A Short History of the Fair Information Practice Principles as a Foundation for Personal Data Sharing Across Borders

Introduction

With the development of data protection and privacy laws around the world, the need to resolve differences in privacy approaches is becoming increasingly urgent. This need is largely driven by four factors:

1. The growing complexity, criticality and ubiquity of information technology and the data it generates;
2. The increase in the volume and importance of cross-border data flows;
3. The growing complexity of privacy laws and the restrictions they impose on cross-border data flows; and
4. The increase in the number of countries adopting data privacy laws.

It is easy to become dispirited by the challenge of reconciling different privacy approaches from around the world. Fortunately, on closer examination, one finds a common foundation uniting them all: the Fair Information Practice Principles (FIPPs). This essential commonality suggests that, while a solution will be difficult to achieve, it is within reach if we keep in mind how much these approaches share in common.

A. United States Fair Information Practice Principles (FIPPs)

The FIPPs are a set of internationally recognized best practices for addressing data privacy concerns. The FIPPs are important because they provide the underlying policy for many national laws addressing data protection and privacy matters. The international policy convergence around FIPPs as core elements for information privacy has remained in place since the late 1970s. The U.S. Privacy Act of 1974 codified many of the FIPPs. Around the world, other countries and regions have adopted data privacy laws and guidance that reflect the FIPPs.

The FIPPs were initially articulated by a U.S. government advisory committee in a 1973 report, Records, Computers and the Rights of Citizens, which was issued by the Secretary's Advisory Committee on Automated Personal Data Systems. The committee was established in response to the growing use of automated data systems containing information about individuals. The outcome of the committee was a code of five basic principles for automated personal data systems:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for an individual to find out what information about him is in a record and how it is used.
3. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
4. There must be a way for an individual to correct or amend a record of identifiable information about him.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

In 2009, the Department of Homeland Security (DHS) memorialized the FIPPs as the foundational principles for DHS privacy policy, and developed a clear and helpful articulation of the principles:

1. **Transparency:** DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII).
2. **Individual Participation:** DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII.
3. **Purpose Specification:** DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
4. **Data Minimization:** DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).
5. **Use Limitation:** DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the department should be for a purpose compatible with the purpose for which the PII was collected.
6. **Data Quality and Integrity:** DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.
7. **Security:** DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
8. **Accountability and Auditing:** DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

U.S. agencies have been required since the Privacy Act of 1974 to comply with similar requirements for "systems of records." While the U.S. embraced the fundamental importance of these principles at an early stage, it also understood that certain exceptions were needed when applying these principles in practice. In particular, the Privacy Act includes specific provisions focused on law enforcement and national security. For example, in implementing principles relating to individuals having access to information maintained on them, the Privacy Act lays out a process by which agencies can exempt certain national security and law enforcement records from disclosure. The existence of law enforcement and national security exceptions is a recurring and important theme that must be kept in mind as we consider how to reconcile different privacy approaches.

B. International Frameworks

1. Organization for Economic Co-operation and Development (OECD)

As the United States, Europe, and countries of the Asia-Pacific region began to develop domestic laws on privacy, they also recognized the need to reconcile differences that might create barriers to information sharing in the commercial sphere. For this reason, OECD member countries considered it necessary to develop guