the basis of submitted facts. The FISC can issue an *ex parte* order as requested approving the electronic surveillance, or a modified order if the judges decide the request does not meet the criteria and requirements.

An order under s.105 FISA can approve electronic surveillance for the period of time that is necessary to achieve its purpose or for 90 days, whichever is less. However, if the order is targeted against a foreign power,[245] or against an agent of a foreign power who is not a US

[241] 50 U.S.C. § 1801 et seq.

[242] These three exceptions are: 50 U.S.C. § 1802 (electronic surveillance of three categories of foreign powers for up to one year without a court order upon AG certification; the three categories, as defined in 50 U.S.C. §§ 1801(a)(1), (2), or (3), cover (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of US persons; or (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments); 50 U.S.C. § 1805(f) (emergency electronic surveillance upon AG certification for up to 72 hours while an FISC order is being sought); and 50 U.S.C. § 1811 (electronic surveillance for 15 calendar days after a congressional declaration of war).

[243] An agent of a "*foreign power*" may include non-US persons that engage in international terrorism or the international proliferation of weapons of mass destruction (including preparatory acts) (50 U.S.C. § 1801 (b)(1)).

[244] 50 U.S.C. § 1805. Under 50 U.S.C. § 1804(b): In determining whether or not probable cause exists a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.

[245] A "*foreign power*" as defined in 50 U.S.C. § 1801(a)(1), (2), or (3) includes *"a foreign government or any component thereof, whether or not recognized by the United States*;" "*a faction of a foreign nation or nations, not substantially composed of United States persons*;" or "*an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments*."

person, then the order can approve an electronic surveillance for the period specified in the order or for one year, whichever is less.

FISA Title III, Subchapter II s.301: To carry out a search of a premise or property that is meant to result in access to data (e.g. through inspection or search of information, material or property), a federal officer is required to make an application to the FISC setting out, *inter alia*, that there is probable cause that the target of the search is a foreign power or an agent of a foreign power; that the premise or property to be searched contains foreign intelligence information and that the premise to be searched is owned, used, possessed by, or is in transit to or from an (agent of a) foreign power.

The application must be approved by the FISC based upon a finding that the relevant criteria and requirements have been met on the basis of submitted facts. The order can be granted for the period necessary to achieve its purpose, or for 90 days, whichever is less. Where an order approves a physical search targeted against a foreign power, it can be granted for the period specified in the application or for one year, whichever is less, and an order under this section for a physical search against an agent of a foreign power may be for the period specified in the application or for 120 days, whichever is less.

Under both s.105 and s.301 FISA, the FISC can grant an application for an extension on the same basis as an original order, but including new findings to support an extension.[246]

FISA Title IV, Subchapter III s.402: Under s.402 FISA, investigating agencies can apply for an order or extension of an order authorising or approving the installation and use of a '*pen register/trap and trace*' devices.[247] The application must be made in writing under oath or affirmation to a FISC judge or US magistrate judge.[248] It must contain a certification by the applicant "*that the information likely to be obtained is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities*" and specify a selector (i.e., a specific person, account, etc.). This use of the selector limits, to the greatest extent reasonably possible, the scope of the information sought. The information sought under s.402 FISA cannot include the content of communications but can include the metadata (e.g. name, address, subscriber number, length/type of service received, source/mechanism of payment).

Generally, an order may authorise the installation and use of a pen register or trap-and-trace device for a period not exceeding 90 days. Extensions of such an order may also be granted for up to 90 days. However, in the case of an application under subsection 1842(c) where the applicant has certified that the information likely to be obtained is foreign intelligence information

[246] 50 U.S.C. § 1801(a) and 50 U.S.C. § 1805(e)(2)(A) and (B). An extension of an order for a surveillance targeted against a foreign-based political organisation, not substantially composed of United States persons or an entity that is directed and controlled by a foreign government or governments, or against a group engaged in international terrorism or activities in preparation for that, that is not a United States person, may be for a period of up to one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period involved. In addition, an extension of an order for surveillance targeted at an agent of a foreign power who is not a US person may be extended to a period not exceeding one year.

[247] These devices capture dialling, routing, addressing or signalling information.

[248] 50 U.S.C. § 1842 (b). The magistrate judge must have been publicly designated by the Chief Justice of the United States to hear these applications.

not concerning a US person, an order, or an extension of an order for a FISA pen register or trap-and-trace device may be up to one year.[249]

FISA Title V, Subchapter V, s.502: Under s.502 FISA, the FBI can submit an application to the FISC or a magistrate judge for an order authorising a common carrier (e.g. a person or entity transporting people by land, water, air or rail for profit), public accommodation facility (e.g. hotel), physical storage facility, or vehicle rental facility to "*release records in its possession for an investigation to gather foreign intelligence information or an investigation concerning international terrorism.*"[250] The application must contain specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power.[251]

Upon application, the judge will enter an *ex parte* order (as requested or as modified), approving the release of the records if the judge is satisfied with the application.[252] The relevant companies are required to comply with an order, and cannot disclose the existence of, and their compliance with, the order as to not undermine the investigation.[253]

National Security Letters (NSLs)

NSL statutes authorise intelligence officials to request certain business record information. Although variously phrased, the purpose for each of the NSLs is to acquire information related to the requesting agency's national security concerns. The most common statement of purpose is "*to protect against international terrorism or clandestine intelligence activities*". Unlike administrative subpoenas and grand jury subpoenas, NSLs can only be used to seek certain transactional information permitted under the five NSL provisions, and NSLs cannot be used to acquire the content of any communications.[254]

The relevant statutes related to transactional information are:

- Right to Financial Privacy Act, for financial institution customer records;[255]
- FCRA for a list of financial institution identities and consumer identifying information from a credit reporting company,[256] or for a full credit report in an international terrorism case;[257]

[249] 50 U.S.C. § 1842 (d).
[250] 50 U.S.C. § 1862 (a).
[251] 50 U.S.C. § 1862 (b).
[252] 50 U.S.C. § 1862 (c).
[253] 50 U.S.C. § 1862 (d).
[254] Each of the NSL statutes includes a requirement that the NSL demand be limited to specifically identified information rather than insisting on delivery of record information for all of a recipient's customers - see 12 U.S.C. 3414(a)(2); 15 U.S.C. 1681u; 15 U.S.C. 1681v; 18 U.S.C. 2709 (b).
[255] 12 U.S.C.§ 3414 (a)(5).
[256] 15 U.S.C.§ 1681u (a) and (b).
[257] 15 U.S.C. § 1681v.

- Electronic Communications Privacy Act ("ECPA") for subscriber information, toll billing records information and electronic communication transactional records from wire or ECSPs.[258] Only the FBI can make requests under the ECPA;[259] and
- National Security Act for financial, consumer, and travel records for certain government employees who have access to classified information.[260] For the purposes of this paper, DSIT will not be looking at this basis, as it will not relate to the data of UK data subjects.

DSIT notes that two of the statutes relate to financial institutions and credit reporting companies, many of which are excluded from participation in the DPF, as "*most depository institutions (banks, federal credit unions, and savings & loan institutions)*" do not fall under the regulatory remit of the DPF.[261] It is therefore likely that some aspects of the above use of NSLs would not be relevant for this assessment. Regardless, the NSL applications must specifically identify the customer, entity, or account to be used as the basis for the production and disclosure of financial records, ensuring that any access to UK personal data would be specific and targeted.

s.702 FISA

Prior to being permitted to collect foreign intelligence information under s.702 FISA, the AG and DNI are required to submit annual certifications to the FISC that identify categories of foreign intelligence information to be acquired, such as intelligence related to counterterrorism or weapons of mass destruction, which must fall within the categories of foreign intelligence defined by the FISA statute.[262] The Privacy and Civil Liberties Oversight Board ("PCLOB")[263] noted that, "*[t]hese limitations do not permit unrestricted collection of information about foreigners*".[264] In addition, these must now also reflect a Legitimate Objective under EO 14086.

s.702 FISA sets out the elements that must be included in each programme certification.[265] The certifications themselves are classified and not publicly available. These certifications:

- identify categories of foreign intelligence information to be gathered, and
- attest that the procedures and additional guidelines adopted to ensure compliance are consistent with the Fourth Amendment, compliant with limitations set out in statute, that a "*significant purpose*" of the programme is to obtain foreign intelligence information and that it meets one of the Legitimate Objectives as set out in EO 14086. These entails ensure that there is a significant foreign intelligence purpose for the surveillance, and not only a criminal law enforcement purpose. Agencies must also apply protections required by EO 14086 to s.702 FISA acquired information.

[258] 18 U.S.C. § 2709.
[259] 18 U.S.C. 2709 (b); 12 U.S.C. 3414(a)(5)(A); 15 U.S.C. 1681u(b).
[260] 50 U.S.C. § 3162.
[261] 15 U.S.C.§ 45(a)(2).
[262] 50 U.S.C. § 1881a (g). The DNI has released a redacted certification - https://www.dni.gov/files/documents/0928/DNI-AG%20702g%20Certification.pdf
[263] The PCLOB is an independent board with a statutory oversight role. Further information on the role and statutory footing of PCLOB is set out below in the Oversight and Enforcement section.
[264] Privacy and Civil Liberties Board, '*Report on the Surveillance Program Operated Pursuant to s.702 of the Foreign Intelligence Surveillance Act*' (July 2, 2014) ('*PCLOB Report*').
[265] s.702(h)(2) of FISA.

These certifications are to be accompanied by targeting minimisation and querying procedures, which are also approved by the FISC and are legally binding on US intelligence agencies.[266]

- The Targeting Procedures require the NSA to assess, based on the totality of the circumstances, that targeting a specific person is likely to acquire a category of foreign intelligence information identified in a certification. In order to avoid indiscriminate surveillance, the US targeting procedures mandate that they can only select a target where they are already aware about them and where they are aware of a specific selector (e.g. email address or telephone number) that is used by the target.[267] The procedures exclude the use of "*general keywords*" or even the names of individuals, on the basis that such terms would not identify specific communications facilities and the USA FREEDOM Act of 2015 prohibits bulk collection of records pursuant to FISA.[268] This ensures that collection of information for intelligence purposes is precisely focused and targeted rather than indiscriminate.[269] In addition, the tasking of the selector must "*be likely to acquire one of the types of foreign intelligence information identified in a Section 702 certification*."
- The Minimisation Procedures require the agencies to establish detailed and binding restrictions on each intelligence agency's acquisition, retention and dissemination of personal information.[270]

In this way, s.702 FISA allows for the approval of an overall programme of surveillance and provides a mechanism for independent judicial specification of the circumstances and conditions under which interference can occur. This process is overseen by the FISC.

The FISC is able to either grant or deny the certification (in full or in part), and can request that procedures be amended. The FISC's review of the procedures encompasses both how the procedures are written and how the procedures are implemented by the government.[271] The FISC has modified surveillance applications where they have required collection procedures be amended and required the government to justify surveillance techniques the court anticipates arising in future cases. The FISC has also directed the IC to effectively suspend certain activity when it has found a problem. Where there are significant interpretations to decisions of the FISC, the DNI is required to declassify and publish these. Overall, the US has released a variety of documents that demonstrate that the FISC is actively engaged in supervising individual targeting decisions under s.702 FISA[272] and provides an ongoing review of targeting procedures, ensuring that compliance is in line with the requirements under s.702 FISA.

[266] 50 U.S.C. § 1881a (i).

[267] See NSA Targeting procedures, page 2.

[268] The PCLOB found that for both Upstream and Downstream, collection is based on the use of selectors which may not be a '*keyword*' or particular term (e.g. '*nuclear*' or '*bomb*') but must be a specific communications identifier (e.g. email address) PCLOB 702 Report at 123.

[269] A US federal appeals court has previously ruled that the government's interpretation of the business records provision of s.502 FISA was "*unprecedented and unwarranted*", leading to the termination of that programme by Congress.

[270] EO 14086 extends these restrictions to foreign nationals.

[271] See e.g. FISC, Memorandum Opinion and Order at 35 (18 Nov. 2020) (Authorised for Public Release on 26 April 2021), (Annex D).

[272] See, for example Decisions, Orders, and Memorandum Opinions of the FISC discussing its supervisory role over the propriety of individual targeting under FISA 702

However, once a certification has been provided, the FISC plays no role in making the actual targeting decisions (such decisions are made by the NSA, with input provided by relevant officials in the Central Intelligence Agency ("CIA") and FBI).

Following approval, the USIC has an extensive process by which the certifications will be translated into SIGINT, which are publicly available through the published targeting procedures document.[273] These requirements ensure that the agencies collecting US SIGINT operationalise the concepts of necessity and proportionality, and that there is proper oversight of each decision to undertake targeting.

Initially, all US departments and agencies that are consumers of foreign intelligence submit their requests for collection on the basis of approved certifications to the SIGCOM.[274] They review those requests, ensure that they are consistent with the NIPF, and assign them priorities using criteria such as how critical the collection is, whether there are better or more cost effective sources of information available, and whether the collection is as tailored as feasible, taking into account time, geographic or other limitations.

The US signals intelligence requirements process also requires explicit consideration of whether the target of the collection, or the methodology used to collect, is particularly sensitive.[275] If so, it will require review and approval by senior policymakers. The Signals Intelligence Committee will also consider whether the collection presents an unwarranted risk to privacy and civil liberties, regardless of nationality, and whether additional dissemination and retention safeguards are necessary to protect privacy or national security interests.

At the end of this process, trained NSA personnel translate the validated priorities into specific selection terms, which are expected to collect foreign intelligence responsive to these priorities. Any selector must be reviewed and approved before it is entered into NSA's collection systems.

After the FISC approves a certification, the US government may issue "*directives*" to electronic service providers subject to FISA in the US to provide communications of non-US persons reasonably believed to be located outside the US and containing the type of foreign intelligence information covered by the certification. The government may then issue requests to the provider for communications data within the scope of the directive, consistent with the Court-approved targeting procedures. The NSA receives the data acquired under s.702 FISA, and the CIA,the FBI and the National Counterterrorism Centre ("NCTC") receive portions of the data. FISA does

(https://www.intel.gov/assets/documents/702%20Documents/declassified/21/2021_FISC_Certification_Opinion.pdf), NSA 2021 Targeting Procedures (https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_NSA_Targeting_Procedures-Amended.pdf) and 24th Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to s.702 of the Foreign Intelligence Surveillance Act (see https://www.intel.gov/assets/documents/702%20Documents/declassified/24th-Joint-Assessment-of-FISA-702-Compliance.pdf).

[273] See: https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_Cert_NSA%20Targeting%20Procedures_10.19.2020.pdf.

[274] https://www.hsdl.org/?abstract&did=441007.

[275] This phrase is not explicitly defined. However, DSIT is content that sensitive data would receive the same protections as other types of data collected by the USIC and only be disclosed under the same limited disclosure requirements.

not impose any generalised data retention obligations on electronic communications service providers.

Individual targeting decisions under s.702 FISA must be recorded by the government; every targeting decision must include the specific rationale for targeting a specific person to obtain foreign intelligence information. The fact-based decision is informed by the analytical judgement, the specialised training and experience of the analyst, as well as the nature of the foreign intelligence information to be obtained. A number of requirements govern the decision as to whether and to what extent signals intelligence can be used to further an identified priority - set out in the 'Consideration of the impact on the privacy of the affected individual(s) in the decision to undertake interference' section below.

The NSA engages in an extensive review process to ensure that a targeting decision is never taken in isolation. Analysts are required to work within strict parameters, after undergoing specific training on what is and is not acceptable. The PCLOB review of s.702 FISA implementation[276] sets out that the NSA must verify that there is a connection between the target and the selector, must document the foreign intelligence information expected to be acquired, this information must be reviewed and approved by two senior NSA analysts,[277] and the overall process will be tracked for subsequent compliance reviews by the ODNI and Department of Justice.[278] Prior to tasking, at least one subject matter expert and one supervisor at NSA review the tasking. This serves the dual role of ensuring that all the precollection requirements have been satisfied, as well as facilitating oversight. The records of the analysts' specific targeting rationale would be made available to the ODNI CLPO and the new redress court established under EO 14086[279] (as it is available to the DoJ oversight office) and, where necessary, the FISC in order to assist with effective oversight.

The requirements under EO 14086 are implemented by the relevant agencies through updated policies and procedures[280] that translate the requirements of EO 14086 into day-to-day operational parameters. In order to aid transparency and oversight, on 3 July 2023 the US government published the updated policies and procedures.[281] They demonstrate both the definition of the rules and how they will be applied in practice by the relevant agencies. Now that the updated policies and procedures are in place, the PCLOB will carry out a review of the procedures to ensure that they meet the requirements of EO 14086.[282] When this review is completed, within 180 days each intelligence agency must address and/or implement any recommendations that PCLOB set out.

[276] PCLOB, s.702 Report, p. 46.

[277] These analysts are trained by the NSA regarding the applicable procedures to ensure NSA personnel responsible for approving the targeting of persons under these procedures, as well as NSA personnel with access to the acquired foreign intelligence information understand their responsibilities and the procedures that apply to this acquisition.

[278] See NSA CLPO, NSA's Implementation of Foreign Intelligence Act s.702, 16 April 2014.

[279] The Data Protection Review Court ("DPRC"), as set out below in the section on redress

[280] S.2(c)(iv) EO 14086

[281] See: https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-proceduresimplementing-new-safeguards-in-executive-order-14086.

[282] S.2(c)(v) EO 14086

Conclusion

DSIT is content that data subjects will be sufficiently able to identify circumstances in which their personal data could be accessed by the US government, especially in light of the amendments made as part of EO 14086. Additionally, the multi-layered approach that involves multiple elements of the USIC and a judicially independent court (FISC) to approve and monitor how access is certified and targeted ensures a robust system is in place for the collection of surveillance.

This robust approach is also aligned with the OECD TGA principles on "*approvals*".[283]

Consideration of the impact on the privacy of the affected individual(s) in the decision to undertake interference

The impact on privacy is taken into account at all stages of the decisions taken as to whether to undertake interference. These include the role of the amicus in advising the court of the impact of any surveillance applications upon individual privacy (see 'Available Routes for Redress' section below).

Furthermore, under s.702 FISA, minimisation procedures also apply to searches for foreign intelligence purposes (physical or electronic). These procedures are designed to minimise acquisition and retention, and to prohibit dissemination of non publicly available information concerning unconsenting US persons, consistent with the needs of the US to obtain, produce and disseminate foreign intelligence.

Alternative FISA bases and NSLs

For alternative FISA bases, consideration is given on a case-by-case basis and forms part of the reasoning as to whether a warrant should be granted. The interference with privacy is balanced against the strict order requirements under the terms of the FISA statute. The whole basis for obtaining a warrant is that the information that is being sought is subject to a reasonable expectation of privacy. In order to ascertain the reasonableness of a particular government action, the FISC must take into account the totality of the circumstances.[284] This includes a consideration of the nature of the intrusion and how it is implemented.[285] The more important the government's interest, the greater the intrusion that may be constitutionally tolerated.[286] This approach requires that the government balance the competing interests at stake when considering when to grant the warrant.[287]

[283] OECD TGA principles, III Approvals.
[284] *Samson v. California*, *547 U.S. 843, 848, 126 S.Ct. 2193, 165 L.Ed.2d 250 (2006).*
[285] Garner, 471 U.S. at 8, 105 S.Ct. 1694; Place, 462 U.S. at 703, 103 S.Ct. 2637.
[286] See, e.g. *Michigan v. Summers, 452 U.S. 692, 701-05, 101 S.Ct. 2587, 69 L.Ed.2d 340 (1981).*
[287] See *Samson, 547 U.S. at 848, 126 S.Ct. 2193; United States v. Knights, 534 U.S. 112, 118-19, 122 S.Ct. 587, 151 L.Ed.2d 497 (2001).*

For NSLs, their use is subject to the general rules and requirements concerning privacy and civil liberties.[288]

S.702 FISA

As set out above, EO 14086 requires that the ODNI CLPO certify to the President that the intelligence priorities identified in the NIPF are only established after appropriate consideration for the privacy and civil liberties of all persons on a programmatic basis.[289]

EO 14086 sets out several constraints on the use of any and all SIGINT activities. EO 14086 translates the underlying concepts (e.g. the balancing exercise between the need to carry out SIGINT with protecting civil liberties and privacy) into specific requirements for the US system. It contains the specific factors that US agencies are required to take into account when deciding to carry out SIGINT activities, all of which help to ensure that the intelligence collection is necessary and proportionate. This encompasses both on a programmatic and case-by-case basis:

SIGINT may only be collected "*following a determination that, based on a reasonable assessment of all relevant factors, the collection is necessary to advance a specific intelligence priority*".[290] In determining whether a specific signals intelligence collection activity is necessary to advance a validated intelligence priority, US intelligence agencies must consider the availability, feasibility and appropriateness of other less intrusive sources and methods, including from diplomatic and public sources.[291] When available, such alternative, less intrusive sources and methods must be prioritised.[292]

When signals intelligence collection is considered necessary, it must be carried out to be as "*tailored as feasible*" and must "*not disproportionately impact privacy and civil liberties*."[293] In making this determination, the analyst will take into account relevant factors including the nature of the pursued objective, the intrusiveness of the collection activity including its duration, the possible contribution of the collection to the objective pursued, the reasonably foreseeable consequences to individuals, and the nature and sensitivity of the data to be collected. In practice, this means that the US will be striking a proper balance between national security needs and the protection of privacy and civil liberties.[294]

[288] There is an exception in cases where financial institutions, under the Right to Financial Privacy Act, may be relevant to a possible violation of any statute or regulation. Such information may include only the name or other identifying information concerning any individual, corporation, or account involved in and the nature of any suspected illegal activity. See 12 U.S.C. § 3403(c).
[289] s.702 of FISA authorisations are conducted on a more broad programme basis, rather than an individualised warrant or court order system.
[290] S.2(b) and (c)(i)(A) EO 14086.
[291] S.2(c)(i)(A) EO 14086.
[292] S.2(c)(i)(A) EO 14086; S.2.4 of EO 12333 requires that the intelligence community use the "*least intrusive collection techniques feasible*".
[293] S.2(c)(i)(B) EO 14086.
[294] S.2(c)(i)(B) EO 14086.

EO 14086 sets out a complementary set of overarching requirements that apply to all signals intelligence activities which have the effect of ensuring that signals intelligence activities are proportionate to the aim pursued:

Agencies must have appropriate safeguards in place to ensure that privacy and civil liberties are integral considerations in the planning of such activities.[295] EO 14086 also sets out that signals intelligence activities can only be carried out "*following a determination, based on a reasonable assessment of all relevant factors, that the activities are necessary to advance a validated intelligence priority*".[296]

Signals intelligence activities can only be conducted "*only to the extent and in a manner that is proportionate to the validated intelligence priority for which they have been authorised, with the aim of achieving a proper balance between the importance of the validated intelligence priority being advanced and the impact on the privacy and civil liberties of all persons, regardless of their nationality or wherever they might reside.*"[297]

Post acquisition use of data

Generally, an analyst has specific obligations to positively affirm, at regular intervals, that the justification for targeting remains valid and that the targeting standard is still met in respect of that collection. Once the targeting standard is no longer satisfied, collection must cease. The analyst's decision is reviewed within 60 days as part of a cyclical process with the DoJ and ODNI. If any issues are uncovered, then the collection is terminated and purged and reported to the court under FISA. The failure to provide a written justification constitutes a documentation compliance incident that must be reported to the FISC and Congress.[298]

DSIT also notes that the US has internal policies and procedures that include requirements for disclosure of information and affirm that all Intelligence Community personnel are required to carry out all their data processing activities in a manner consistent with applicable laws and with regard to safeguarding privacy and civil liberties.[299]

General procedural safeguards also exist under FISA in the form of mandatory minimisation procedures, which must be applied to acquisitions of data under s.702 FISA.

[295] S.2(a)(ii) EO 14086.
[296] S.2(a)(ii) EO 14086.
[297] S.2(a)(ii)(B) EO 14086.
[298] See Semi-annual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to s.702 of the FISA, Submitted by the AGI and the DNI, Reporting Period: December 1, 2016 – May 31, 2017, p. 41 (October 2018), DoJ/ODNI Compliance Report to FISC for Dec. 2016 – May 2017 at p. A-6, available at https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf. NSA targeting procedures, p. 8. See also PCLOB, s.702 Report, p 46.
[299] See Intelligence Community Directives 501 (https://www.dni.gov/files/documents/ICD/ICD_501.pdf) and 701 (https://www.dni.gov/files/documents/ICD/10-3-17_Atch1_ICD-701-Unauthorized-Disclosures_17-00047_U_SIGNED.pdf).

Alternative FISA bases

Under all bases information can only be used or disclosed for lawful purposes[300] and where information is disclosed for law enforcement purposes, neither the information or any information derived therefrom may be used in a criminal proceeding without prior authorisation of the AG.[301]

s.301 FISA also restricts and regulates the uses of information collected under a FISA physical search. In particular, federal officers and employees must comply with minimisation procedures if they use or disclose information gathered from a physical search under FISA concerning a US person.[302]

s.402 FISA sets additional limits on the use of information obtained through the use of a pen register or trap and trace device. In particular, federal officers and employees may only use or disclose such information with respect to a US person without the consent of that person in accordance with s.1845 requiring advance authorization of the AG and notice to the aggrieved person.[303]

National Security Letters

Information collected under NSL statutes are subject to specific dissemination requirements. In particular:

Right to Financial Privacy Act

Information can only be disseminated under AG approved guidelines and, with respect to dissemination to an US agency, only if such information is clearly relevant to the authorised responsibilities of such agency.[304]

FCRA (§1681u)

Limits dissemination to sharing within the FBI, or with other agencies to the extent necessary to secure "*approval or conduct of a foreign counterintelligence investigation*."[305]

ECPA

Limits dissemination information except under AG approved guidelines. In particular, with respect to dissemination to an US agency, only if such information is clearly relevant to the authorised responsibilities of such agency.[306]

[300] 50 U.S.C. § 1806(a), 50 U.S.C. § 1825(a), 50 U.S.C. § 1845(a)(2).
[301] 50 U.S.C. § 1806(b), 50 U.S.C. § 1825(c), 50 U.S.C. § 1845(b).
[302] 50 U.S.C. § 1825(a).
[303] 50 U.S.C. § 1845(a)(1).
[304] 12 See also, 18 U.S.C. 2709(d).
[305] 15 U.S.C. 1681u(g).
[306] 18 U.S.C. § 2709(e).

s.702 FISA

Limitations

The processing of personal data collected by the US through SIGINT is subject to further specific safeguards, in part set out in the specific targeting, minimisation and querying procedures authorised by the FISC.

Each agency must put in place policies and procedures designed to minimise the dissemination and retention of personal data collected through signals intelligence.[307]

EO 14086 sets out requirements that limit the processing of data to authorised personnel who have a need to know the information to perform their mission and have received appropriate training on the requirements of the relevant laws, policies and procedures. This requirement ensures that the processing of data is carried out in tightly controlled circumstances.

EO 14086 explicitly sets out that authorised USIC elements can only disseminate non-US persons' personal data if it contains one or more specific types of information set out under s.2.3 of EO 12333, that would also allow the personal data of US persons to be shared.

Retention

As a general rule, the USIC can retain personal information collected through SIGINT methods if it relates to an authorised intelligence requirement (as set out in the NIPF); be reasonably believed to be evidence of a crime; or meet one of the other standards for retention of US person information identified in EO 12333, s.2.3 (the standards for retention apply to signals intelligence). The DNI has a mechanism to monitor the collection and dissemination of SIGINT that is particularly sensitive because of the nature of the target or the means of collection, to ensure that it is consistent with the determinations of policymakers.

Where data is retained permanently, a specific reason must be provided, in line with wider priorities and considering the views of multiple levels of oversight, to ensure no decision is taken in isolation. EO 14086 requires[308] that non-US persons' data can only be retained if comparable information concerning US persons would be allowed under s.2.3 of EO 12333. As regards data retention, non-US persons' personal information collected through signals intelligence is subject to the same retention periods that would apply to comparable information concerning US persons in accordance with EO 14086. Generally, this establishes a maximum retention period of 5 years for personal information that is unevaluated. In certain circumstances, such unevaluated personal information may be kept for longer than five years, in particular where necessary to protect the national security of the US, or where necessary to protect against imminent threat to human life[309]. Unless reviewed and approved for longer retention, the data

[307] S.2(c)(iii)(A) EO 14086.

[308] S.2(c)(iii)(A)(2)(a)-(c) EO 14086. More generally, each agency must put in place policies and procedures designed to minimise the dissemination and retention of personal data collected through signals intelligence (S.2(c)(iii)(A) EO 14086).

[309] See, e.g. Section 309 of the Intelligence Authorization Act for Fiscal Year 2015, which covers non-public telephone or electronic communications acquired without the consent of a person who is a party to the communication, read in conjunction with S.2 (c)(iii)(A)(2) EO 14086, which clarifies that personal information of

must be deleted. Where no such determination has yet been made regarding retention and dissemination, such personal information can only be accessed in order to make such determinations (or conduct authorised administrative, testing, development, security, or oversight functions). The agencies have internal procedures and processes to ensure that these requirements are met. This access barrier helps to limit the use of personal information where there are still outstanding requirements to be placed upon its dissemination and retention and ensures appropriate oversight can still occur.

Accuracy and objectivity

Intelligence agencies must comply with Intelligence Community standards for accuracy and objectivity, in particular with respect to ensuring data quality and reliability, the consideration of alternative sources of information and objectivity in performing analysis.

Dissemination

Specific rules apply to the dissemination of collected data under s.702 FISA. Generally, personal data on non-US persons can only be disseminated if it contains the same type of information that could be disseminated about a US person.[310] Personal data may not be disseminated solely because of a person's nationality or country of residence or for the purpose of circumventing the requirements of EO 14086.[311] The permissible types of information that may be disseminated include where:[312]

- it is publicly available;
- it directly relates to an authorised foreign intelligence requirement;
- it is related to a crime that has been, is being or is about to be committed; or
- it indicates a possible threat to the safety of any person or organisation.

Dissemination within the US government may only take place if an authorised and trained individual has a reasonable belief that the recipient has a need to know the information and will protect it appropriately.[313] To determine whether personal data can be disseminated to recipients outside the US government (including a foreign government or international organisation), the purpose of the dissemination, the nature and extent of the data being disseminated, and the potential for harmful impact on the person(s) concerned must be taken into account.[314]

non-US persons is subject to the same retention periods as the ones that would apply to the information of US persons

[310] S.2(c)(iii)(A)(1)(a) and 5(d) EO 14086, in conjunction with S.2.3 EO 12333. S.2(c)(iii)(A)(1)(b) and (e)EO 14086.

[311] S.2(c)(iii)(A)(1)(b) and (e)EO 14086.

[312] NSA PPD-28 S.4 Procedures § 7.2. Similar restrictions apply under CIA and FBI procedures. These will be superseded by the new procedures under EO14086.

[313] S.2(c)(iii)(A)(1)(c) EO 14086.

[314] S.2(c)(iii)(A)(1)(d) EO 14086.

Requirements for Access

In the US system, information collected must then be "*queried*" by a trained analyst. Access to data must be limited to authorised and appropriately trained personnel, with a definite need to know the information in order to carry out their mission.[315]

Each intelligence agency is required to implement controls and procedures that ensure appropriate data security and limit access to just authorised people. The minimum information security requirements for these controls and procedures are contained in statute, guidelines and relevant standards.[316] In particular:

- Title VIII of the Counterintelligence and Security Enhancement Act of 1994, which is incorporated into the National Security Act in 50 U.S.C. §§ 3161-3164, directs the establishment of procedures for access to classified material in adherence to certain minimum standards and in accordance with interests of due process. These procedures are reflected in EO 13526, which sets out the requirements for access to classified information and in further implementation directives, guidelines, and procedures;
- S.1.5 EO 12333 requires the Director of National Intelligence to ensure the establishment by the Intelligence Community of common security and access standards for managing and handling foreign intelligence systems, information, and products;[317]
- National Security Directive 42, "*National Policy for the Security of National Security Telecommunications and Information Systems*" directs the Committee on National Security Systems to provide system security guidance for national security systems to executive departments and agencies); and
- National Security Memorandum 8, "*Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*" establishes timelines and guidance for how cybersecurity requirements will be implemented for national security systems, including multi factor authentication, encryption, cloud technologies, and endpoint detection services.

The agencies are required to ensure that their employees are appropriately trained, including on how to identify, report and address violations of relevant law, which will include EO 14086.[318]

Deletion requirements

The Minimisations procedures mandate that the intelligence agencies are required to destroy communications that are not to, from, or about the specified target.[319] Age off requirements specify that data must be deleted after it exceeds its specific retention period.[320]

[315] S.2(c)(iii)(B)(2) EO 14086.
[316] S.2(c)(iii)(B)(1) EO 14086.
[317] S.1(5)(g) EO 12333.
[318] S.2(d)(ii) EO 14086.
[319] Exceptions to this requirement apply for administrative purposes (e.g. to effect compliance) and substantive purposes (e.g. the information contains significant foreign intelligence information). These exceptions appear in each agency's minimisation procedures.
[320] See https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards-in-executive-order-14086

Under the new redress mechanism, as set out below, the ODNI CLPO and the new Data Protection Review Court ("DPRC") can order the relevant USIC agency to delete data that has been acquired without lawful authorisation, or to delete the results of inappropriately conducted queries of otherwise lawfully collected data.

As set out elsewhere in this document, the ODNI CLPO, the DPRC and the FISC all have the power to order the erasure of personal data held by public authorities.

Generally, DSIT considers that the protections set out above ensure that there are multiple requirements and safeguards in place for the protection of UK personal data if it is collected.

They also ensure that data held by US government agencies is handled in a transparent way, aligning with the OECD TGA principles.[321]

Any particular categories of personal data treated differently

The US has confirmed that the classified procedures under which the agencies operate contain restrictions on the use and collection of specific categories of data, including legally privileged information. These include requirements to provide increased protections to some categories and types of data, and the FISC has been involved in cases where it has instructed the NSA and other agencies in how to properly treat certain types of data demonstrating an active consideration of the need to properly protect sensitive data.[322]

Alternative FISA bases and NSLs

FISA Title I, Subchapter I, S.106 sets out specifically that communications which are considered to be privileged information (ie. legally privileged information) when intercepted remain privileged when stored.[323] Otherwise, internal procedures govern the protection of particularly sensitive information.

There are also specific rules set out in the Federal Criminal Procedure Rules that provide additional protection for privileged communications.[324]

S.702 FISA

EO 14086 sets out that, in deciding to undertake SIGINT activity, the balancing exercise must include "*the nature and sensitivity of the data to be collected*".[325] This includes a consideration of the type of data and its source.

[321] OECD TGA, Article IV Data Handling.

[322] Additionally, other laws provide further protections to certain types of sensitive and privileged information, such as the Federal Criminal Procedure Rules which protect privileged communications (2 Wright, Federal Practice and Procedure §275 (Crim. 3d ed. 2000).

[323] 50 U.S.C. § 1806 (a).

[324] 2 Wright, Federal Practice and Procedure §275 (Crim. 3d ed. 2000).

[325] S.2(c)(i)(B) EO 14086.

Conclusion

DSIT is satisfied that the information received from the US on these points ensures that data of a more sensitive nature will be safeguarded appropriately. DSIT is further reassured that, as set out above, there are legislative and procedural requirements that provide a basis for these protections and safeguards.

Available routes for redress

The US provides data subjects (including UK data subjects) with a number of routes to bring a claim in order to challenge US government access to data in front of an independent and impartial tribunal, with binding powers. Depending on the nature of the claim brought, there are avenues for claimants to have the lawfulness of government access reviewed, to access their personal data and, in the case where a violation has occurred, have the relevant violation remedied through rectification or erasure of the relevant data. These avenues include:

Data subjects' ability to exercise their data protection rights under a variety of pieces of legislation in front of a court established under Article III of the US Constitution.

The FISA statute includes a civil course of action for monetary damages (including litigation costs) against the US when information about them obtained in electronic surveillance under FISA has been unlawfully and wilfully used or disclosed. A data subject can challenge the legality of surveillance (and seek to suppress the information) in the event the US government intends to use or disclose any information obtained or derived from electronic surveillance against the individual in judicial or administrative proceedings in the US.[326] FISA also provides criminal penalties for individuals who intentionally engage in unlawful electronic surveillance under the pretext of law or who intentionally use or disclose information obtained by unlawful surveillance.

There are several further avenues to seek legal recourse against government officials for unlawful government access to, or use of, personal data, including for purported national security purposes (i.e., the Computer Fraud and Abuse Act; Electronic Communications Privacy Act; and Right to Financial Privacy Act).[327] [328] [329] All of these legal actions concern specific data, targets and/or types of access (e.g. remote access of a computer via the internet) and are available under certain conditions (e.g. intentional/wilful conduct, conduct outside of official capacity, harm suffered).

The recipient of a NSL (e.g. the organisation or institution who holds the data or information requested in relation to an authorised national security investigation) has the right to challenge in US District Court an NSL for which the recipient believes compliance would be either "*unreasonable, oppressive, or otherwise*." The recipient may also challenge in US District Court any applicable nondisclosure provisions. As a default, the NSLs themselves are not classified,

[326] 50 U.S.C. § 1806.
[327] 18 U.S.C. § 1030.
[328] 18 U.S.C. §§ 2701-2712.
[329] 12 U.S.C. § 3417.

nor is the material received in return from NSLs classified,[330] though the requesting agency can seek a non-disclosure order alongside the NSL in specified circumstances.[331] The non-disclosure orders prohibit recipients from disclosing that the government authority has sought or obtained access to the relevant information.[332] The recipient can challenge the non-disclosure order and also disclose it to a lawyer to seek legal advice or assistance. Both NSL requests and accompanying non-disclosure requirements can be judicially reviewed, and the NSL itself must advise the recipient of this right.[333] Whilst the US District Court will take into account the position of the public authority, there are examples of where the court's rulings have criticised the actions of the FBI, leading to change being enacted.[334]

The US also provides other means of redress for non-USPs under the Judicial Redress Act for those claims that meet the requirement of that statute. The Privacy Act of 1974[335] allows both US and non-US persons (by virtue of the Judicial Redress Act of 2015)[336] to sue a US federal agency for the improper handling of covered records; to obtain injunctions or monetary damages; and to review, copy, and request amendments to their records. The Judicial Redress Act of 2015 allows for citizens of a covered country to bring a claim against an agency for the wilful or intentional disclosure of covered records in violation of the Privacy Act, or when a designated US governmental agency or component declines to amend an individual's record in response to an individual request.

All these routes are available, subject to the individual being able to establish standing to bring a claim. To establish standing, a claimant must include factual allegations that demonstrate that they either have suffered some actual injury that can fairly be traced to the challenged action of the defendant, and that the injury is likely to be remedied by a favourable decision.[337] This can be complicated in respect of privacy violations, as it can be difficult to establish a concrete and particularised injury, with proof or actual or imminent harm, without knowledge that surveillance has in fact occurred. A speculative claim that an "*injury*" could occur, or that an individual may be (or may have been) the subject of surveillance, is insufficient. The difficulty of establishing an injury in fact is compounded by non-disclosure provisions in FISA. The recipients of requests under FISA cannot reveal the existence of the request, particularly to the target. However, the

[330] See commentary on page 19 - 20 for congressional consideration of this here: https://crsreports.congress.gov/product/pdf/RL/RL33320

[331] These cover cases where the disclosure of the request or response might result in a danger to national security; might interfere with diplomatic relations or with a criminal, counterterrorism, or counterintelligence investigation; or might endanger the physical safety of an individual. See 18 U.S.C. 2709(c)(1); 12 U.S.C. 3414(c)(1); 15 U.S.C. 1681u(d)(1); 15 U.S.C. 1681v(c)(1); 50 U.S.C. 3162(b)(1); 18 U.S.C. 3511(b)(3).

[332] 12 U.S.C. § 3414 (3). Non compliance with a non disclosure order is punishable as contempt of court, and if committed knowingly and with the intent to obstruct an investigation or related judicial proceedings is punishable by imprisonment for not more than five years and/or a fine of not more than $250,000 (not more than $500,000 for an organisation).

[333] 18 U.S.C. 2709 (d).

[334] DSIT notes that, whilst there are examples of successful challenges of the non-disclosure provisions where the court has published the relevant information. In both cases, the judges ruled that the non disclosure orders were unconstitutional.

[335] As amended, 5 U.S.C. § 552a.

[336] This right was extended to non-US persons under the Judicial Redress Act.

[337] This standard is derived from US case law and applies to all cases (regardless of nationality), stems from the 'case or controversy' requirement under Article 3 of the US Constitution.

US has taken action to ensure that individuals still have a route to redress in relation to signals intelligence activities, as set out in the 'Available Routes for Redress' section below.

In general however, for all intelligence collected against individuals, if evidence has been obtained illegally it is not admissible and may not be used in a US criminal proceeding.[338] Therefore, if procedural formalities set out by FISA were not followed, the surveillance evidence obtained would not be admissible. The US government is required to notify the court when such evidence is being used. Where such evidence is used, the defendant would have the ability to challenge its collection. This is applicable for any disclosures in judicial proceedings against individuals where information has been collected under FISA,[339] with similar requirements where NSLs are concerned.

In cases where disclosure would cause harm to national security, the US government is able to invoke ''*state secrets privilege*" which permits the government in a lawsuit to block the release of information that it would otherwise be legally required to disclose.[340] [341] Application of this privilege can require the court to dismiss the claim because there is no feasible way to litigate the matter without unjustifiably risking the disclosure of state secrets. However, the state secrets privilege cannot be invoked by the government and will not be applied by the new DPRC set up under the DPF as a way to remedy these kinds of claims and challenges.

Additionally, any data subject can seek access to existing federal records in US government systems under the Freedom of Information Act of 1967, as amended ("FOIA") that are retrievable by a personal identifier, and this includes records that contain the individual's personal data.[342] A data subject could use this route to establish whether an agency held data on the individual, thereby allowing them to bring a claim under the above routes, and would assist with them establishing standing for that claim. As in the UK, the US government is able to withhold information for a number of exemptions, including access to classified national security information and information concerning law enforcement investigations.[343] Where a claimant is dissatisfied with the response received, they are able to challenge it through administrative then judicial review, with cases heard by the US judicial system.

---

[338] The Exclusionary Rule under the US legal system is based on the fourth amendment to the US Constitution that is intended to protect citizens from illegal searches and seizures.

[339] Notice must be given to the aggrieved person, defined as *"a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance.*" and as well as the court or other authority involved. See 50 U.S.C. § 1801(k) and 50 U.S.C. § 1806(c).

[340] *United States v. Reynolds, 345 U.S. 1, 6-7 (1953)* - A state secrets privilege may be invoked by the government where it is shown, "*from all the circumstances of the case, that there is a reasonable danger that compulsion of the evidence will expose . . . matters which, in the interest of national security, should not be divulged.*"

[341] This privilege belongs to the government, is constitutionally-based, and cannot be abrogated by the Congress or the courts. A President can not impose a limitation on exercise of the privilege that would be binding on future Presidents.

[342] 5 U.S.C. § 552.

[343] If this is the case, the individual will normally only receive a standard reply by which the agency declines either to confirm or deny the existence of any records. See *ACLU v. CIA, 710 F.3d 422 (D.C. Cir. 2014)*. Additionally, FOIA (5 U.S.C. §552(b)(3)(A)(i) allows for disclosures to be exempted where statute "*requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue*" which can support the Neither Confirm Nor Deny response.

Where complaints are brought under one of the statutory routes set out above, they will be brought in front of an Article III court. An Article III court is established under Article III of the US Constitution and normal appeal routes can be followed.[344] [345]

The decisions made by the Article III courts in relation to the lawfulness of surveillance can be appealed to the US Courts of Appeals and the US Supreme Court, using normal court procedures. In this way, the decision of the FISC in deciding to grant the warrant can be challenged if the government introduces FISA information as evidence in a criminal proceeding before an Article III court. The issues of standing do not matter here, as the defendant will have been accused of a crime, so there is a "*case and controversy*" to establish standing.

Any determinations of the FISC can be appealed to the Foreign Intelligence Surveillance Court of Review ("FISCR").[346] The FISCR is made up of judges appointed by the Chief Justice of the US and drawn from US district courts or courts of appeals, serving for a staggered seven-year term.[347] Ultimately, their decisions can be appealed to the US Supreme Court.

New redress mechanism under EO 14086

In addition to the above routes, the US has established a new redress mechanism under EO 14086 and in line with the requirements of the AG Regulation. This includes an initial investigation by the ODNI CLPO, and a second stage where individuals can request to have the outcome of this investigation reviewed by the DPRC. The DPRC is empowered to hear complaints concerning alleged violations of EO 14086, s.702 FISA,[348] EO 12333 and relevant subsequent legislation that adversely affects their privacy and/or civil liberties.[349] Any individual who reasonably believes that they have had their personal data transferred from the UK to the US, and that they may have been subject to a violation in relation to SIGINT activities, is able to submit a complaint to this redress mechanism through the ICO.

---

[344] Article III (https://www.archives.gov/founding-docs/constitution-transcript#3) sets out that "*The judicial Power of the United States, shall be vested in one supreme Court, and in such inferior Courts as the Congress may from time to time ordain and establish. The Judges, both of the supreme and inferior Courts, shall hold their Offices during good Behaviour, and shall, at stated Times, receive for their Services, a Compensation, which shall not be diminished during their Continuance in Office*".

[345] The federal judiciary operates separately from the executive and legislative branches, but often works with them as the Constitution requires. Federal laws are passed by Congress and signed by the President. The judicial branch decides the constitutionality of federal laws and resolves other disputes about federal laws. Article III of the Constitution governs the appointment, tenure, and payment of Supreme Court justices, and federal circuit and district judges. These judges, often referred to as "Article III judges," are nominated by the president and confirmed by the US Senate. Article III states that these judges *"hold their office during good behavior*," which means they have a lifetime appointment, except under very limited circumstances. Article III judges can be removed from office only through impeachment by the House of Representatives and conviction by the Senate. Article III judgeships are created by legislation enacted by Congress. The Constitution also provides that judges' salaries cannot be reduced while they are in office. Article III judicial salaries are not affected by geography or length of tenure.

[346] 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

[347] 50 U.S.C. § 1803 (b).

[348] The new redress mechanism is not applicable to other methods of surveillance under alternative FISA bases or NSLs.

[349] Attorney General Regulations - PART 201 - DATA PROTECTION REVIEW COURT; Authority: 5 U.S.C. 301; 28 U.S.C. 509, 510-512.

The signals intelligence redress mechanism is available to individuals who believe their data was transferred to the US from countries or regional economic integration organisations that have been designated by the US AG as "*qualifying states*" (s.3(f) EO 14086). In accordance with EO 14086, the US AG will designate the UK as a "*qualifying state*" upon satisfactory completion of their own assessment of the UK.

The US AG Regulations contain the process for the establishment of the new redress mechanism.[350] Under the US legal system, an agency-issued regulation has the binding force of law, making it a suitable vehicle for defining the procedures for the review of redress requests and complaints.[351] The DoJ regularly issues such regulations under existing statutory authorities and pursuant to established and public procedures.[352]

The first investigation of a qualifying complaint[353] is carried out by the ODNI CLPO[354]. The ODNI CLPO has demonstrated its effectiveness in conducting oversight and ensuring compliance. They will receive a qualifying complaint transmitted from the ICO, as the relevant data protection authority in the UK.[355] A qualifying complaint must be made in writing and relate to a natural, not legal, person. The ICO will verify the identity of the complainant and that the complaint:

- Alleges a covered violation has occurred that relates to personal information of, or about, the complainant that is reasonably believed[356] to have been transferred to the US from the UK;
- Includes basic information to enable a review (including any information that forms the basis for the allegation and the nature of relief sought);
- Is not frivolous, vexatious, or made in bad faith; and
- Has been brought on behalf of the complainant, acting on their own behalf. It cannot be brought by a representative of a governmental, nongovernmental, or intergovernmental organisation.[357]

The ODNI CLPO's remit has been strengthened under EO 14086 to safeguard their ability to carry out their role in investigating complaints.[358] The ODNI CLPO is required to investigate, review and, as necessary, order appropriate remediation for qualifying complaints following the

[350] The AG delegates to the DPRC their powers to review an appealed UK complaint, while structuring the Tribunals to maximise its independence. The US Supreme Court has recognised the ability of the AGI to establish independent, decision making bodies.

[351] See *United States v. Nixon.*

[352] See *United States ex rel. Accardi v. Shaughnessy*, *347 U.S. 260 (1954)* and *United States v. Nixon*, *418 U.S. 683, 695 (1974)*.

[353] The definition of a "*qualifying complaint*" is set out in S.4(k) EO 14086.

[354] Supporting document available from Director of National Intelligence: https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf

[355] S.4(k) EO 14086.

[356] The claimant need not demonstrate that their data has been accessed as a matter of fact under applicable US law. The US has confirmed that it will not take an absolute view as to what is "*reasonable*": both in terms of the means of transfer (e.g. if the DPF was named, but it, as a matter of fact, transferred under SCCs) or in relation to the route taken by the data.

[357] S.4(k)(iv) EO 14086.

[358] S.3(c)(iv) EO 14086. See also National Security Act 1947, 50 U.S.C. §403-3d, S.103D concerning the role of the CLPO within the ODNI.

process set out in EO 14086.[359] When conducting their review, the ODNI CLPO has access to all documents and information needed for their assessment, and can rely on the compelled assistance of CLPOs in the different intelligence agencies. [360]When applying the law, the ODNI CLPO is under a duty to apply the law *"impartially*," with regard given to both the national security interests in signals intelligence activities and privacy protections.[361]

In concluding their review, the ODNI CLPO will determine whether a covered violation has occurred and direct appropriate remediation.[362] The directions made by the ODNI CLPO are binding on the Intelligence Community. When reaching a decision, the ODNI CLPO is required to keep a written record of their decision, and produce a classified decision that sets out the basis for their factual findings, determination with respect to whether a covered violation occurred, and determination of the appropriate remediation.[363] In cases where they have identified a violation that is subject to the oversight of the FISC, the ODNI is required to submit a classified report to the Assistant AG for National Security who can take further enforcement action, under their obligation to report non-compliance to the FISC.[364]

Upon completion of their review, the ODNI CLPO will inform the complainant, through the ICO, that the "*the review either did not identify any covered violations or the CLPO of the ODNI issued a determination requiring appropriate remediation*".[365] It will also set out the right of the complainant to apply for review of the ODNI CLPO's decision by the DPRC and, if they chose to do so, a special advocate will be selected by the DPRC to advocate regarding the complainant's interest in the matter. The receipt of a "*neither confirm nor deny*" ("NCND") response from the ODNI CLPO does mean that the complainant will not know what remedy, if any, has been awarded. However, DSIT does not consider that this unduly prejudices the complainant's ability to seek effective redress as they are able to bring a claim to the DPRC, where additional safeguards, including through a special advocate to represent the complainant's interest, are in place.

An application for review of the ODNI CLPO's decision can be submitted to the DPRC by either the complainant or the relevant element of the USIC. The application for review must be submitted (via the ICO) within 60 days of the public authority receiving the notification from the ODNI CLPO that their review is complete and include any information that the complainant wishes to provide to the DPRC. This includes arguments on questions of law, or the application of the facts of the case.[366] As the data subject will not necessarily know whether or not they have been subject to surveillance, this allows them to set out any evidence or information that they wish the DPRC to take into account, in order to ensure as much of an adversarial process as possible within the confines of the need to protect national security.

[359] S.3(c)(i) EO 14086.
[360] S.3(c)(iii) EO 14086.
[361] S.3(c)(i)(B)(i) and (iii) EO 14086.
[362] S.3(c)(i) EO 14086.
[363] S.3(c)(i)(F)-(G) EO 14086
[364] S.3(c)(i)(D) EO 14086.
[365] S.3(c)(i)(E)(1) EO 14086.
[366] S.201(6)(a)-(b) AG Regulation.

Judges who sit on the DPRC, as set out below, are required to maintain materially the same standards as judges in an Article III court, to ensure that they operate independently and impartially. The DPRC consists of at least 6 judges, who are appointed by the AG in consultation with the PCLOB, Secretary of Commerce and the DNI for renewable four-year terms.[367] Every judge who sits on the DPRC must be a legal practitioner with specific expertise in privacy and national security law. The selection of judges is informed by the criteria used in assessing candidates for the federal judiciary, giving weight to any prior judicial experience, and they are required to act in compliance with the US Code ("U.S.C") for Judges[368] [369]. The AG must endeavour to ensure that at least half of the judges at any given time have prior judicial experience. In order to ensure that the DPRC is able to fully hear and investigate all complaints, all judges must hold security clearances that enable them to access classified national security information[370].

To guarantee the ability of the judges to act independently and impartially, only individuals who meet the above requirements, and who are not employees of the executive branch at the time of their appointment, or in the preceding two years, can be appointed to the DPRC. During their term of office at the DPRC, the judges may not have any official duties or employment within the US government (other than as judges at the DPRC).[371] [372]

The DPRC judges have specific employment protections to avoid interference. DPRC judges are not subject to the day-to-day supervision of the AG[373] and may only be dismissed by the AG for cause (i.e., misconduct, malfeasance, breach of security, neglect of duty or incapacity), after taking due account of the standards applicable to federal judges laid down in the Rules for Judicial-Conduct and Judicial-Disability Proceedings.[374] Just as the regulation narrows the AG's discretion to assess complaints, so do the appointment and removal provisions narrow their otherwise greater discretion to hire and fire.

Complaints are heard by a panel of three judges.[375] The panel will also be assisted by a Special Advocate selected by the presiding judge,[376] whose role it is to ensure that the interests of the complainant are represented, and that the DPRC panel is well informed about all relevant issues

[367] S.201(3)(b) AG Regulation.
[368] S.201(3)(b) AG Regulation.
[369] S.3(d)(i)(B) EO 14086.
[370] S.3(d)(i)(B) EO 14086.
[371] S.3(d)(i)(A) EO 14086 and S.201(3)(a) and (c) AG Regulation.
[372] An exception exists to allow the judges to participate in extrajudicial activities, including business, financial activities, non-profit fundraising and fiduciary activities, as well as the practice of law, as long as such activities do not interfere with the impartial performance of their duties or the effectiveness or independence of the DPRC. See S.201(7)(c) AG Regulation.
[373] S. 201(7) AG Regulation.
[374] S.3(d)(iv) EO 14086 and S.201(7)(d) AG Regulation.
[375] In carrying out their functions, the DPRC and special advocate is supported by the Office of Privacy and Civil Liberties of the Department of Justice (OPCL). S.201(5) AG Regulation. It is their role to select the three person panel on a revolving basis, with the general aim that each panel has at least one judge with prior judicial experience. If no panel member has prior judicial experience, then the presiding judge will be the first judge selected by the OPCL.
[376] For each review of an application, the presiding judge selects a Special Advocate to assist the panel. See S.201(8)(a) AG Regulation.

of law and fact.[377] This is to ensure that the DPRC is able to properly investigate the complaint and engage in an adversarial process without compromising national security concerns. The complainant and the Special Advocate do not have an attorney-client relationship, nor do they act as the agent of the complainant. They will have access to all information that relates to the case, including classified information.[378] In order to ensure that the Special Advocate is properly informed, they are able to ask for further information from the complainant through written questions. The questions are reviewed by the Office of Privacy and Civil Liberties ("OPCL"), in consultation with the relevant USIC agency, to identify and then exclude any classified, privileged, or protected information before forwarding it to the complainant for response. Any additional information received by the Special Advocate will then form part of their submissions to the DPRC.

The Special Advocates are appointed by the AG, in consultation with the Secretary of Commerce, the DNI, and the PCLOB, for a two-year renewable term. There will be at least two Special Advocates, who are required to have appropriate experience in the field of privacy and national security law, be experienced attorneys, active members in good standing of the bar and duly licensed to practice law. The Special Advocates, at the time of their initial appointment, must not have been employees of the executive branch for the preceding two years to avoid conflicts of interest. For each review of an application, the presiding judge selects a Special Advocate to assist the panel.[379]

The inclusion of the Special Advocate is key to ensuring that the redress is effective for the claimant. Their role ensures that the process is adversarial, ensuring that the interests of the claimant are property represented. The Special Advocate will have obtained relevant information from the complainant and will be able to advocate for them. Crucially, the Special Advocate ensures proper and detailed investigation prior to the provision of a NCND response, and ensures that the DPRC is interrogating the ODNI CLPO's determination.

The DPRC will review the determination (reasoning and outcome) made by the ODNI CLPO. At a minimum, their review will be based on the documentation maintained by the ODNI CLPO during their investigation, as well as any information and/or submissions provided by the complainant, the Special Advocate or an intelligence agency.[380] The DPRC panel has access to all the information that it needs to conduct its review and the DPRC judges must "*hold the requisite security clearances to access classified national security information*." In the case that the DPRC panel needs to supplement its review, the DPRC can obtain further information or factual findings through the OPCL.[381] Under EO 14086, each element of the intelligence community *"shall provide access to information necessary to conduct the review […] that a Data Protection Review Court panel requests*." EO 14086 also sets out that the AG and intelligence

[377] S.3(d)(i)(C) EO 14086 and S.201(8)(e) AG Regulation.
[378] S.201(8)(c) and 201(11) AG Regulation.
[379] S.201(9) AG Regulation.
[380] S.3(d)(i)(D) EO 14086.
[381] S.3(d)(iii) EO 14086 and S.201(9)(b) AG Regulation.

agencies are prohibited from interfering or improperly influencing the DPRC's review of the ODNI CLPO's decision.[382]

After concluding its review, the DPRC will determine either:

- that there is no evidence in the record indicating that signals intelligence activities occurred involving personal information of or about the complainant;
- that the ODNI CLPO's determination as to whether a covered violation occurred was legally correct, supported by substantial evidence, and the determination of a remedy was consistent with EO 14086;
- that the ODNI CLPO's determination as to whether a covered violation occurred was legally correct, supported by substantial evidence, and the determination of a remedy, was inconsistent with EO 14086. If so, the DPRC panel shall issue its own determination;[383] or
- that the ODNI CLPO determination was legally incorrect and issue its own recommendation.

The DPRC will adopt its decision by a majority vote, which will be binding in respect of the complaint under consideration.[384] In addition, if the review reveals a violation of any authority subject to the oversight of the FISC, the DPRC must also provide a classified report to the Assistant AG for National Security, who in turn is under an obligation to report the non-compliance to the FISC, which can take further enforcement action to remedy systemic defects.[385]

The DPRC will then transmit their decision to the ODNI CLPO.[386] The complainant will be notified through the ICO that the DPRC completed its review, and that "*the review either did not identify any covered violations or the DPRC issued a determination requiring appropriate remediation*."[387] The determination of the DPRC will be full and final, and binding on the agencies. The US has confirmed that the remedies ordered by the ODNI CLPO and/or the DPRC will be enacted, and that this will be subject to the oversight of PCLOB.

DSIT has considered whether the provision of a "NCND" response is consistent with effective redress for the complainant and assesses that it is consistent. While the complainant will not know whether redress has been ordered or in what form, there is a valid reason for this: the US has determined that it cannot provide this information without potentially jeopardising its national security arrangements. The DPRC mechanism operates on the basis of an investigation of the specific facts of each case, rather than any assumed facts, so a more specific response could not be issued without indicating whether or not surveillance has occurred, with implications for

[382] S.3(d)(iii)-(iv) EO 14086 and S.201(7)(d) AG Regulation.

[383] S.3(d)(i)(E) EO 14086 and S.201(9)(c)-(e) AG Regulation.

[384] S.3(d)(ii) EO 14086 and S.201(9)(g) AG Regulation. The DPRC is required to adjudicate complaints impartially and is bound by its published rules of procedure, which are adopted by majority vote. Se.3(d)(i)(D) EO 14086 and S.201(9) AG Regulation. These will be published online once fully agreed by the panel. S.3(d)(i)(F) EO 14086 and S.201(9)(i) AG Regulation.

[385] S.3(d)(i)(F) EO 14086 and S.201(9)(i) AG Regulation.

[386] S.201(9)(h) AG Regulation.

[387] S.3(d)(i)(H) EO 14086 and S.201(9)(h) AG Regulation.

the secrecy and effectiveness of the surveillance system and US national security. As a general principle, it has been recognised that the remedy available for a violation of privacy rights may be limited in the context of a surveillance system without negating the existence of effective redress, given the need for secrecy,[388] and DSIT considers that this is such a situation - particularly taking into account the wide margin of appreciation which states should be given in assessing what is needed to protect themselves from national security threats. DSIT notes that this practice is consistent with the UK's IPT and with the OECD Trusted Government Access principles (pt. VII).

Goal of the new redress mechanism

The new redress mechanism is empowered to adopt "*appropriate remediation*".[389] EO 14086 sets out a non-exhaustive list of remedial actions that can be ordered: all are designed to fully redress the "*identified covered violation regarding a specific complainant and limited to measures designed to address that specific complainant's complaint, taking into account the ways that a violation of the kind identified have customarily been addressed*".[390] The remedial action ordered could therefore include an order to rectify incorrect information, or to erase information.

The DPRC will not have the power to award monetary compensation for any breaches, nor will the redress mechanism permit the complainant to access data that is held about them. DSIT considers that this is understandable - awarding such remedies would indicate that the individual had been subject to surveillance, which might jeopardise US national security interests. Given the circumstances, DSIT does not consider that this precludes the DPRC from providing effective redress, given that the DPRC is able to order other remediation in relation to any violations found, including erasure or rectification of personal data.

Publication of decisions

In terms of the requirement for a public hearing, both civil and criminal pretrial proceedings and trials are presumptively open to the public under the Sixth Amendment to the US Constitution.[391] There are two caveats to this. First, in some circumstances, any court may determine that certain information must be kept private and will close part of the proceedings or trial (however, the

[388] For example, in *Klass v. Germany (1978)* 2 EHRR 214, paragraph 69: "*an "effective remedy" under Article 13 (art. 13) must mean a remedy that is as effective as can be having regard to the restricted scope for recourse inherent in any system of secret surveillance*".

[389] The description of appropriate remediation includes: curing through administrative measures violations found to have been procedural or technical errors relating to otherwise lawful access to or handling of data, terminating acquisition of data where collection is not lawfully authorised, deleting data that had been acquired without lawful authorization, deleting the results of inappropriately conducted queries of otherwise lawfully collected data, restricting access to lawfully collected data to those appropriately trained, or recalling intelligence reports containing data acquired without lawful authorization or that were otherwise disseminated in a manner inconsistent with United States law. See S.4(a) EO 14086.

[390] S.4(a) EO 14086, including addressing procedural issues through administrative means, terminating collection of or deleting already collected data where it was collected without lawful authorisation.

[391] The public and the press have a qualified First Amendment right of access to court proceedings and records. Although the First Amendment does not explicitly mention the right of access, the Supreme Court has held that the right to attend criminal proceedings is implicit in freedom of speech and serves an important function in a democratic society by enhancing trial fairness and its appearance.

closure must not be broader than necessary, and in practice DSIT understands that this is interpreted strictly). Secondly, given the subject matter of its work, FISC proceedings are held in secret and decisions are classified. However, as noted above, the DNI is required to declassify and publish significant decisions of the FISC.

In relation to the determinations of the DPRC, the OPCL maintains a record of all information reviewed by the DPRC and all decisions issued, which is made available for consideration as non-binding precedent for future DPRC panels.[392] The DoC is also required to maintain a classified record of each complainant who submitted a complaint.[393] In order to aid transparency about the system, at least once every five years, the DoC is required to contact the relevant agencies to confirm whether the information pertaining to a DPRC review has been declassified.[394] If it has, then the complainant will be notified that the information may be available to them under applicable law: in this case, this relates to the FOIA under which the complainant may request access.

In addition, PCLOB will also have access to all relevant information needed in order to conduct their review into the functioning of the new redress mechanism established under EO 14086.

Conclusion

Based on the information contained herein, DSIT assesses that the totality of the routes of redress available to UK data subjects whose personal data could be accessed by public authorities if transferred to certified US organisations under the DPF are sufficiently robust. DSIT considers there to be sufficient rights of redress for UK data subjects in relation to the potential unlawful collection of personal data by public authorities. In particular, the new redress mechanism available under EO 14086, which has been explicitly made available to UK data subjects by the US through designation of the UK as a qualifying state, provides a meaningful route for redress.

The US approach to redress is also consistent with the OECD TGA principles for which an underlying principle is effective judicial and non-judicial redress to identify and remedy violations of the national legal framework (whilst taking into account the need to preserve confidentiality of national security and law enforcement activities).[395]

Oversight and enforcement

The use of investigatory powers by the USIC is subject to a comprehensive regime of overlapping oversight mechanisms at executive, legislative and judicial level. It ensures that agencies are accountable for both their administration and expenditure, and the legality and propriety of their activities. The US system is made up of different, complementary layers of oversight, which means that there is no single body with an overarching power to identify or remedy violations of applicable US law. Supported by statutory and voluntary reporting and

[392] S.201(9)(j) AG Regulation.
[393] S.3(d)(v)(A) EO 14086.
[394] S.3(d)(v) EO 14086.
[395] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

accountability requirements, the US oversight system ensures a robust and in-depth assessment of the day-to-day and overarching use of the powers available to the US government when accessing data. None of the mechanisms can be looked at in isolation: it is precisely the multiple layers and reporting requirements that ensure robust supervision and oversight.

Bodies with responsibility for supervision and oversight

Judicial oversight

The FISC plays a central role in the oversight of foreign intelligence collection by the US government. It was established under FISA and sits in the judicial branch (as per Article III of the US Constitution), meaning that it is formally independent from the executive and legislative branches of government. The Chief Justice of the US Supreme Court selects the individuals who will serve on the FISC for a seven-year term from among federal district court judges.[396] To ensure their independence, federal judges have life tenure and salary protection, with removal only through impeachment by Congress. The judges are supported by a standing panel *amici curiae* comprised of five attorneys and technical experts that have expertise in national security matters as well as civil liberties.[397] This Constitutional structure guarantees the independence of the FISC and the judges that serve on it.

As Article III judges, the FISC judges are able to exercise their powers as they would in any other court. To ensure that they are able to provide proper oversight whilst maintaining necessary secrecy, the FISC has the power to gather all the information that it needs to carry out its investigations, including full access to classified information, and it enjoys "*the inherent authority of a court [...] to determine or enforce compliance*" with rules and procedures.[398] [399]

To aid their deliberations, the FISC is explicitly authorised to appoint an outside lawyer as an independent advocate (an *amicus curiae*) on behalf of privacy in cases that, in the opinion of the FISC, present novel or significant legal issues.[400] The court also has the power to appoint an amicus "*to provide technical expertise, in any instance as such court deems appropriate or, upon motion, permit an individual or organisation leave to file an amicus brief*."[401] These lawyers are authorised to make legal arguments that advance the protection of individual privacy and civil liberties, and will have access to any information, including classified information, that the court determines is necessary to their duties. In particular, this ensures that privacy and civil liberties are taken into account and given due prominence in the court's assessments.

The FISC has a number of roles in the oversight of the USIC:

- Granting orders or other authorisations under the alternative basis for access under FISA;

[396] These judges are nominated by the President and then approved by the Senate. They are drawn from at least seven different U.S. judicial circuits - 50 U.S.C. § 1803(a).
[397] 50 U.S.C. § 1803 (i)(1),(3)(A).
[398] 50 U.S.C. §1803 (h).
[399] https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf
[400] The FISC can also find that such an appointment is not appropriate. See 50 U.S.C. § 1803 (i)(2)(A).
[401] FISA Act of 1978 s.103 (i)(2)(B).

- Exclusive jurisdiction under FISA to issue orders for all foreign intelligence surveillance carried out in the US. This includes orders for individual surveillance (such as under alternative FISA bases), as well as prior programmatic approval and subsequent oversight of larger intelligence programmes (such as through s.702 FISA). The record of proceedings before the FISC, including the docket, applications and orders, is by statute "*maintained under security measures established by the Chief Justice in consultation with the Attorney General and the Director of National Intelligence*". These security measures have been made public.[402]
- Compliance officers in US intelligence agencies are required to report any violations of FISA 702 targeting, minimisation, and querying procedures requirements to the DoJ and ODNI, who in turn report them to the FISC.[403] Agencies report violations of s.702. FISA to DoJ and ODNI, and all other FISA violations outside of s.702 to DoJ specifically. Under long standing legal principles, the DoJ lawyers owe a duty of candour to the court and are required to report to the FISC any violations of FISA 702 targeting procedures. These lawyers conduct oversight of intelligence agencies' compliance with FISA independently from foreign intelligence priorities, and have frequent meetings / interactions with the FISC to discuss the oversight of s.702.
- The DoJ and ODNI submit semi-annual joint oversight assessment reports to the FISC, identifying targeting compliance trends, explaining categories of compliance incidents and why they occurred, plus what measures intelligence agencies have taken to avoid recurrence.[404] [405] If the FISC identifies any violations, it has the power to order the offending agency to take appropriate remedial action.[406] This can range from an individual to organisation change - e.g. spanning terminating data acquisition, deletion of unlawfully obtained data to a change in the collection practice, including in terms of guidance and training for staff, or additional oversight and reporting.[407]
- In addition, the FISC can and does require the government to explain compliance incidents and describe how they have been remedied. If the FISC is not satisfied, it can terminate the government's authority to engage in data acquisition, or refuse to reauthorise a programme based on targeting decisions that have been made.

[402] See *Security Procedures Established Pursuant to Public Law No. 95-511, 92 Stat. 1783, as Amended, by the Chief Justice of the United States for the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review.*

[403] Rule 13 of the FISC Rules of Procedure.

[404] See, for example, Semi-annual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to s.702 of FISA, Submitted to the FISC by the AG and the DNI, Reporting Period: June 1, 2015 – November 30, 2015 at 35-36 (Nov. 2016), available at https://www.dni.gov/files/documents/icotr/15th-702Joint-Assessment-Nov2016-FINAL-REDACTED1517.pdf The report demonstrates steps taken to remedy non compliance, including the deletion of all data collected unlawfully.

[405] Each individual selector tasked for data acquisition is reviewed for compliance with the targeting procedures.

[406] 50 U.S.C. § 1803(h). See also PCLOB, s.702 Report, p. 76.

[407] See e.g. FISC, Memorandum Opinion and Order at 76 (6 Dec. 2019) (Authorised for Public Release on 4 September 2020), in which the FISC directed the government to submit a written report by 28 February 2020 on the steps the government was taking to improve processes for identifying and removing reports derived from FISA s.702 information that were recalled for compliance reasons, as well as on other matters. See also Annex VII.

Internal controls

The functions of the USIC and the purposes for which they may exercise these functions are set out in the enabling statute for each agency. This limits the activities that can be carried out by that agency, meaning that signals intelligence collection is limited to specified and public purposes. The entire USIC is accountable to Congress.

The head of each intelligence agency is accountable to the DNI.[408] The DNI is appointed by the President, confirmed by the US Senate, and serves at the discretion of the President. Activities conducted by and at the direction of the DNI are subject to independent oversight by all three branches of government. Within the executive branch, the Director's action can be reviewed by the Inspector General ("IG") of the intelligence community, the PCLOB, and the President's Intelligence Oversight Board ("PIOB"). Further, the DNI's action with respect to their responsibilities under FISA is overseen by the FISC.[409] s.102A provides the DNI's with responsibility and authority with respect to ensuring compliance with the Constitution and laws of the US by the USIC[410], and in part these responsibilities are delegated to the CLPO.[411]

Specifically, EO 14086 includes requirements for each intelligence agency to have senior level oversight and compliance officials to ensure compliance with the relevant US laws.[412] This role is fulfilled by the IGs and CLPOs, as well as dedicated officers with a specific compliance role.[413] In particular, the officials are required to conduct periodic oversight of signals intelligence activities and ensure that any instances of non-compliance (specific or systemic) are remedied. In order to ensure that the relevant officials are able to carry out their responsibilities, the intelligence agencies are obligated to provide the officials with access to all relevant information to carry out their oversight functions and may not take any actions to impede or improperly influence their oversight activities. Any significant non-compliance incident identified by an oversight official or any other employee must promptly be reported to the head of the intelligence agency and the DNI, who must ensure that any necessary actions are taken to remediate and prevent recurrence.[414] In relation to s.702 FISA, EO 14086 provides insulation from reprisals and interference in its investigations. This is especially important considering their role within the new redress system for UK data subjects.

Each USIC agency has various individuals (for example, an IG, a CLPO and various other internal employees) who are responsible for advice, feedback, and internal oversight related to the protection of privacy and civil liberties in all activities conducted by its parent organisation.

---

[408] Established by the Intelligence Reform and Terrorism Prevention Act of 2004.

[409] In addition, Article III courts could in theory have broader oversight if a person with standing brings a claim. This would not be litigated in front of FISA. See *Clapper v. Amnesty International USA*, *568 U.S. 398 (2013).*

[410] The Office of the DNI is an executive agency that sits within the US IC and provides coordination and oversight of the other intelligence IC agencies. In addition it has the authority to collect publicly available information and overtly collect information, receive information acquired from other IC elements (e.g. National Counterterrorism Center (NCTC) has access to certain raw FISA information pertaining to counterterrorism) and through sub-parts of ODNI including(namely NCTC) creates new intelligence products that it disseminates.

[411] 50 U.S.C. § 3024 *

[412] S.2(d)(i)(A)-(B) EO 14086.

[413] S.2(d)(i)(B) EO 14086.

[414] S.4(l) EO 14086.

These provide a well-staffed and significant internal audit function that acts as a key safeguard. The involvement of multiple offices and agencies across the USIC increases the transparency and multi-layered oversight approach taken by the US in their national security framework. This increases the protections and identification of compliance issues and ensures that they can be remedied effectively through multiple routes. The continual auditing and assessment process that is undertaken across the intelligence community also reduces the chances of compliance issues being prolonged and not resolved in a timely and effective manner.

Inspectors General

Each element of the USIC's activities is overseen by an independent Office of the IG. This is a statutorily independent unit whose role is to oversee the legality of the activity of the agency, including ensuring compliance with internal privacy policies, as well as how well agencies comply with and enforce federal laws mandating privacy guarantees for both US and non-US persons. IGs also have broad discretion to exercise oversight authority to review programmes and activities of their choosing.

The IGs are permanent and nonpartisan officials who are appointed by, and can only be removed by, the President. To exercise this power, the President would be required to submit a written justification to Congress 30 days before removal. The appointment process is designed to ensure that there is no undue influence by the executive branch officials in the selection, appointment, or removal of an IG. The Executive Office of the President continually reviews how the role of the IG is working in practice. The IGs were created by statute to be an independent and objective unit within the various agencies in order to provide day-to -day, robust oversight that puts the consideration of civil liberties and privacy concerns at the heart of the agencies.

In exercising their authority, the law ensures that IGs have the independent resources to execute their responsibilities and access to all the information needed to execute their responsibilities. This includes the authority to have direct access to all agency records and information detailing the programmes and operations of the agency regardless of classification; the authority to subpoena information and documents; and the authority to administer oaths.[415]

The IGs are subject to reporting and transparency requirements. They are required to complete semi-annual reports that describe identified issues, such problems as well as corrective actions taken to date.[416] These reports can contain non-binding recommendations to the executive branch agencies. Executive Agencies will take recommendations from the IG seriously and will take action to remedy non-compliance: the IG's reports are often made public, and in any event are provided to the Congress: this includes follow-up reports in case corrective action

[415] In limited cases, the head of an Executive Branch agency may prohibit an IG's activity if, for example, an IG audit or investigation would significantly impair the national security interests of the United States. Again, the exercise of this authority is extremely unusual and requires the head of the agency to notify Congress within 30 days of the reasons for exercising it. Indeed, the DNI has never exercised this limitation authority over any IG activities.

[416] S.2(3), 4(a), and 5 of the IG Act; S.103H(k) of the Nat'l Sec. Act; S.17(d) of the CIA Act. The IG of the Department of Justice makes its publicly released reports available on the internet at http://oig.justice.gov/reports/all.htm. Similarly, the IG for the Intelligence Community makes its semi-annual reports publicly available at https://www.dni.gov/index.php/who-we-are/organizations/icig/icig-publications/icig-all-reports.

recommended in previous reports has not yet been completed. Congress is therefore informed of any non-compliance and can exert pressure, including through budgetary means, to achieve corrective action. IGs are also responsible for keeping both heads of executive branch agencies and Congress fully and currently informed through reports of fraud and other serious problems, abuses, and deficiencies relating to the Executive Branch programmes and activities. This double lock of reporting is designed to provide further transparency into the process.

In addition, the IGs have responsibility for taking the claims of Executive Branch whistle-blowers to the appropriate congressional oversight committees for disclosures in relation to alleged fraud or abuse in Executive Branch programs and activities.[417] As the whistle-blowers are often the source for IG investigations, this is key to the effectiveness of the IG's oversight.

The DoJ's Office of the IG has also taken an active role in amending the use of the NSL statutes. For instance, providing recommendations that were then adopted by the FBI in order to ensure that the FBI acted in a manner "*consistent with the privacy protections and civil liberties that [they] are sworn to uphold*."[418] The AG then ordered the FBI and the DoJ to enact change according to the recommendations. Such recommendations and changes are constantly being reviewed to ensure that the authority is being used in a lawful manner. If issues are identified, the various oversight routes and bodies highlighted above have been effective in bringing about change.

To maintain consistent standards between IGs, the Congress established the Council of IGs to develop standards for audits, investigations and reviews. It also promotes training and has the authority to conduct reviews of allegations of IG misconduct. All requirements under the AG approved procedures and guidelines are subject to oversight and periodic auditing by the IGs of the intelligence agencies.

Civil Liberty and Privacy Officers (CLPOs)[419]

The CLPOs have a variety of roles to ensure protection of privacy and civil liberties. They serve as the principal advisor to ensure that the various departments, agencies, and elements that make up the USIC have adequate procedures to address complaints from individuals who allege such a department, agency, or element has violated their privacy or civil liberties[420]. They conduct privacy reviews of proposed and existing agency programmes, advise the heads of their agencies on integrating privacy protection into new policies and initiatives, and ensure that the agency has adequate procedures to investigate and respond to privacy violations. The CLPO is charged with providing advice and oversight regarding how data can be collected, processed

[417] Whistle-blowers will have their identities protected.

[418] See https://archives.fbi.gov/archives/news/pressrel/press-releases/response-to-doj-inspector-general2019s-report-on-fbi2019s-use-of-national-security-letters.

[419] There is a statutory obligation to appoint a CLPO, which also codifies a requirement that agencies ensure they have all necessary information, resources and material to conduct their oversight role. The investigatory powers of the CLPO, as set out in its establishing act, are strengthened by S.803 of the Implementing Recommendations of the 9/11 Commission Act of 2007, codified in the United States Code at 42 U.S.C. § 2000-ee1 (S.1062 of the Intelligence Reform and Terrorism Prevention Act of 2004) which requires that the CLPO be "*provided with all information, material and resources necessary to fulfil the CLPO's duties*". This is further reflected in the ODNI's Intelligence Community Directive 107.

[420] Overview of the broader role of a CLPO: https://www.dni.gov/files/documents/ICD/ICD-107.pdf

and disseminated under the US law by the USIC.[421] They have access to all information needed to perform their responsibilities.

Department and agency CLPOs with national security responsibilities submit semi-annual reports to Congress and the PCLOB on the number and types of privacy reviews, privacy violations, and other privacy matters at the agency. The PCLOB's enabling statute directs the Board to receive these reports and, when appropriate, make recommendations to the privacy and civil liberties officers regarding their activities.

The ODNI CLPO, a position established by statute.[422] The duties of the ODNI CLPO include ensuring that the policies and procedures of the elements of the intelligence community include adequate protections for privacy and civil liberties, and reviewing and investigating complaints alleging abuse or violation of civil liberties and privacy in ODNI programmes and activities.[423] This requires active participation and consultation between the IC, including through each IC element's privacy and civil liberties officers, and the ODNI CLPO.[424]

The ODNI CLPO is a civil servant position appointed by the DNI after a consultation with other heads of the USIC and the Principal Deputy DNI: they are not appointed by, serve at the pleasure of, or can be removed by the President. The ODNI CLPO can only be dismissed by the DNI for cause, i.e., in case of misconduct, malfeasance, breach of security, neglect of duty or incapacity. There are no statutory or specific requirements that must be adhered to when filling the position of the CLPO. Current and previous position holders (under both republican and democratic administrations) have had significant privacy backgrounds and many have trained and worked as lawyers before being appointed CLPO. This independence ensures its effectiveness in the US system.

The CLPO is also responsible for providing appropriate transparency of the USIC to the public through periodic reports[425] and the maintenance of a website that publishes declassified documents, reports and fact sheets.[426] The ODNI CLPO provides information to the public on its website, including instructions for how to submit a complaint. If the ODNI CLPO receives a privacy or civil liberties complaint involving USIC programmes and activities, it will coordinate with other USIC elements on how that complaint should be further processed within the USIC. If information indicates that an agency is non-compliant with privacy requirements, then agencies

[421] S.103B, National Security Act.

[422] The National Security Act 1947 mandates the creation of the ODNI CLPO who reports directly to the DNI and See 50 U.S.C. § 3029.

[423] The ODNI CLPO will work with the ODNI Office of General Council (OGC). ODNI CLPO and ODNI OGC then advise the DNI on the sufficiency of the procedures as they undertake their formal consultative role. The ODNI CLPO and ODNI OGC played this same role for the development of the procedures called for under PPD-28 8 and EO 14086.

[424] For example, S.2.3 of EO 12333 and requires each USIC element to develop procedures governing the collection, retention, and dissemination of US person information. Those procedures must be approved by the AG, in consultation with the DNI.

[425] Latest report (April 2021): https://www.intel.gov/assets/documents/702%20Documents/statistical-transparency-report/2021_odni_annual_statistical_transparency_report_for_cy2020.pdf

[426] https://icontherecord.tumblr.com/.

have compliance mechanisms to review and remedy the incident. Agencies are required to report significant incidents and non-compliance to the ODNI under EO14086 s.2(d)(iii).

The ODNI undertakes an annual review of the USIC and their performance against the NIPF priorities as a whole. This takes into account all types of intelligence collection, investigations into violations and looks both forward and backwards with regards to achieving objectives.

In relation to s.702 FISA, the ODNI CLPO, alongside the DoJ National Security Division, ODNI Office of General Counsel and the ODNI Mission Integration Office of Mission Performance, Analysis and Collection undertakes a regular joint assessment of the USIC's compliance with procedures and guidelines. This joint assessment results in a report required by statute to be submitted every 6 months to the FISC and relevant congressional committees. This joint assessment forms a critical part of the ODNI CLPO's oversight role. Through the joint assessment the CLPO reacts to and assesses both '*ad hoc*'/non-periodic compliance issues and incidents, takes proactive oversight actions,[427] and conducts general oversight actions to identify, assess, and recommend remedial actions to address multi-year compliance trends.

The OPCL at the DoJ supports the duties and responsi-bilities of the Department's Chief Privacy and Civil Liberties Officer ("CPCLO").[428] The principal mission of OPCL is to protect the privacy and civil liberties of the American people through review, oversight, and coordination of the DoJ's privacy operations. OPCL provides legal advice and guidance to Departmental components; ensures the DoJ's privacy compliance with relevant laws; develops and provides Departmental privacy training, policies and reporting; and reviews the information handling practices of the Department to ensure that such practices are consistent with the protection of privacy and civil liberties.

In order to avoid potential conflict within the CLPO's role, the office of the CLPO has a separation within it for teams that advise on policy and teams that manage oversight and complaints. While the oversight teams may review individual decisions and scoping work, the ODNI CLPO does not authorise individual collection or targeting decisions, but has been involved in the development of policies and procedures for each of the USIC agencies governing collection standards, retention limits, access controls, and other privacy and civil liberties protections. The US government has advised DSIT that the 2 roles of the ODNI CLPO are separated within the office to ensure that there is no conflict of interests. This separation for the ODNI CLPO is important in consideration of their oversight and redress role within the USIC and demonstrates their independence from the authorisation and targeting of signals intelligence. However, they are still involved as a consultant in ensuring that policies and procedures take account of the privacy and civil liberties requirements.

This ensures that the protection of civil liberties and privacy have a key role in the development of the highest levels of US signals intelligence.

There is an argument that could be made that by having a role under the new redress mechanism (set out within EO 14086), the ODNI CLPO is not fully independent of the system they are

[427] These could include regular/periodic reviews within the USIC, which include onsite inspections of targeting decisions and disseminations of data.
[428] OPCL provides information to the public about its responsibilities at http://www.justice.gov/opcl.

intended to provide oversight of. However, on balance, DSIT does not consider this to be a substantive matter. The ODNI CLPO is involved in providing insight on privacy and civil liberties from the earliest stages of the development of intelligence and surveillance prioritisation and decisions being taken by the DNI and USIC. DSIT considers that this provides both early checks and balances of this process, and also ensures that the CLPO ODNI better understands the rationale of decisions that were taken, and therefore, if relevant, whether the subject of a complaint was justified when undertaking an investigation. This is similar to the dual role of the UK's National Security Advisor in both advising the UK government on national security issues and heading up the National Security Secretariat, which looks at, inter alia, the policy, ethical and legal issues across the UK intelligence community.

Executive and legislative controls

Presidential oversight of compliance with the Constitution and applicable rules by USIC is carried out by the Intelligence Oversight Board ("IOB"), which is established within the President's Intelligence Advisory Board ("PIAB"). The PIAB is an advisory body within the Executive Office of the President that consists of 16 members appointed by the President from outside the US government. The IOB consists of a maximum of 5 members designated by the President from among PIAB members. The head of each intelligence agency is required to report any intelligence activity for which there is reason to believe that it may be unlawful or contrary to an EO or Presidential Directive, to the IOB.[429] To ensure that the IOB has access to the information necessary to perform its functions, EO 13462 directs the DNI and heads of intelligence agencies to provide any information and assistance the IOB determines is needed to perform its functions, to the extent permitted by law.[430] The IOB is in turn required to inform the President about intelligence activities it believes may be in violation of US law (including EOs) and are not being adequately addressed by the AG, DNI or the head of an intelligence agency. In addition, the IOB is required to inform the AG about possible violations of criminal law.

The US Senate and the House of Representatives have designated intelligence committees with oversight responsibilities.[431] The committees hold hearings, in public or in private, can access confidential information and may issue subpoenas for testimony or documents from CLPOs, agency heads or other officials.[432] The committees receive frequent briefings from intelligence and oversight officials and reports from the intelligence agencies as required by law. The President is required to keep the committees "*fully and currently informed of the intelligence activities*" of the government. FISA requires the AG to "*fully inform*" the Senate and House Intelligence and Judiciary Committees regarding the government's activities under relevant sections of FISA.[433]

[429] EO12333.

[430] EO13462.

[431] The US Senate Select Committee on Intelligence was set up in 1976. It is comprised of 15 senators who have access to intelligence sources, methods, programs and budgets. Supported by staff members, the Committee regularly conducts closed hearings to hear from senior intelligence officials. The US House of Representatives established its 22 senator strong Committee in 1977, with a similar function.

[432] At least once a year the Committee holds a public hearing to receive testimony on national security threats.

[433] 50 U.S.C. §§ 1808, 1807, 1825, 1826, 1846, 1861, 1862, 1871, 1881f

The AG and the DNI are required by law to make regular reports to the relevant committees of the House and the Senate regarding the use of FISA and to report compliance incidents to allow Congress to exercise oversight over the use of signals intelligence through statutorily required reports to the Intelligence and Judiciary Committees, and frequent briefings and hearings.[434] Congress will take these disclosures into account when deciding whether various sections of FISA should continue to operate as is, or be amended or repealed. These include:

- a semi-annual report by the AG documenting the use of s.702 and any compliance incidents;[435]
- a semi-annual assessment within the report by the AG and the DNI documenting compliance with s.702 the targeting and minimisation procedures, including compliance with the procedures designed to ensure that collection is for a valid foreign intelligence purpose;[436]
- an annual report by heads of intelligence elements which includes a certification that collection under s.702 continues to produce foreign intelligence information;
- an annual unclassified reports on the use of the FISA Title I, Subchapter I, s.105 authority[437], which must be released to the public;[438] and
- separate semi-annual reports regarding all FISA uses of pen registers and trap-and-trace devices under s.302,[439] the use of the s.402 authority to use of such pen registers and trap-and-trace devices[440] and the use of the s.502 authority.[441]

Government employees and contractors are legally empowered[442] (and protected) to report serious problems related to surveillance to either committee directly following the processes and procedures authorised by statute.[443]

---

[434] These transparency requirements were passed by Congress in the USA FREEDOM Act of 2015. They are codified at 50 U.S.C. 1872, 1873. Additional reporting requirements to congressional overseers were passed into law in 2003 and in 2004 and are found in 50 U.S.C. 1871-1873.

[435] 50 U.S.C.§1881f. These reports provide an overview of the implementation of Section 702 by US intelligence agencies during the reporting period. The reports provide examples (not each incident) of targeting and other compliance incidents, provide statistical information regarding trends in compliance incidents and remedial measures the government is taking to reduce such incidents. This report also details the external and internal oversight processes involved in 702.

[436] See id. §1881a(l)(1).

[437] 50 U.S.C. § 1807 (a).

[438] 50 U.S.C. § 1807 (b). If the AG can not make it public due to national security concerns, they must make publicly available an unclassified summary or a redacted version of the report.

[439] 50 U.S.C. § 1846(a).

[440] 50 U.S.C. § 1846(b).

[441] 50 U.S.C. § 1862.

[442] IC whistle-blower laws are codified in four separate statutes: the Inspector General Act of 1978, as amended (5 U.S.C. App. §8H), which applies to the inspectors general of all IC elements; the Central Intelligence Agency (CIA) Act of 1949, as amended (50 U.S.C. §3517), which applies to the inspector general of the CIA; the National Security Act of 1947, as amended (50 U.S.C. §3033), which applies to the ICIG; and Title VI of the Intelligence Authorization Act for Fiscal Year 2014, as amended (50 U.S.C. §3234) which provides protections for whistle-blowers making a lawful disclosure. Presidential directive and IC directives also provide further protections and guidance.

[443] See e.g. Intelligence Community Whistle-blower Protection Act of 1998, as amended, Title VII of the Intelligence Authorization Act for Fiscal Year 1999, P.L. 105-272, §§701-702, codified in 5 U.S.C. App. §8H, 50 U.S.C. §3033, and 50 U.S.C. §3517. Under this procedure, the Office of Inspector General ("OIG") the employee and/or contractor must report the violation to the relevant IG. They then have 14 days to determine whether the

US Congress has the responsibility of (re)authorising surveillance programs, as well as responding to reported issues with the system by curtailing some powers. s.702 is subject to "*sunset*" provisions under which it expires on a fixed date unless reauthorised. Since initially enacted in 2008, s.702 has twice been reauthorised: in 2012 and again in 2018, after extensive committee hearings and debate. The most recent reauthorisation included modifications to s.702 improving privacy protections.

National Security Letters (NSL)

The statutes set out that the relevant government authority is required to make annual reports to "*fully inform*" on the use of NSL authorities to congressional intelligence and judiciary committees. Requests under the FCRA must also be made to the banking committees.[444] The IG of the DoJ is required to audit and to report to the judiciary and intelligence committees as to the Department's use of the authority, as well as direct the AG and the DNI to report to Congress on the feasibility of establishing minimisation requirements for the NSLs.[445] The USA Freedom Act instructs the DNI to publish annually on his website the number of NSLs issued in the previous year.[446] It authorises recipients to periodically disclose publicly the number of NSLs and requests they have received.[447] The relevant committees have the ability to question and investigate the use of NSLs. Previous congressional committees have impacted on the way in which NSLs are used. For example, Congress directed the FBI to declassify as much information as possible concerning the use of NSLs in order to allow the maximum amount of public awareness of the extent of our use of the NSL tool consistent with national security concerns.

Privacy and Civil Liberties Oversight Board (PCLOB)

The PCLOB is an independent agency established by statute,[448] with a long history of thorough investigations into US surveillance activities. Its status as an independent agency ensures that it is able to provide proper oversight of US systems. PCLOB constitutes a 5-member, bipartisan Board that is appointed by the President and approved by the Senate. The members sit for a fixed six-year term.[449] In order to avoid partiality, the members of the Board must be selected solely on the basis of their professional qualifications, achievements, public stature, expertise in civil liberties and privacy, and relevant experience, and without regard to political affiliation. There may in no event be more than 3 members of the Board that belong to the same political

"*complaint or information appears credible*". If the determination is positive, then that information is transferred to the relevant committee for their review. If the complainant disagrees with the IG's determination, they can report directly to the Committee, after notifying the relevant IG. The petitioner must still follow procedures to protect classified information. This means that the violations of any law or procedure that violate the rights of a non-US person can form the basis for a whistle-blower report to Congress.

[444] P.L. 109-177, §118(a) (adding the judiciary committees as recipients of all NSL required reports); 12 U.S.C. 3414(a)(5)(C)(intelligence committees); 15 U.S.C. 1681u(i) (intelligence, and banking, finance and urban affairs committees of the house and senate), 15 U.S.C. 1681v(g) (judiciary, financial services, intelligence, and banking, housing and urban affairs committees of the house and senate); 18 U.S.C. 2709 (intelligence and judiciary committees)

[445] S.119 of the USA Patriot Improvement and Reauthorization Act.

[446] 50 U.S.C. 1873.

[447] 50 U.S.C. 1874.

[448] 42 U.S.C. § 2000ee.

[449] 42 U.S.C. § 2000ee (h).

party. An individual appointed to the Board may not, while serving on the Board, be an elected official, officer, or employee of the federal government, other than in the capacity as a member of the Board. These requirements for independence are similar to those required of the judges on the DPRC.

PCLOB's purpose is to ensure that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties. The PCLOB sets its own agenda and determines what oversight or advice activities it wishes to undertake. The Board has 2 fundamental responsibilities — oversight and advice. It is responsible for reviewing counterterrorism programmes and policies (and their implementation), including the use of signals intelligence, and other relevant actions taken by the US government to ensure that they adequately protect privacy and civil liberties. It also ensures that privacy and civil liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the nation from terrorism.

To aid in its work, PCLOB receives reports from the civil liberties and privacy officers of several federal departments/agencies, may request in writing that the AG, on the Board's behalf, issues subpoenas compelling parties outside the Executive Branch to provide relevant information, may issue recommendations to the government and intelligence agencies, and regularly reports to congressional committees and the President.

PCLOB has issued several public reports on USIC activities, including an analysis of the programmes run on the basis of s.702 FISA and the protection of privacy in this context, as well as the implementation of Presidential Policy Directive-28 ("PPD-28")[450] and EO 12333. These reports are made public to the greatest extent possible.[451] In its reviews, PCLOB is able to access any relevant agency records, reports, audits, reviews, documents, papers and recommendations, including classified information, conduct interviews and hear testimony to ensure its investigations are full and thorough.[452] Though it lacks formal investigative powers, PCLOB has a track record of making influential commentary on US systems.[453]

PCLOB has statutory public transparency requirements. This includes keeping the public informed of its activities by holding public hearings and making its reports publicly available, to the greatest extent possible consistent with the protection of classified information. In addition, the PCLOB is required to report when an Executive Branch agency declines to follow its advice.The PCLOB also charged with carrying out specific oversight functions as regards the implementation of EO 14086, in particular by reviewing whether agency procedures are consistent with EO 14086 and evaluating the correct functioning of the redress mechanism.

[450] Now predominantly superseded by EO 14086, with the exception of S.3 (and the complementing Annex) and S.6.
[451] 42 U.S.C. § 2000ee (f).
[452] 42 U.S.C. § 2000ee (g).
[453] For example, PCLOBs January 2014 report on the bulk telephone metadata programme provided an outside assessment of legal and policy issues raised by that programme that influenced Congress's eventual passage of the USA Freedom Act, which ended that specific programme.

Conclusion

Overall, the above assessment highlights the multi-layered approach to oversight that exists within the US government, including the USIC, and including both administrative and independent mechanisms and agencies with clearly established statutory roles. DSIT considers that the totality of the above provides an effective system of checks and balances that will ensure high standards and safeguards are maintained where data has been collected or accessed by government agencies.

The OECD TGA principles also include the commitment to "*effective and impartial oversight*".[454]

Oversight, review and monitoring activities

The US government has introduced various transparency requirements to ensure that people are informed about the US government's work, in a manner commensurate with the need to protect national security.

Each intelligence agency is required to appoint an Intelligence Transparency Officer (ITO) within its leadership to foster transparency and lead transparency initiatives. The ITO must work closely with each intelligence agency's CLPO to ensure that transparency, privacy, and civil liberties continue to remain top priorities.

PCLOB are required to undertake a review of the updated policies and procedures to ensure that they are consistent with the EO. Within 180 days of completion of such a review by the PCLOB, each intelligence agency must carefully consider and implement or otherwise address all of the PCLOB's recommendations.

The DoJ and ODNI conduct compliance reviews at least every two months at each agency that receives unminimised s.702 FISA information, which include reviews of targeting decisions. They report any incidents of non-compliance to the FISC and to Congress.

s.702 FISA

Authorisation to collect data under s.702 FISA may be made "*for a period up to one year from the effective date of the authorization*."[455] However, if the government seeks to reauthorise or replace an existing authorisation, that authorisation remains in effect until the FISC rules on the request to reauthorise or replace it.[456] Requests to reauthorise or replace a s.702 FISA authorisation are reviewed by the FISC under the same rigorous standards as an initial request for authorisation.[457]

For each yearly opinion put out by the court as to the certification, the FISC will also look back at the previous year in determining whether sufficient protections were in place as part of the

[454] OECD TGA Article VI Oversight.
[455] 702(a) of FISA.
[456] 702(j)(5)(B) of FISA.
[457] 702(j)(3), (5) of FISA.

next year's certifications, taking into account instances of non-compliance.[458] If the FISC determines that the government's certifications were not sufficient, including because of particular compliance incidents, it can issue a so-called "*deficiency order*" requiring the government to remedy the violation within 30 days or requiring the government to cease or not begin implementing the s.702 certification. Finally, the FISC assesses trends it observes in compliance issues and may require changes to procedures or additional oversight and reporting as a result.

All approved surveillance activity (including the targeting justifications) must be reviewed at least every 60 days through on-site inspection by the DoJ and ODNI to ensure consistency with the approved targeting and minimisation standards, to ensure that surveillance is strictly limited to foreign intelligence related purposes outside the US and does not extend to US persons.[459] The DoJ and ODNI must also provide twice annual assessments to the FISC and Congress confirming compliance with these protocols. Any violations are required to be reported to the FISC and Congress.[460] The DoJ has published versions of these reports.[461]

The USIC has published many of its policies, procedures, FISC decisions, and other declassified materials, to allow public understanding and inspection of its procedures. Each year, the US also publishes statistics on the government's use of national security collection authorities, including the DNI publishing the total number of s.702 FISA targets in public, annual Statistical Transparency Reports.[462]

FISC and other opinions, as well as other relevant documentation declassified and published on IC on the Record, plus accompanying database.[463] The ODNI has a dedicated public website on which they publish information about their foreign intelligence activities.[464] On this website, it has published a set of concrete transparency principles and an implementation plan that translates the principles into concrete, measurable initiatives. The US Congressional Research

[458] Specifically, every identified compliance incident is reported to the FISC by the government through notices and reports; additionally, the government reports other implementation and compliance information such as the number of targets and other statistical information, the results of oversight reviews, and assessment of compliance trends.

[459] ODNI oversight reviews the information relied upon in the intelligence agencies' FISA determinations. For example, if the intelligence agency claims that the basis for collection against an individual is because that individual is a member of a terrorist organisation, the ODNI will review that information to ensure that the intelligence agency, in fact, has made a sufficient assessment that the individual is a member of a terrorist organisation.

[460] PCLOB, s.702 Report, pp. 70-72; Rule 13(b) of the Rules of Procedure of the United States Intelligence Surveillance Court, available at https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

[461] See, for example, https://www.intelligence.gov/assets/documents/702%20Documents/declassified/23rd_Joint_Assessment_of_FISA_for_Public_Release.pdf.

[462] https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2021/item/2210-statistical-transparency-report-regarding-national-security-authorities-calendar-year-2020.

[463] https://www.intelligence.gov/ic-on-the-record-database.

[464] https://icontherecord.tumblr.com/, accessed 13 September 2021.

Service has published a summary of how the use of NSLs has been investigated and amended as a result of the actions taken by Inspectors General, Congress and the relevant courts.[465]

Companies that receive s.702 FISA directives may publish aggregate data (via transparency reports) on the requests they receive.[466]

EO 14086 redress mechanism

Under the terms of EO 14086, PCLOB is requested to conduct an annual review of the functioning of the redress mechanism to assess whether the ODNI CLPO and DPRC have processed complaints in a timely manner, whether they have had the necessary access to all the information to conduct their investigations, whether the safeguards contained in EO 14066 have been properly considered during the review process and also whether the USIC had fully complied with any determinations made by the ODNI CLPO and the DPRC.[467] The PCLOB is further requested to make an annual public certification as to whether the redress mechanism is processing complaints consistent with the requirements of EO 14086.

After conducting their review the PCLOB is requested to produce a classified report that is sent to the President, the AG, the DNI, the heads of the intelligence agencies, the ODNI CLPO and the relevant congressional intelligence committees. An unclassified version of the report is also to be made public. Unclassified reports of the PCLOB will feed into any review that the UK carries out on the redress mechanism. Such reports should contain any recommendations that the PCLOB deems necessary to ensure the proper functioning of the mechanism. The AG, the DNI, the heads of the intelligence agencies and the ODNI CLPO are required to implement or otherwise address all the recommendations included in such reports.

DSIT is content that the PCLOB has a long standing history of properly auditing, challenging, and obtaining change in relation to the practices of intelligence agencies. As an example, PCLOB has previously produced landmark reports relating to intelligence programmes such as s.702 FISA.[468] This report is still cited as a major authority, demonstrating the rigour of its scrutiny and the esteem in which it is held.[469] Their input has led to the previous overturning of US surveillance programmes on the basis of the content of their reports. In addition, PCLOB has already pushed the USIC to declassify information so that the PCLOB's reports can better inform the public.[470]

---

[465] See: https://crsreports.congress.gov/product/pdf/RL/RL33320

[466] 50 U.S.C. § 1874.

[467] S.3(e) EO 14086. See also: https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e-2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf

[468] See: https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf/.

[469] See: e.g. *United States v. Hasbajrami, 945 F.3d 641, 649 n.4 (2dCir. 2019)* in which the discussion of s.702 "*is drawn in large part*" from the PCLOB report).

[470] As an example, in its report on FISA s.702, the Privacy and Civil Liberties Oversight Board stated: [T]he Board requested declassification of additional facts for use in this Report. The Intelligence Community carefully considered the Board's requests and has engaged in a productive dialogue with PCLOB staff. The Board greatly appreciates the diligent efforts of the Intelligence Community to work through the declassification process, and as a result of the process, many facts that were previously classified are now available to the public. (P. 3)

The USA Freedom Act (2015) modified US surveillance and other national security authorities. It also increased public transparency on the use of these authorities and on decisions of the FISC. It strikes a balance between ensuring that the intelligence agencies have the powers that they need to protect citizens, whilst ensuring that privacy is protected appropriately. In addition, the Act introduces further transparency requirements:

- In consultation with the AG, the DNI is required to either declassify, or publish an unclassified summary of each decision, order or opinion issued by the FISC or the FISCR that includes a significant construction or interpretation of any provision of law.
- Each year the US government must disclose to Congress and the public the number of FISA orders and certifications sought and received; estimates of the number of US persons and non-US persons targeted and affected by surveillance; and the number of appointments of *amici curiae*, among other items of information.
- Additional public reporting by the government about the numbers of National Security Letter requests about both US and non-US persons.

DSIT will take steps in our monitoring work to ensure that the requirements under EO 14086 are complied with and maintained. DSIT notes that EO 14086 sets forth a robust role requesting the PCLOB review agency procedures, provide recommendations, and to provide an annual certification that the requirements of EO 14086 are being complied with. USIC will be required to pay attention to and consider the recommendations. This will act as an oversight body for compliance.

DSIT is satisfied that the US has a genuine commitment to transparency in relation to how the government can access data, both where mandated by legislation and also on a voluntary basis. They publish significant amounts of judgments, policies, reports, etc. - all of which can be used to further identify the routes and reasons for which the US may undertake surveillance, as well as how the law will be applied in practice. In broader terms, the US is a liberal democracy, with strong protections for the freedom of the press. The press is able, and do, publish information and stories about how the US government can access data, which provides further insight about how laws are applied in practice.

Conclusion

Though DSIT acknowledges that there are limitations in what can be publicly shared where national security interests and considerations take precedence, DSIT considers that there are steps and processes in place to provide transparency where able without undermining wider interests. Therefore, DSIT is content that there are appropriate monitoring and oversight systems in place, and ensured through law or directive, to provide adequate transparency of the intelligence gathering mechanisms.

This approach is also in line with the Transparency principle of the OECD TGAs[471]

[471] OECD TGA Article V.

Oversight and monitoring conclusion

Overall, DSIT considers that the monitoring and oversight systems in place in the US, including those that have been recently established by EO 14086, ensures a robust system of checks and balances that will provide transparency, accountability and oversight. Additionally, given the nascent nature of some of the newer safeguards and requirements that were brought in under EO 14086, DSIT will monitor the effectiveness of these safeguards on an ongoing basis to ensure they are functioning as expected and as set out in the above analysis.

National security conclusion

Given the totality of what is set out above, DSIT is satisfied that when the US authorities access data for the purposes of national security, they do so in a manner provided for by law, and in accordance with a framework that ensures sufficient limitations and safeguards that ensure that interferences are necessary and proportionate, and conducted in the pursuit of legitimate aims. These safeguards and limitations sufficiently mitigate the potential for abuse. There is effective redress to rectify unlawful interferences. In addition, the specific requirements under the US legislative instruments highlights the importance of privacy and civil liberties considerations throughout the US signals intelligence procedure.

Law Enforcement

Introduction

In compliance with the specific limitations, safeguards, oversight and redress mechanisms available under US law, US law enforcement agencies are able to obtain personal data and other records from corporations in the US for law enforcement purposes. There is the possibility, therefore, that UK data subjects' personal data could be accessed after being transferred from the UK to a certified US organisation under the DPF.

The US system's various investigative tools that can be used to obtain personal data (and other records) for criminal investigation purposes are subject to a comprehensive and complex system of limitations, safeguards and oversight that ensures that access to data is limited to purposes that are necessary and proportionate to achieve a legitimate aim. Amongst others, it takes into account the federal nature of the US system.

The US Constitution represents the baseline standard for the manner in which US law enforcement agencies are able to access personal data. See the assurances contained in Annex F (DoJ letter). The US system in relation to data processing for law enforcement purposes is underpinned by the basic safeguards afforded by the Fourth Amendment of the US Constitution. These safeguards are considered in detail within the contents of this analysis and principally include requirements for a court order, warrant, subpoena, or consent in order for the use of the various investigative tools. Furthermore, routes of challenge available to UK data subjects who are subject to interference include the ability to seek to have evidence obtained or derived from an unlawful search suppressed if that evidence is introduced against them at trial.

Under US law, violations of state law are investigated by individual states and tried in state courts, but the standard of protections afforded under state law cannot fall below the standard of the Constitution as set out above. As set out in Annex F (DoJ Letter):

> *State law enforcement authorities use warrants and subpoenas issued under state law in essentially the same manner as described herein, but with the possibility that state legal process may be subject to additional protections provided by state constitutions or statutes that exceed those of the US Constitution. State law protections must be at least equal to those of the US Constitution, including but not limited to the Fourth Amendment.*

On that basis, this assessment sets out the relevant protections available within federal law, while giving due consideration to examples of practice in state law in a manner which is proportionate to such an assessment.

Rules governing public authority access

Data transferred to the US and held by US organisations can be accessed by the US government for the purposes of law enforcement only when authorised by statute.

In domestic criminal investigations, the Fourth Amendment of the US Constitution generally requires law enforcement officers to obtain either a court-issued warrant, order, or subpoena, or consent before conducting a search.

Foreign Intelligence Surveillance Act (FISA)[472]

FISA allows the government to compel a company for national security purposes to turn over physical and electronic evidence or conduct surveillance if specific conditions are met. FISA is analysed in detail in the National Security analysis above.

Electronic Communications Privacy Act of 1986 (ECPA)[473]

The Electronic Communications Privacy Act ("ECPA") of 1986 sets forth a system of statutory privacy rights that limit law enforcement access to data regarding customers and subscribers of internet service providers (also known as "ISPs"), telephone companies, and other third-party service providers beyond what is required under constitutional law from customers and subscribers of ISPs. Under the Stored Communications Act ("SCA") of 1986, as enacted as Title II of the ECPA, law enforcement agencies[474] have a variety of legal mechanisms by which they can obtain access to subscriber information, traffic data and stored content of "*electronic communication services*"[475] ("ECS") and "*remote computing services*"[476] ("RCS").

ECPA's provisions are codified in:

- **The Wiretap Act (amended by ECPA)**.[477] Among other things, the Wiretap Act makes it unlawful (subject to certain exceptions)[478] to intentionally intercept[479] wire, oral, and electronic communications while in transit, or to use or disclose the contents of any communication obtained in violation of the statute.
- **The Stored Communications Act (SCA)**.[480] The SCA protects the privacy of wire and electronic communications (for example, emails and messages between social media

[472] Note that US agencies may be able to access data in relation to national security as set out in the National Security analysis above.
[473] 18 U.S.C. §§ 2510-2522.
[474] Law enforcement agencies include the FBI, the Department of Homeland Security ("DHS"), the Internal Revenue Service, Criminal Investigation ("IRS-CI"), and others.
[475] An electronic communication service ("ECS") is defined as any service that enables users to send or receive wire or electronic communications (18 U.S.C. § 2510(15)).
[476] The SCA defines an RCS as providing "*computer storage or processing services by means of an electronic communications system*" to the public (18 U.S.C. § 2711(2); *Quon v. Arch Wireless Operating Co.*, *529 F.3d 892, 902 (9th Cir. 2008)*, rev'd and remanded sub nom. *City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010)* (referring to the RCS as providing processing or data storage by an offsite third party or a "*virtual filing cabinet*")).
[477] 18 U.S.C. §§ 2510-2522.
[478] 18 U.S.C. § 2701 (c).
[479] I.e. - use any electronic, mechanical, or other device to acquire the contents (18 U.S.C. §§ 2510(4)).
[480] 18 U.S.C. §§ 2701-2712.

accounts) and records (for example, email service subscriber names) while in electronic storage, as opposed to "*in transmission.*" The SCA targets two types of online service, electronic communication services, and remote computing services. It contains a blanket prohibition on covered providers from unauthorised access to electronic communications,[481] as well as sharing electronic communications with any person or entity.[482] In a series of exceptions to this prohibition, the SCA also specifies the procedures by which public authorities can compel the disclosure of stored communications and regulates voluntary disclosure by service providers of customer communications and records.[483]

- **The Pen Register and Trap and Trace Devices Statute**.[484] Regulates the government's use of "*pen registers*" and "*trap and trace devices*" related to wire or electronic communications, such as telephone and internet communications.

These laws are binding on federal law enforcement and regulatory authorities. As set out in various statutes, non-compliance with the requirements of the rules can lead to a variety of consequences, including suppression of any evidence gathered and civil actions against individuals or the United States.

To note, with regard to The CLOUD Act[485] and executive agreements under the CLOUD Act do not extend the reach of US law enforcement authorities to conduct wiretaps outside of the US, including via service providers in the EU and the UK.

Applicability of the rules to data subjects

The general and predominant rule is that law enforcement processing of personal data is the same for both US persons and non-US persons.[486] As a general matter, the protections of the Constitution and US laws apply to any person in the US and any criminal defendant in the US.[487] Despite this Constitutional distinction, based on assurances given by the US government (see Annex F DoJ Letter), DSIT is confident that the procedures that govern the routes by which data can be accessed from a US organisation for law enforcement purposes apply to all individuals, including UK data subjects, in the same manner irrespective of the nationality or the physical location of the individual(s) whose data is being accessed.[488]

[481] U.S.C. § 2701

[482] U.S.C. § 2702.

[483] U.S.C. § 2703. Note that § 2703(b) provides the ability to obtain content under an administrative subpoena or disclosure order if the target is given prior notice.

[484] 18 U.S.C. §§ 3121-3127.

[485] HR 4943.

[486] DSIT notes that certain national security and surveillance laws do apply differently to foreign nationals and US citizens, and to foreign nationals who are located in the US and those who are located outside the US. These are set out in the national security analysis.

[487] See David Cole, Are Foreign Nationals Entitled to the Same Constitutional Rights as Citizens?, 25 T. Jefferson L. Rev. 367, 370 (2003), https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1302&context=facpub.

[488] See for instance, with respect to the Wiretap Act, Stored Communications Act and Pen Register Act (mentioned in more detail in recital 92-95), *Suzlon Energy Ltd v. Microsoft Corp., 671 F.3d 726, 729 (9th Cir. 2011)*.

Routes to challenge the requirement on private organisations to disclose the data

Compliance with the disclosure requirements detailed below is mandatory. The private organisation[489] is always able to challenge the disclosure requirement:

Warrant

The subject of a search warrant may move to quash the warrant as overbroad, vexatious or otherwise improperly obtained and aggrieved parties with standing may move to suppress any evidence obtained in an unlawful search.[490]

Subpoena

The recipient of the subpoena can challenge the subpoena on the grounds that it is unreasonable, i.e., overbroad, oppressive or burdensome. If this happens, the court can uphold, quash, add conditions to or otherwise modify the subpoena to respond to the complaint brought.[491]

Court order

Where the court issues an order, the service provider is able to "*promptly*" make a motion to have the order quashed or modified on the grounds that the information or records requested are unusually voluminous in nature or compliance with such order would otherwise cause an undue burden on the provider.

Conclusion

DSIT is content that these provide for the ability to challenge the request in a manner that ensures that the government's use of its powers is subject to various layers of court scrutiny. Where a route does not require the prior authorisation of a court, there is the possibility of an *ex post* judicial scrutiny of the reasonableness of the route used.[492]

Voluntary disclosure

To note, the ECPA also makes specific provision for situations where private organisations voluntarily provide the contents of a communication, a record or other information pertaining to a subscriber to or customer of such service, in a set of defined circumstances.[493] In broad terms, these apply to where there is express authorisation relating to investigative or law

[489] Challenges may be brought by other parties as well, such as the individuals to whom the records or communications pertain.

[490] See *Mapp v. Ohio*, *367 U.S. 643 (1961).*

[491] See *Google Inc v. Hood (2015)*, for an example of such a successful challenge to a subpoena

[492] Perhaps the most noteworthy case was when Twitter challenged a subpoena for Wikileaks records in late 2010/early 2011. Specifically, Twitter challenged the NDO that accompanied the subpoena and prevailed, with a federal judge ordering the subpoena to be unsealed. Twitter then notified its subscribers of the existence of the subpoena. https://www.reuters.com/article/idINIndia-54022420110108.

[493] 8 U.S.C. § 2702 (b).

enforcement,[494] where there is a good faith belief on the part of the provider that disclosure is required in an emergency situation involving danger of death or serious physical injury, with the lawful consent of the originator, an addressee, intended recipient or subscriber, or where the provider has incidentally obtained the information and it appears to pertain to the commission of a crime.

Limitations on access to data by public authorities

Purposes for which public authorities can access personal data

Under US law, federal prosecutors[495] and law enforcement agencies are able to compel production of documents and other record information from corporations subject to US jurisdiction[496] that is needed to investigate criminal offences enumerated in Title 18 of the US Code.[497] They can use several types of compulsory legal processes, including grand jury subpoenas, administrative subpoenas and search warrants, and may acquire other communications pursuant to federal criminal wiretap and pen register authorities. The Affidavit supporting a compulsory process, such as a search warrant or court order, will specify the law enforcement personnel who will have access to the information collected.

The limitations and conditions under which interference with privacy can occur

US Constitution

The Fourth Amendment of the US Constitution provides the baseline rule against a government officer conducting unreasonable searches of seizures.

This Fourth Amendment has been interpreted by the Supreme Court to mean that "*It is unconstitutional under the Fourth Amendment to conduct a search and seizure without a warrant anywhere that a person has a reasonable expectation of privacy, unless certain exceptions apply.*"[498] US law therefore makes distinctions between the nature of the records that the US

[494] 18 U.S.C. § 2517 relates to when information is used / disclosed to an investigative / law enforcement officer, where it is appropriate to the proper performance of the duties of that officer. § 2511(2)(a) relates to where an employee, agent, or officer of a provider is intercepting, disclosing, or using a communication in the normal course of his employment, and where providers are providing information, facilities or technical assistance to persons authorised by law to intercept communications or conduct electronic surveillance, in certain circumstances.
[495] Federal prosecutors are attorneys with the DoJ.
[496] If US law enforcement authorities require information from a foreign entity, they will likely use the MLAT process, which allows them to seek the assistance of foreign counterparts who can obtain the requested data.
[497] 18 U.S.C. § 2516 (1).
[498] See *Katz v. United States, 389 U.S. 347 (1967).*

government is seeking to obtain, taking into account the expectation of privacy related to the information sought. This impacts on the nature of the legal process that must be used.[499] [500]

To obtain a warrant the agency must demonstrate to a magistrate judge[501] on a showing o*f* "*probable cause*" that a crime was committed or is about to be committed and that items connected to the crime are likely to be found in the place specified by the warrant. The warrant must identify the person or property to be searched / seized, designate the magistrate judge to whom it must be returned and require that the warrant be executed within 14 days.[502] Although the Supreme Court has not ruled on whether the Fourth Amendment applies to such contents, in conformance with a federal appeals court ruling, criminal investigators typically obtain search warrants from judges in order to collect the contents of communications or stored data from a commercial communications service provider.[503]

When the warrant requirement does not apply, searches and seizures are still subject to a "*reasonableness*" test[504] under the Fourth Amendment.[505] The Constitution itself, therefore, ensures that the US government does not have limitless, or arbitrary, power to seize private information.

Search and seizure

Under the search and seizure requirement, a warrant will be required for search and seizure, which can include access to electronically stored information.[506] A judge may issue a warrant authorising the interception of communications for up to 30 days[507] upon the request of a federal law enforcement officer or an attorney for the government. To obtain a warrant, the requesting authority must demonstrate probable cause that a crime was committed or is about to be

[499] For example, ECPA distinguishes between the content of communications and records, the former receiving greater protection.In addition, the US makes a distinction between whether a business in the possession of relevant electronic information voluntarily discloses it and those that are compelled by the government to disclose it. The content of electronic information cannot be disclosed without appropriate legal authorisation, but the business can voluntarily provide basic subscriber information and to/from information. They can also provide any information with the "*consent of the subscriber or customer to such disclosure*". See 19 U.S.C. § 2703 (c)(1)(C).

[500] Whether the customer or subscriber will be notified helps drive the type of legal process needed to obtain older communications.

[501] Rule 41 (Search and Seizure, FRCP) explains the circumstances in which a magistrate judges have the authority to issue warrants.

[502] FRCP 41(e)(2)(A).

[503] *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

[504] The reasonableness test means that the court will balance the degree of intrusion on the individual's right to privacy and the need to promote government interests and special needs in exigent circumstances. The court will examine the totality of the circumstances to determine if the search or seizure was justified. When analysing the reasonableness standard, the court uses an objective assessment and considers factors including the degree of intrusion by the search or seizure and the manner in which the search or seizure is conducted.

[505] In a 2018 judgment the US confirmed this position: the US Supreme Court confirmed that a search warrant or warrant exception is also required for law enforcement authorities to access historical cell site location records, that provide a comprehensive overview of a user's movements and that the user can have a reasonable expectation of privacy with respect to such information (*Timothy Ivory Carpenter v. United States of America*, No. 16-402, 585 U.S. (2018)).

[506] The SCA, 18 U.S.C. §§ 2701 et seq.

[507] 18 U.S.C. § 2518(5).

committed, and that there is a reasonable basis for believing that the evidence of the crime being investigated is present at the location specified in the warrant.[508]

Probable cause is not described in the Constitution. The US Supreme Court has favoured a flexible approach to interpretation, defining it as a "*practical, non-technical*" standard that calls upon the "*factual and practical considerations of everyday life on which reasonable and prudent men [...] act.*"[509] As regards to search warrants, probable cause exists when there is a fair probability that a search will result in evidence of a crime being discovered.[510]

The warrant must identify the person or property to be searched[511] / seized, and designate the magistrate judge to whom it must be returned. The warrant will need to be executed within 14 days and be returned to the magistrate judge designated in the warrant.[512]

Subpoenas

Criminal subpoenas are used to support targeted law enforcement investigations. A subpoena is a written order to compel an individual to give testimony on a particular subject, often before a court, but sometimes in other proceedings (such as a congressional inquiry). The applicant must demonstrate that the information sought must be relevant to the investigation and the subpoena cannot be unreasonable because it is overbroad, or because it is oppressive or burdensome. When using this route, the government entity is not required to provide notice to the subscriber or customer.

The subpoena can include a requirement to provide documentation, including electronically stored information. Failure to comply with such an order to appear may be punishable as contempt.

There are two main routes by which businesses can be subpoenaed:

- A Grand Jury Subpoena may be issued by a grand jury (an investigative arm of the court impanelled by a judge or magistrate) to require someone to produce, or make available business records, electronically stored information or other tangible items. They can be issued during investigations of specified crimes and are usually issued at the request of a federal prosecutor.[513]
- An Administrative Subpoena may be exercised in criminal or civil investigations. In the criminal law enforcement context, several federal statutes authorise the use of administrative subpoenas to produce or make available business records, electronically stored information, or other tangible items in investigations involving health care fraud,

[508] 18 U.S.C. § 2518(3)(a)6.
[509] See *Illinois v. Gates, 462 U.S. 213, 232 (1983).*
[510] Ibid.
[511] Rule 41 of the FRCP allows magistrate judges to grant federal agents a single search warrant for multiple computers in different locations.
[512] FRCP 41(e)(2)(A).
[513] This power derives from the Fifth Amendment to the US Constitution, which requires grand jury indictment for any "*capital or otherwise infamous crime*". In order to determine whether a probable cause exists to believe whether a crime has been committed, grand juries have inherent investigative powers that allow them to issue subpoenas to obtain information.

child abuse, Secret Service protection, controlled substance cases, and IG's investigations implicating government agencies.[514]

Grand juries in the US – required for all serious crimes by the US Constitution[515] – are kept sealed and secret.[516] Participants cannot disclose the contents of grand jury proceedings, and those who do are subject to punishment by contempt of court.[517] Typically consisting of between 16 and 23 people, grand juries are private juries that generally serve up to 18 months, though extensions may be granted.[518] While grand juries play an investigative role, they also perform a gatekeeping function, allowing prosecutions to proceed to court and trial only if the prosecutor has assembled evidence sufficient to show "*probable cause*".[519] Secrecy is an enormous component of the grand jury process.[520] The DoJ maintains extensive policies regarding who can, and cannot, violate the veil of secrecy over grand jury proceedings.[521]

Under Rule 17 of the FRCP, which governs how federal criminal prosecutions are handled in the US, the information sought under each subpoena must be relevant to the investigation and the subpoena cannot be unreasonable, i.e., overbroad, oppressive or burdensome.

When documents are produced, the company can withhold information or documents on the basis of privilege. They must disclose the nature of the document or information without revealing the privileged or protected information.

In addition to law enforcement purposes, the US government can use administrative subpoenas to obtain information from certified US organisations for civil or regulatory purposes. The ability for an agency to do this must be set out in statute, where specific limitations are contained on their use. The use of subpoenas will be subject to the "*reasonableness*" requirement, as already set out in the above section on 'Limitations on access to data by public authorities'. The US Supreme Court has set out that in using an administrative subpoena, the investigation must be pursuant and relevant to a legitimate purpose, the information is not already in the possession of the relevant agency, that further examination has been determined to be, and that the other administrative steps required have been followed.[522] In addition, the US Supreme Court has set out that the use of administrative subpoenas must balance the individual and organisational privacy interests with the public interest in the information being sought.[523]

[514] Annex F (DoJ Letter).
[515] Constitution, Amendment V, https://www.law.cornell.edu/constitution/fifth_amendment; the Supreme Court has interpreted the Constitution to only require the federal government to use grand juries for all felony crimes.
[516] FRCP 6(e), https://www.law.cornell.edu/rules/frcrmp/rule_6.
[517] Ibid.
[518] FRCP. 6(g), https://www.law.cornell.edu/rules/frcrmp/rule_6.
[519] Ibid.
[520] FRCP. 6(e), https://www.law.cornell.edu/rules/frcrmp/rule_6.
[521] Disclosure of Matters Occurring Before the Grand Jury to Department of Justice Attorneys and Assistant United States Attorneys, US Dept. of Justice (Jan. 22, 2020), https://www.justice.gov/archives/jm/criminal-resource-manual-156-disclosure-matters-occurring-grand-jury-department-justice-attys.
[522] See *United States v. Powell, 379 U.S. 48 (1964).*
[523] See *Oklahoma Press Publishing Co. v. Walling*, *327 U.S. 186 (1946).*

Court orders for Pen Register and Trap-and-Trace Information[524]

This information comprises incoming[525] and outgoing[526] telephone numbers and Dialing, Routing, Addressing and Signalling (DRAS) information.[527] When a URL (internet address) conveys substantive information, it is considered content.[528] Pen/trap devices do not collect the contents of communications. Neither pen register nor trap-and-trace information are protected by the Fourth Amendment as it has a lower reasonable expectation of privacy. Any competent court can issue an order authorising the collection of this information if the law enforcement authority has certified that the evidence sought is "*relevant to an ongoing criminal investigation.*"[529] The order can apply to "*any person or entity providing wire or electronic communications services in the US whose assistance may facilitate the execution of the order*"[530] and must specify the identity, if known, of the suspect; the attributes of the communications to which it applies and a statement of the offence to which the information to be collected relates.

The use of a pen register or trap-and-trace device may be authorised for a maximum period of 60 days, which may only be extended by a new court order. The use or installation of such a device outside the law is a federal crime, punishable by a fine or up to a year's imprisonment.[531]

Collection under the Stored Communications Act (SCA), as enacted as part of Title II of the Electronic Communications Privacy Act (ECPA)[532]

The SCA sets forth a system of statutory privacy rights that limit law enforcement access as set out in the 'Rules governing public authority access' section above. To obtain the content of communications data under the SCA, a federal law enforcement officer or an attorney for the government must obtain a warrant.

The SCA can also enable access to basic subscriber information that constitutes the "*identifying information for the owner or controller of an internet service account*[533] *and metadata, which may include to/from and time/date stamps on communications, the size or length of communications, location data, and other technical data related to a communication*."[534] The government can

[524] 18 U.S.C. §§ 3121, et seq.

[525] Recorded by trap-and-trace devices.

[526] Recorded by pen registers.

[527] DRAS information would include everything typically contained in the header of an email, excluding the subject line, which would be defined as content.

[528] See Google Inc. Cookie Placement Consumer Privacy Lit., 806 F. 3d 125, 137 (3d Cir. 2015), http://www2.ca3.uscourts.gov/opinarch/134300p.pdf; Under 18 U.S.C. § 2510(8), "content" refers to ""any information concerning the substance, purport, or meaning of [a] communication."

[529] 18 U.S.C. § 3123 (a)(1)-(2).

[530] 18 U.S.C. § 3123 (a)(1).

[531] 18 U.S.C. § 3121.

[532] 18 U.S.C. §§ 2701-2712.

[533] 18 U.S.C. § 2703 (c)(2). This includes the name, address, and any assigned number or identity (e.g. phone number, user name, IP address or email address).

[534] Whilst this is personal information, it is not covered by the Fourth Amendment as the defendant would not have a "*reasonable expectation of privacy*" as it has been shared with a third party business / provided in the "*ordinary course of business*" (*Katz v. United States, 389 US 347, 358 -59 (1967)*) in relation to the information: This is a US doctrine, confirmed by the US Supreme Court that there is no reasonable expectation of privacy in relation to such information.

compel production of this through the use of a warrant, a subpoena,[535] or a court order (known colloquially as a "D" order),[536] or upon formal written request when relevant to a law enforcement investigation. The government can also obtain this information with the subscriber's or customer's consent.

"D" orders in particular may be used to obtain "*the myriad types of data maintained by a provider to enable a customer's use of the service,*"[537] such as customer information, the times and types of communications, the size or length of communications, or other non-content metadata. The procedure for obtaining a court order is as set out in the 'Limitations on access to data by public authorities' section above. A company can also disclose basic subscriber information to a law enforcement agency on request, without penalty under the ECPA.[538]

There are numerous court cases that have been brought in the US challenging where the limits are drawn about what can be considered metadata, demonstrating that the issues are under active judicial consideration, and that the orders are granted on consideration of the issues at play, rather than there being a blanket policy.[539]

The SCA provides for increasing levels of privacy protections depending on the intrusiveness of the collection, though all require a warrant, a subpoena or a court order (as set out above) in order to compel access.

Real time interception of data[540]

When seeking a warrant under the Wiretap Act, the law enforcement agency must also:

- Specify details as to the particular offence that has been, is being, or is about to be committed; a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, a particular description of the type of communications sought to be intercepted,[541] and the identity of the person, if known, committing the offence and whose communications are to be intercepted;[542]
- Set out whether or not other investigative procedures have been tried and failed, or why they reasonably appear to be unlikely to succeed if tried or be too dangerous;[543]

[535] Subpoenas may only be used to obtain limited information as set out in 18 U.S.C. § 2703(c)(2).

[536] Issued under U.S.C. § 2703 (d).

[537] See In re United States for an Order Pursuant to 18 U.S.C. § 2703(d), 2018 U.S. Dist. LEXIS 52183, *12 (D.D.C. Mar. 8, 2018)

[538] 18 U.S.C. § § 2703 (c)(1)(E).

[539] Historically, location data was considered metadata subject to a "D" order. In 2017, in *Carpenter vs. U.S. Supreme Court* held that the Fourth Amendment required a probable cause order for government access to location information, under the facts of that case. That case involved government access to historical records of cell phone location. Under Carpenter, location information of sufficient duration and precision requires a probable cause warrant, while shorter duration or less precise location information may be available under a "D" order. Future case law will more fully define when location information requires a probable cause warrant. See *Carpenter v. U.S.*, 585 US (2018), https://www.oyez.org/cases/2017/16-402

[540] 18 U.S.C. § 2518.

[541] Subject to limited exceptions.

[542] 18 U.S.C. § 2518 (1)(b).

[543] 18 U.S.C. § 2518 (1)(c)

- Set out the duration of the interception, or a particular description of the facts establishing probable cause to believe that additional communications of the same type will occur thereafter and thus no termination date should be set;[544] and
- Give notice of the wiretap to the intercepted individual within 90 days of the completion of the wiretap.[545] However, such failure to give notice does not result in suppression of evidence gathered by the wiretap unless either (1) the defendant can show they were actually prejudiced by the failure to give notice, or (2) they were entitled to notice under the statute or discretion of the judge authorising the wiretap.[546]

Consideration of the impact on the privacy of the affected individual(s)

As set out above, the Fourth Amendment to the Constitution provides the most fundamental level of protection. In *Berger v. State of New York*, the court stated that it is *"[t]he basic purpose of this Amendment, as recognized in countless decisions of this Court, [...]to safeguard the privacy and security of individuals against arbitrary invasions by government officials.*"[547]These standards are applied when the applicant seeks any of the routes by which data can be accessed.

The Constitution itself, therefore, ensures that the US government does not have limitless, or arbitrary, power to seize private information. In practice, the Fourth Amendment sets a default rule that any search or seizure without a warrant is unreasonable, and that a warrant is only obtainable on the showing of "*probable cause*."

In addition, further safeguards are provided for in various DoJ policies and guidelines, including the Attorney General Guidelines for Domestic FBI Operations ("AGG-DOM"), which, *inter alia* require that the FBI uses the least intrusive investigative methods feasible, taking into account the effect on privacy and civil liberties.[548] Any departure from the guidelines must be approved in advance by the FBI's Director, Deputy Director or Executive Assistant Director designated by the Director. If prior approval cannot be obtained due to the immediacy or gravity of a threat to the safety of persons or property or to national security, then the Director (or other authorising person) must be notified as soon as practical. Where the guidelines are not followed, the FBI must notify the DoJ, where the relevant person will inform the AG and Deputy AG.[549]

---

[544] 18 U.S.C. § 2518 (1)(d).

[545] 18 U.S.C. § 2518 (8) (d).

[546] *U.S. v. Principie*, *531 F.2d 1132, 1141 (2d Cir. 1976),* https://casetext.com/case/united-states-v-principie.

[547] 388 U.S. 41, 53 (1967) (citing *Camara v. Mun. Court of San Francisco, 387 U.S. 523, 528 (1967)).*

[548] Attorney General's Guidelines for Domestic FBI Operations (September 2008), available at http://www.justice.gov/archive/opa/docs/guidelines.pdf. Additional rules and policies that prescribe limitations on the investigative activities of federal prosecutors are set out in the United States Attorneys' Manual (USAM), available at

[549] The internal policies and procedures do not create enforceable rights. They could be used as evidence, but the individual would still need an independent right (e.g. unreasonable search) to bring an action in court. An individual could also raise a breach of an internal policy or procedure to the relevant IG.

Post-acquisition use of data

Handling of information

Post-acquisition handling of data is governed by a central policy (Office of Management and Budget ("OMB") Circular No. A-130)[550] that all federal agencies, including law enforcement authorities, are required to implement and follow when handling personally identifiable information.[551] Personally identifiable information is defined as "*information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individua*l".[552]

OMB Circular No. A-130 sets out that all federal agencies are required to *"limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of personally identifiable information to that which is legally authorised, relevant, and reasonably deemed necessary for the proper performance of authorised agency functions*."[553] In addition, to the extent reasonably practicable, federal agencies must ensure that personally identifiable information is accurate, relevant, timely and complete, and reduced to the minimum necessary for the proper performance of an agency's functions. To ensure compliance with the relevant privacy requirements, the agencies must establish a comprehensive privacy programme;[554] develop and evaluate privacy policies and manage privacy risks; maintain procedures to detect, document and report privacy compliance incidents; develop privacy awareness and training programmes for employees and contractors; and put in place policies and procedures to ensure that personnel are held accountable for complying with privacy requirements and policies.[555]

Rule 6 of the FRCP limits disclosure of matters before the grand jury, including documents obtained pursuant to a grand jury subpoena.

Access to and security of information

Under the E-Government Act,[556] the federal government is required to put in place information security protections that reflect the risk and magnitude of the harm that would result from unauthorised access, use, disclosure, disruption, modification, or destruction. They are also required to appoint a Chief Information Officer whose role it is to ensure compliance with the information security requirements and to perform an independent evaluation[557] on an annual basis of their information security programmes and practices.[558]

---

[550] OMB Circular No. A-130: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.
[551] This guidance is issued by the Office of Management and Budget (OMB), under authority provided by the Clinger-Cohen Act (*P.L. 104-106, Division E*) and the Computer Security Act of 1987 (*P.L. 100-235*).
[552] OMB Circular No. A-130, p. 33.
[553] OMB Circular No. A-130, Appendix II, p. 17.
[554] For example, https://www.doi.gov/privacy/privacy-program
[555] OMB Circular No. A-130, Appendix II (5).
[556] Pub. L. 107-347.
[557] The independent evaluation can be carried out by the IGI.
[558] 44 U.S.C. § 3506(a)(2).

Privacy Impact Assessments

Privacy Impact Assessments ("PIAs") are required by s.208 of the E-Government Act for all federal government agencies that develop or procure new information technology that collects, maintains, or disseminates information that is in an identifiable form or that initiates a new collection of information that will be collected, maintained, or disseminated using information technology and includes any information in an identifiable form permitting the physical or online contacting of a specific individual (if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the federal government). A PIA is an analysis of how information in identifiable form is collected, stored, protected, shared, and managed.[559]

The purpose of a PIA is to demonstrate that system owners and developers have incorporated privacy protections throughout the entire life cycle of a system. The Act requires an agency to make PIAs publicly available, except when an agency in its discretion determines publication of the PIA would raise security concerns, reveal classified (i.e., national security) information, or sensitive (e.g. potentially damaging to a national interest, law enforcement effort or competitive business interest contained in the assessment) information.

The Federal Records Act

The Federal Records Act ("FRA") and supplementing regulations require information held by the federal agencies to be held subject to safeguards ensuring the physical integrity of the information, as well as preventing unauthorised access.[560] In relation to data retention,[561] US federal agencies are required to establish retention periods for their records which must be approved by the National Archives and Record Administration. The National Archives and Record Administration has the authority to assess agency records management practices, and may determine whether continued retention of certain records is warranted.[562]

The OMB and the NIST have developed a set of standards that specify the minimum information security requirements that have to be put in place. These are binding on the federal agencies and relate to access controls, ensuring awareness and training, contingency planning, incident response, auditing and accountability tools, ensuring system and information integrity, conducting privacy and security risk assessments, etc.[563]

[559] For example, see the FBI'S PIA of it's SENTINEL Program. https://www.fbi.gov/how-we-can-help-you/more-fbi-services-and-information/freedom-of-information-privacy-act/department-of-justice-fbi-privacy-impact-assessments/sentinel

[560] 44 U.S.C. §3101 et seq.

[561] FRA, 44 U.S.C. §§3101 et seq.

[562] 44 U.S.C. §2904(c), 2906.

[563] These are contained in (for example) OMB Circular No. A-130; NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations (10 December 2020); and the NIST Federal Information Processing Standards 200: Minimum Security Requirements for Federal Information and Information Systems.

Breaches

Under OMB guidelines, all federal agencies are required to maintain and implement a plan for handling data breaches, including when it comes to responding to such breaches and assessing the risks of harm.[564]

Dissemination

Circular No. A-130 contains requirements relating to the dissemination of personally identifiable information. When sharing personally identifiable information with other entities, US federal agencies are required to impose, where appropriate, conditions (including the implementation of specific security and privacy controls) that govern the processing of the information through written agreements,[565] including contracts, data use agreements, information exchange agreements and memoranda of understanding.[566]

Additional requirements may also apply to particular bodies, under more specific rules and internal procedures that govern their use of personal data.

In the law enforcement context, grand jury material can only be produced under specific circumstances.[567] Certain laws also prohibit onward transfers/disclosures of data, for example, the Bank Secrecy Act limits disclosure of Suspicious Activity Reports (SARS).[568] Certain evidence collected pursuant to compulsory process (e.g. search warrants, subpoenas) may also be subject to restrictions on onward transfers. The affidavit supporting a warrant or the application for a court order may specify the law enforcement personnel who will have access to the information. Information collected via a subpoena will be subject to the limits on disclosure set out in Rule 6 of the Federal Rules of Criminal Procedure (FRCP).[569]

In addition, the Privacy Act of 1974 establishes a code of fair information practices[570] that governs the collection, maintenance, use, and dissemination of information about individuals[571] that is maintained in systems of records by federal agencies.The Privacy Act requires that

---

[564] Memorandum 17-12, '*Preparing for and Responding to a Breach of Personally Identifiable Information*' available at https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf and OMB Circular No. A-130. For example, the procedures for responding to data breaches of the Department of Justice, see https://www.justice.gov/file/4336/download.

[565] Written agreement on data sharing practices between agencies for this purpose are commonly included within Memoranda of Understanding between agencies and departments outlining areas of cooperation. For example, a MoU between the FDA and the CDC includes a section on the exchange of information that is not publicly available, see https://www.fda.gov/about-fda/domestic-mous/mou-225-14-017#amendment-2.

[566] OMB Circular No. A-130, Appendix II §3(d).

[567] See, e.g. https://www.justice.gov/archives/jm/criminal-resource-manual-156-disclosure-matters-occurring-grand-jury-department-justice-attys, https://www.law.cornell.edu/rules/frcrmp/rule_6

[568] See: https://www.federalregister.gov/documents/2010/12/03/2010-29880/confidentiality-of-suspicious-activity-reports

[569] https://www.law.cornell.edu/rules/frcrmp/rule_6

[570] 5 U.S.C. § 552a.

[571] Statutory privacy rights and protections within the Privacy Act apply only to US individuals. Where federal agencies maintain '*mixed*' systems of records, OMB guidance advises agencies to treat non-US individuals' information as if it was subject to the Privacy Act. See: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf, pg 2591.

agencies notify the public of their systems of records[572] by publication in the Federal Register. The Act also prohibits the disclosure of a record about an individual from a system of records without the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions.[573]

There may be scenarios in which data accessed may be transferred to state level law enforcement agencies. In any context, state laws and policies cannot violate the US Constitution.

Certain police misconduct laws enforced by the DoJ cover the actions of state, county, and local police officers, though none explicitly deal with privacy or civil liberties.[574] Enforcement is accomplished by the DoJ's Civil Division, which brings cases (either through litigation or an administrative investigation) against a governmental authority or law enforcement agency.

Many state level jurisdictions have in place policies relating to privacy and civil liberties, particularly for law enforcement intelligence centres.[575] Some jurisdictions have also adopted requirements targeted to specific technologies and practices.[576]

Regarding onward transfer of personal data, states generally have a code of criminal procedure which will have similar provisions as Rule 6 of the FRCP.[577] The privacy policies, statutes, and guidance cited above related to law enforcement intelligence centres also contain restrictions on onward transfers, such as disseminating "*criminal intelligence information only to law enforcement or criminal investigative authorities with a right to know and a need to know the information in the performance of law enforcement duties*,"[578] and *"[i]nvestigative and treatment information shall not be disseminated to any department, agency or individual unless the*

[572] A system of records is defined as a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

[573] OMB Guidelines on compliance with the Privacy Act state that the twelve statutory exceptions included within the Privacy Act are permissive, not mandatory exceptions (with the exception of disclosures made in compliance with a FOIA request). See https://www.justice.gov/d9/pages/attachments/2021/02/24/omb_1975_guidelines_0.pdf. Of the twelve exceptions, the most frequently used are the '*Need to Know*' exception (5 U.S.C. § 552a(b)(1)), which covers "*those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties*", the '*FOI Act Disclosure*' exception (5 U.S.C. § 552a(b)(2)) which covers disclosures "*required under section 552 of this title [the Freedom of Information Act]*", and the "*Routine Uses*"' exception (5 U.S.C. § 552a(b)(3)). "*Routine uses" in this instance is defined in Subsection (a)(7) of the Act as meaning "with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected*."

[574] https://www.justice.gov/crt/addressing-police-misconduct-laws-enforced-department-justice;These laws protect all persons in the United States (citizens and non-citizens) so are unlikely to directly apply to UK data subjects. However, they are an example of how law enforcement agencies are held accountable.

[575] For example, the Pennsylvania State Police (PSP), for example, have published a privacy policy for the Pennsylvania Criminal Intelligence Center with information about the PSP's compliance with laws regarding privacy, civil rights, and civil liberties.

[576] New York City Council, for example, passed the Public Oversight of Surveillance Technology (POST) Act in 2020, which was designed to address the growing number of surveillance devices the New York Police Department uses. The law requires the NYPD to disclose the technology tools it uses, as well as those it plans to acquire, along with the policies that govern their use. Over the past few years, several states have passed laws limiting law enforcement's use of facial recognition and biometric data.

[577] https://www.law.cornell.edu/rules/frcrmp/rule_6 This may be known by alternate names, such as rules of criminal procedure.

[578] (E)(1) of "*Attorney General Guidelines on the Collection, Handling, Storage and Dissemination of Intelligence in New Jersey*" https://www.nj.gov/lps/dcj/agguide/intelligence.pdf

department, agency or individual requesting the information is a criminal justice agency which requests the information in connection with its duties, and the request is based upon a name, fingerprints, modus operandi, genetic typing, voice print or other identifying characteristic."[579]

The DoJ has issued guidance to assist state and local law enforcement agencies in developing their policies on data sharing and privacy, such as the *'Privacy, Civil Rights, and Civil Liberties Policy Development Guide for State, Local, and Tribal Justice Entities'*.[580] Law enforcement agencies on the state and local level can choose to reflect the OMB guidance on data breach notifications[581] in their policies where there is no relevant state law otherwise in effect. The DoJ has also issued the '*Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems*'[582] and the '*Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise*'.[583]

Any particular categories of data treated differently

The treatment of specific categories of data is covered under the guidelines set out above. In establishing their policies and procedures, the agencies must take into account, amongst other things, the nature of the information, which will include whether its disclosure could adversely impact a person's privacy or welfare. The ECPA sets out that any privileged information intercepted under the act will not lose its privileged status.

Privileged information and materials in particular are handled very carefully by law enforcement.[584] If the prosecution team (the DoJ attorneys and FBI agents, for example) knows or has reason to believe information is privileged, that information must be reviewed by a filter team which is separate from the prosecution team. The filter team will review the information and segregate potentially privileged materials and release the rest to the prosecution team for review. If the prosecution team becomes aware of privileged material after beginning their review, they must immediately stop and send the material to the filter team.[585]

---

[579] 18 Pa. CS § 9106(c)(4) https://www.legis.state.pa.us/WU01/LI/LI/CT/HTM/18/00.091.006.000..HTM

[580] https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/privacy_policy_cover_and_body_compliant.pdf

[581] https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf

[582] https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/Privacy_Civil_Rights_and_Civil_Liberties_Policy_Templates_0.pdf

[583] https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/privacy%20civil%20rights%20and%20civil%20liberties%20compliance%20verification%20for%20the%20intelligence%20enterprise.pdf

[584] The DOJ's '*Justice Manual*' details the safeguards and procedures federal agencies must follow in ensuring privileged materials are not improperly viewed, seized or retained. See: https://www.justice.gov/jm/jm-9-13000-obtaining-evidence#9-13.420, S.9-13.420(D), (E), (F).

[585] The DOJ regularly reviews the compliance of law enforcement personnel to ensure safeguards for privileged information are followed. By way of example, in 2020 a Special Matters Unit within the Criminal Division's Fraud Section was created "*to focus on issues related to privilege and legal ethics." The unit "(1) conducts filter reviews to ensure that prosecutors are not exposed to potentially privileged material, (2) litigates privilege related issues in connection with Fraud Section cases, and (3) provides training and guidance to Fraud Section prosecutors.*"

Subpoena

Documents can be withheld on the basis that they are privileged or subject to protection under the attorney-client privilege or other privileges. To do so, the person producing the documents must expressly describe the nature of the withheld information in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim. Similarly, if information that was produced is then subject to a claim for privilege or protection, then the party that received the information must (under Rule 45 of the FRCP) "*promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim*."[586]

Particular circumstances in which personal data held by public authorities must be erased

Data that is gathered outside the scope of a request must be destroyed or returned. There may also be internal data retention policies specifying that after a certain period of time and/or if there is no more use for certain data, the policy either allows for, or requires destruction.[587] Courts may also order destruction or return of records.

Use of data in legal proceedings

Whilst an individual is unlikely to be aware that their data is being accessed at the time of access, if the US seeks to use evidence gathered through a search or seizure in a criminal case, constitutional and statutory requirements impose obligations to disclose certain information. This means that the defendant can challenge the legality of the US government's collection and use of the evidence, and can move to suppress evidence obtained or derived from an unlawful search.[588]

An important Fourth Amendment remedy is the exclusionary rule. If a law enforcement agency conducts an unreasonable search or seizure in violation of the Fourth Amendment, any evidence collected therein cannot be introduced in a criminal trial against the defendant.[589] For instance, if a warrant is required for a search and not obtained, evidence gathered in that search will be excluded. If a search warrant was issued without probable cause, evidence gathered under that search warrant will be excluded.

[586] Rule 45 of the FRCP.
[587] For example, The Department of Justice's 'Justice Manual' for DoJ agencies details its policy on the disposal of evidence gathered for closed criminal cases. See: https://www.justice.gov/jm/9-14000-procedure-disposal-seized-evidence-closed-criminal-cases
[588] See *Mapp v. Ohio*, *367 US 643 (1961).*
[589] See *Mapp v. Ohio, 367 US 643 (1961).*

Individual rights and redress

Available routes for redress

As a general rule, and as set out above, the US law enforcement agencies must seek and obtain prior judicial authorisation to collect personal data.[590] US law provides for a variety of avenues by which individuals can bring a claim against a public authority or specific officials for unlawful interference with or processing of personal data. The avenues for redress are available to anyone, regardless of nationality.

Individuals seeking civil redress through the courts must establish that they have sufficient standing to bring a claim.[591] In *TransUnion LLC v. Ramirez*,[592] the Supreme Court held that "*informational injuries*" (such as data breaches or the unauthorised disclosure of data) are not an exception to injury-in-fact requirements, and only satisfy the requirements for standing if they produce an adverse effect. In *Spokeo, Inc. v. Robins*,[593] the Supreme Court held that a claimant cannot "*allege a bare procedural violation, divorced from any concrete harm and satisfy the injury in fact requirement of Article III [standing].*"

ECPA

ECPA criminalises certain conduct. Under the ECPA, an individual can bring a civil action in a US federal district court.[594]

Breaches of the unauthorised access prohibitions in 18 U.S.C. § 2701 expose offenders to penalties of imprisonment for not more than five years (not more than ten years for a subsequent conviction) and/or a fine. Interception, use, or disclosure in violation of the 18 U.S.C. § 2511 is punishable by imprisonment for not more than five years and/or a fine. The use or installation of a pen register or trap-and-trace device by anyone other than the service provider (in limited cases) or those acting under judicial authority is punishable by imprisonment for not more than a year and/or a fine.[595]

[590] Note that prior authorisation is not required for administrative subpoenas. These are only required in specific circumstances.

[591] An individual must be able demonstrate that they have suffered (or will suffer) concrete harm or injury, caused by the unlawful action alleged in the complaint, which would be redressed by a court decision in their favour.

[592] *TransUnion LLC v. Ramirez, 594 US (2021).*

[593] *Spokeo, Inc. v. Robins*, *578 US (2016).*

[594] See *Campbell v. Facebook, Inc., No. 17-16873 (9th Cir. 2020)* for an example of a successful claim brought under the ECPA. The Ninth Circuit held that the plaintiffs had standing to assert claims under ECPA based on the unconsented interception, cataloguing, and use of URLs the plaintiffs had shared in private messages. The Court ruled that the plaintiffs' alleged injury was sufficiently "*concrete*" to confer standing as the ECPA expressly provides a private right of action and protects against the viewing or using of private communications which are analogous to harm traditionally covered by the tort of intrusion upon seclusion. It further reasoned that the plaintiffs need not allege any further harm to have standing because, historically, under common law privacy torts, the intrusion itself was sufficient to render the defendant liable.

[595] 18 U.S.C. § 3121.

SCA

UK individuals could bring a civil action for violations of the SCA.[596] In particular, an individual (including a provider of electronic communications service) can bring a claim[597] against a person or entity who has wilfully committed the unlawful acts, including against the United States.[598] A claim must be brought within two years of the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation. Suits against the US government may result in actual damages or $10,000 USD, whichever is greater, in addition to litigation costs.

If a court or appropriate department or agency determines that the US, or its departments or agencies have violated the SCA, and that the circumstances raise serious questions about whether or not an office or employee of the US acted wilfully or intentionally, then the relevant department or agency will start a process to determine whether disciplinary action is warranted. If the head of the department or agency involved determines that it is not warranted, then they shall notify the relevant IG with the reasons for the decision.[599]

Any wilful disclosure of a "*record*"[600] obtained by an investigative or law enforcement officer made outside the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation.[601]

It is a complete defence to have, in good faith, relied on one of the routes for access set out in this paper, or that one of the statutorily required grounds for permitted disclosure grounds[602] was properly made out. Claims cannot be brought against the provider for complying with the terms of a relevant court order, warrant, subpoena, statutory authorisation or certification.

Victims of a Wiretap Act violation may be entitled to equitable or declaratory relief; actual, statutory, and punitive damages; reasonable attorney's fees; and reasonable litigation costs.[603] The same defences would apply: that the agency, in good faith, relied on one of the routes for access set out in this paper, or that one of the statutorily required grounds for permitted disclosure grounds[604] was properly made out.

---

[596] 18 U.S.C. §§ 2701-2712.

[597] An example of a successful claim being brought under the SCA can be found in *re Facebook, Inc. Internet Tracking Litig. 2 (2017)*. The Ninth Circuit held that Facebook's practice of tracking users' online browsing habits was a violation of the SCA that resulted in a concrete injury, noting that "*these statutory provisions codify a substantive right to privacy, the violation of which gives rise to a concrete injury sufficient to confer standing*."

[598] 18 U.S.C. § 2707(a); 18 U.S.C. § 2712. A civil action against a party other than the US must allege that the conduct constituting the violation was engaged in with a "*knowing or intentional state of mind*." A civil case against the US must allege a wilful violation.

[599] 18 U.S.C. § 2707(d).

[600] Note that "*record*" here refers to the definition under 5 U.S.C. § 552(a)(4): "*any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his . . . criminal . . . history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph*" (emphasis added.) These are records that a government agency maintains. "*Agency*" is specifically defined as *"each authority of the government of the United States, whether or not it is within or subject to review by another agency . . .*" 5 U.S.C. § 551(1).

[601] 18 U.S.C. § 2707(g).

[602] 18 U.S.C. § 2511(3), 2702(b), or 2702(c).

[603] 18 U.S.C. § 2520(b).

[604] 18 U.S.C. §§ 2511(3), 2511(2)(i), or 2511(2)(j).

In addition, the AG has the power to initiate a civil action in a US District Court to seek an injunction (or other necessary action) when it appears that a person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of the Wiretap Act in order to "*prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought*".[605]

When a person receives notice that their communications have been accessed, they can seek to quash and/or modify the order.

Any personnel who are found to have breached relevant policies could face disciplinary actions.[606] As noted above, a court could also order whatever penalty it deemed appropriate for the given circumstances.

Administrative subpoenas will be subject to judicial review in cases where the recipient challenges it on the grounds that the subpoena is onerous, burdensome, or where the issuing agency seeks to enforce the subpoena in court.

The FOIA entitles data subjects to seek access to existing federal records, including records that contain the subject's personal data. Data subjects may make use of the FOIA as a route to determine whether or not a federal agency holds their data as a precursor for other avenues of redress, and entitles the data subject to challenge the US government where they are dissatisfied with their response under the FOIA.[607]

Effective Redress

DSIT has considered how redress is, in practice, effective, reliable, and independent from political or undue influence. DSIT is content that the US court system operates as an effective, reliable and independent mechanism. The US Constitution establishes three separate but equal branches of government: the legislative branch (makes the law), the executive branch (enforces the law), and the judicial branch (interprets the law).

Effective and reliable

The US Court system has a significant case history of hearing cases that examine the application of the Fourth Amendment. These have caused the US government to change its approach, and have confirmed that the US Court system can, and will, provide effective redress.

There are no additional requirements that need to be satisfied for a foreign data subject to bring a claim. There have recently been cases in which non-US persons have sued for violations of

[605] 18 U.S.C. § 2521.

[606] For example, the SCA requires that if a court or appropriate department or agency determines that the US, or its departments or agencies, have violated the SCA, and that the circumstances raise serious questions about potential wilful misconduct or violation, then the relevant department or agency will, on receipt of the court's findings, initiate a process to see if disciplinary action against the officer or employee is warranted. 18 U.S.C. § 2712(c).

[607] Refer to Section on 'Available routes for redress' in the National Security analysis for further treatment of the redress available under the FOIA.

the ECPA and SCA. The fact that the complainant was a foreign data subject was not relevant to the court, which analysed the facts and legal precedent just as it would for any other plaintiff.[608]

Independence

The independence of the judiciary is set out earlier in this analysis.

Right to challenge or complain: access to information

DSIT considers below how individuals have sufficient information to be able to challenge or raise complaints in relation to processing by public authorities (where secrecy permits). Where secrecy prevents information being provided at the relevant time, consideration is given to whether processing can be challenged retrospectively.

Delays and protective orders

Under the SCA, a governmental entity must provide prior notice to the subscriber or customer in limited cases.[609] In certain circumstances, where an administrative subpoena authorised by a Federal or State statute or a Federal or State grand jury subpoena is obtained, the governmental entity may seek to delay providing notice to the affected individual. The governmental entity may include in its application for a court order a request for an order delaying the notification for a period not to exceed 90 days,[610] which the court shall grant if it determines that there is reason to believe that notification of the existence of the court order may have an adverse result.[611] In both cases, an "*adverse result*" is: endangering the life or physical safety of an individual, flight from prosecution, destruction of or tampering with evidence, intimidation of potential witnesses, or otherwise seriously jeopardising an investigation or unduly delaying a trial.[612]

The SCA does not by default forbid a provider from notifying anyone of their receipt of legal process to provide records.[613] Providers will be prohibited from voluntarily notifying their users under the SCA only if the government obtains a protective order under 18 U.S.C. § 2705 based on a need for protection from disclosure. In such cases, a governmental entity must apply to a court for an order requiring a provider to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification will result in endangering the life or physical safety of an individual, flight from prosecution, destruction of or tampering with evidence, intimidation of potential witnesses, or otherwise seriously jeopardising an investigation or unduly delaying a trial.[614]

---

[608] See *Al-Ahmed v. Twitter, Inc., No. 21-CV-08017-EMC, 2023 WL 27356 (N.D. Cal. Jan. 3, 2023)* and *Abdulaziz v. Twitter, Inc., No. 19-CV-06694-LB, 2020 WL 6947929, at *3 (N.D. Cal. Aug. 12, 2020)*.

[609] 18 U.S.C. § 2703(b)(1)(B).
[610] 18 U.S.C. § 2705(a)(1)(A).
[611] 18 U.S.C. § 2705(a)(1)(B); 18 U.S.C. § 2703(b).
[612] 18 U.S.C. § 2705(a)(2).
[613] 18 U.S.C. § 2703.
[614] 18 U.S.C. § 2705(b).

The DoJ has issued a memorandum which requires prosecutors to make a detailed and comprehensive determination about the need for a protective order,[615] including a justification to the court that all the statutory requirements for the protective order are met in the case.[616] In addition, the memorandum sets out that the protective order should not normally seek to delay notification for longer than one year. Where a longer timeframe is required, it can only be sought with the written agreement of a supervisor designated by the US Attorney or an appropriate AG. When an investigation is concluded, the relevant prosecutor must immediately assess whether there is a basis to maintain any existing protective orders. Where this is not the case, they must terminate them and inform the relevant service provider.[617]

Goal of redress

Under the ECPA, an individual can bring a claim for damages (actual and punitive). Damages start at $1,000 and can be imposed punitively for wilful or intentional conduct. Courts may also order "*equitable or declaratory relief as may be appropriate*."[618] This is a broad authority, and courts could use it to provide virtually any kind of relief. They could order erasure, as noted above, particularly if the data is not relevant to the proceedings.

Rectification is not usually applicable in the law enforcement context; the personal data obtained is important in its actual state as "*historical data*" (i.e., data as it was at the time it was created). Courts could theoretically order that an individual be given access to their personal data, but such an order would be highly unusual and potentially damaging to an investigation. Federal prosecutors already have a duty to turn data over to a defendant (e.g. exculpatory material).[619]

Publication of decisions

The Fifth Amendment requires law enforcement agencies to present serious crimes to a grand jury to obtain an indictment before the crime can be prosecuted.[620] As discussed further below, grand juries are required for all felony prosecutions in federal court.[621] Strict rules apply for the secrecy of evidence presented to a grand jury, and for grand jury deliberations.[622] The public

[615] 18 U.S.C. § 2705(b).

[616] See the Memorandum issued by Deputy AG Rod Rosenstein on 19 October 2017 on a more restrictive policy on applications for protective (or non-disclosure) orders, available at https://www.justice.gov/criminal-ccips/page/file/1005791/download. The memorandum is binding on all Department of Justice attorneys and agents.

[617] Memorandum issued by Deputy AG Lisa Monaco on 27 May 2022 on a supplemental policy regarding applications for protective orders pursuant to 18 U.S.C. §2705(b). Available at: https://www.justice.gov/d9/pages/attachments/2022/05/31/section_2705b_supplemental_policy_-_dag_memo_-_05.27.22_005.pdf.

[618] The computation of damages generally differs between statutes, see e.g. 18 U.S.C. § 2707(c) and 18 U.S.C. § 2520(c).

[619] This is documented in DOJ policies, such as the Justice Manual: https://www.justice.gov/jm/jm-9-5000-issues-related-trials-and-other-court-proceedings.

[620] Constitution, Amendment V, https://www.law.cornell.edu/constitution/fifth_amendment.

[621] *Charging*, United States Department of Justice (Mar. 29, 2021), https://www.justice.gov/usao/justice-101/charging.

[622] Fed. R. Crim. Proc. 6 (e) (2), https://www.law.cornell.edu/rules/frcrmp/rule_6.

nature or secrecy of hearings has been discussed above in the National Security sections 'Publication of decisions' section.

Grand juries in the US – required for all serious crimes by the US Constitution[623] – are kept sealed and secret.[624] Participants cannot disclose the contents of grand jury proceedings, and those who do are subject to punishment by contempt of court.[625] Typically consisting of between 16 and 23 people, grand juries are private juries that generally serve up to 18 months, though extensions may be granted.[626] While grand juries play an investigative role, they also perform a gatekeeping function, allowing prosecutions to proceed to court and trial only if the prosecutor has assembled evidence sufficient to show "*probable cause*."[627] Secrecy is an enormous component of the grand jury process[628]. The DoJ maintains extensive policies regarding who can, and cannot, violate the veil of secrecy over grand jury proceedings.[629]

Oversight and enforcement

The activities of federal criminal law enforcement agencies are subject to oversight by various bodies. These are set out more completely in the analysis relating to national security as both national security and law enforcement agencies abide by many of the same overarching oversight authorities.[630] In addition, the constitutionality of various laws can be challenged in the Supreme Court.[631]

Supervision and oversight by bodies or entities and utilisation of power[632]

CIvil Liberty and Privacy Officers (CLPOs)

Departments that have law enforcement responsibilities appoint at least one Privacy Officer and CLPO.[633] The various departments are required to ensure that all relevant CLPOs have all the materials and resources available to them to allow them to fulfil their mandate and carry out their role, including all material and personnel necessary. They must be consulted on all proposed policy changes.[634] The DoJ's CLPO provides legal advice and guidance to Departmental

[623] Constitution, Amendment V, https://www.law.cornell.edu/constitution/fifth_amendment; the Supreme Court has interpreted the Constitution to only require the federal government to use grand juries for all felony crimes.
[624] Fed. R. Crim. Proc. 6(e), https://www.law.cornell.edu/rules/frcrmp/rule_6.
[625] Id.
[626] See Fed. R. Crim. Proc. 6(g),https://www.law.cornell.edu/rules/frcrmp/rule_6.
[627] Id.
[628] See Fed. R. Crim. Proc. 6(e), https://www.law.cornell.edu/rules/frcrmp/rule_6.
[629] Disclosure of Matters Occurring Before the Grand Jury to Department of Justice Attorneys and Assistant United States Attorneys, US Dept. of Justice (Jan. 22, 2020), https://www.justice.gov/archives/jm/criminal-resource-manual-156-disclosure-matters-occurring-grand-jury-department-justice-attys.
[630] In particular CLPOs and IGs.
[631] By way of example, in the case of *Facebook, Inc. v. Wint, 199 A.3d 625, 627 (D.C. 2019)* the US Supreme Court upheld the constitutionality of the SCA.
[632] Areas of this section are substantially covered by similar sections in the above analysis on national security.
[633] 42 U.S.C. § 2000ee-1. Note that departments use different terms to describe the individuals serving as a privacy and/or civil liberties officer. "CLPO" has been adopted here for readability.
[634] 42 U.S.C. § 2000ee-1(d).

components, ensures the Department's privacy compliance, and develops Departmental privacy policy. This includes matters concerning the DoJ's collection, use, and dissemination of personal information, as well as its compliance with privacy-related laws and policies.[635]

Inspectors General

An independent IG provides oversight to the activities of the DoJ, including the FBI and Department of Homeland Security. The position is independent by statute. The DoJ Office of Inspector General ("OIG") reports to both the AG and Congress, and its mission is to investigate allegations of waste, fraud, and abuse in DoJ's programmes and personnel, and to promote economy and efficiency in DoJ operations.[636] Individuals may report concerns, including for misconduct, relating to a DoJ employee, programme, contract, or grant to the DoJ OIG.

If a court or appropriate department or agency determines that the US, or its departments or agencies have violated the SCA, and that the circumstances raise serious questions about potential wilful misconduct or violation, then the relevant department or agency will, on receipt of the court's findings, initiate a process to see if disciplinary action against the officer or employee is warranted.[637] If it is decided that it is not warranted, then the head of the department or agency involved is required to notify the relevant IG with the reasons for the decision. The Inspectors General will accept and investigate complaints from individuals and their websites usually contain instructions for submission and sometimes information about the IG's role and responsibilities.

Specific congressional oversight committees

The relevant committees conduct oversight through a variety of different routes, including hearings (thematic and to conduct oversight), investigations, reviews and reports.

There are also requirements under specific pieces of legislation for reports to be made to the relevant committees in order to enable oversight.

For example, the Director of the FBI is required to "*fully inform*" the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all requests made under 18 U.S.C. § 2709(b) (requests for subscriber information and telephone toll billing records related to an authorised investigation to protect against international terrorism or clandestine intelligence activities).[638]

Under 18 U.S.C. § 2702 (d), the AG is required to report to Congress on where the powers have been used for emergency disclosures, where disclosures have been made in good faith.[639]

In June of each year the Director of the Administrative Office of the United States Courts is required to submit a report to Congress setting out the number of applications for orders

[635] See https://www.justice.gov/opcl/faq.
[636] See https://oig.justice.gov/sites/default/files/2020-04/2020-Strategic-Plan_0.pdf.
[637] 18 U.S.C. § 2712(c).
[638] 18 U.S.C. § 2709(f); https://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports.
[639] 18 U.S.C. § 2702(d); https://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports.

authorising or approving the interception of wire, oral, or electronic communications, and the number of orders and extensions granted or denied under the ECPA during the preceding calendar year.[640]

Administrative authorities' responsibilities to review, monitor, or investigate compliance

DSIT has considered the responsibilities for administrative authorities to review, monitor, or investigate compliance, including whether the outcomes of these activities are published (in full, redacted, or at a principles-level).

CLPOs

Whilst the specific powers of the CLPOs will vary depending on the department, they have general responsibilities for ensuring that privacy and civil liberties concerns are adequately considered in the relevant departments' practices and procedures, as well as ensuring that there are adequate complaints procedures in place for individuals who consider that unlawful interference with their privacy has taken place. Of particular concern to law enforcement, the Chief Privacy Officer for the Department of Homeland Security (DHS) is responsible under statute for preserving and enhancing privacy protections within the department, and for promoting transparency within the department.[641] To fulfil these requirements, all DHS systems, technology, forms and programs are subject to the oversight of a nominated Chief Privacy Officer who has access to all relevant records, reports, audits, reviews, documents, papers, recommendations, and other materials in order to the Department, and if need be by subpoena.

A CLPO may periodically provide reports to Congress, including on the number and nature of the complaints received by the department/agency and a summary of the disposition of such complaints, the reviews and inquiries conducted and the impact of the activities carried out by the Officer.[642]

Inspectors General

The IG has specific authority for conducting independent investigations, audits and inspections of their department's programmes and operations. This includes in relation to law enforcement activities. In order to carry out their activities, the IG has access to all relevant information (by request or subpoena if necessary and can obtain testimony from relevant individuals).[643]

The IG will issue its findings on any areas, with non-binding recommendations to the agency to take corrective action, if necessary. They will also report on whether the agency has complied with their recommendations.[644] The reports will normally be made public and provided to relevant

[640] 18 U.S.C. § 2519(3).

[641] 6 U.S.C. 142, S.222.

[642] 42 U.S.C. §§ 2000ee-1 (f)(1)-(2). For an example of a report provided by an agency's CLPO to Congress, see https://www.dni.gov/files/documents/CLPO/Semiannual_803_Report_Jan_-_Jun_2018.pdf.

[643] See Inspector General Act of 1978, § 6.

[644] See in this respect for instance the overview prepared by the DoJ Office of the IG of its recommendations made and the extent to which they have been implemented through department and agency follow-up actions, https://oig.justice.gov/sites/default/files/reports/22-043.pdf.

Congressional Committees.[645] There are several public examples of where the IG reports have included references to investigations into individuals for unlawful conduct which demonstrates the real impact of the investigations of the IG - see for example most recent (at time of writing) semi-annual report from the Office of the IG within the Department of Justice.[646]

Maintenance of Impartiality and independence with oversight and/or enforcement bodies

Further assessment of the impartiality and independence of CLPOs and Inspectors General is set out in this analysis in the 'Oversight and enforcement' section in the National Security analysis.

The relevant attorneys are also bound by their own professional responsibility obligations. For example, the District of Columbia Bar (of which federal attorneys will be a member) has a Rule of Professional Conduct devoted to the special responsibilities of a prosecutor, including overarching duties to maintain the rule of law and uphold duties to due process and the courts).[647] Breaches of professional obligations can result in sanctions.

The DoJ's Office of Professional Responsibility ("OPR") can also investigate attorney professional misconduct and issue findings and conclusions, which can result in disciplinary decisions and sanctions for current DoJ attorneys. The DoJ's Professional Misconduct Review Unit also authorises referrals to the appropriate bar authority when OPR of the DoJ Office determines that a current or former DoJ attorney engaged in conduct during his or her tenure with the DoJ that implicates a rule of professional conduct.[648]

Law enforcement conclusion

As set out within this analysis, the US system is underpinned by robust limitations, safeguards, oversight and redress mechanisms in relation to law enforcement access to personal data. Based on the totality of this assessment, DSIT is content that the protections available for UK data subjects are not undermined when their personal data is transferred to the US under the UK Extension.

[645] See Inspector General Act of 1978, §§ 4(5), 5.
[646] 1 October 2021- 31 March 2022, https://oig.justice.gov/node/23596.
[647] https://www.dcbar.org/For-Lawyers/Legal-Ethics/Rules-of-Professional-Conduct/Advocate/Special-Responsibilities-of-a-Prosecutor
[648] https://www.justice.gov/jm/jm-1-4000-standards-conduct#1-4.320

Monitoring and Review

Under Section 17B Data Protection Act 2018, if adequacy regulations are made in favour of the UK Extension the Secretary of State must monitor, on an ongoing basis, developments in the US which might affect the protection provided for transfers under the UK Extension. The Secretary of State must also carry out a periodic review of whether there continues to be an adequate level of protection, at intervals of not more than four years.

DSIT will monitor the operation of the UK Extension and the protection provided for personal data transferred to the US under it, with a particular focus on the areas identified in this analysis as meriting further monitoring. This will include the implementation and operation of EO 14086 and the new redress mechanism under it, as well as the way in which the DPF Principles and protections under the UK Extension are applied in practice by certified US organisations, and enforced by regulators.

Operationally, US and UK officials will meet on a periodic basis in order to discuss issues including the functioning of the DPF and the UK Extension. These discussions will encompass consideration of current issues related to the functioning, implementation, supervision, and enforcement of the UK Extension, which may feed into our review and general monitoring of the adequacy regulations.

Conclusion

Following a thorough review of the level of protection provided by the UK Extension and other relevant laws and practices in the US as set out above, DSIT considers that the US ensures an adequate level of protection for personal data transferred to certified US organisations.

Annexes

Annex A - Full text of the EU-US Data Privacy Framework

Annex B - Department of Commerce letter from Secretary of Commerce Gina M. Raimondo, dated 14 July 2023

Annex C - International Trade Administration (Department of Commerce) letter from Under-Secretary for International Trade Marisa Lago, dated 13 July 2023

Annex D-1 and **D-2** - Federal Trade Commission letter from Chair, Federal Trade Commision, Lina M. Khan, dated 13 July 2023, including Appendix A (*"Privacy Shield and Safe Harbor Enforcement"*)

Annex E - Department of Transportation letter from Secretary of Transportation Pete Buttigieg, dated 14 July 2023

Annex F - Department of Justice letter from Deputy Assistant Attorney General and Counselor for International Affairs Bruce C. Swartz, dated 14 July 2023

Annex G - Office of General Counsel of the Office of the Director of National Intelligence, Christopher C. Fonzone to Leslie B. Kiernan, General Counsel of the U.S Department of Commerce, dated 9 December, 2022

Annex H - Glossary of terms

This publication is available from: www.gov.uk/government/organisations/department-for-science-innovation-and-technology

If you need a version of this document in a more accessible format, please email alt.formats@dsit.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.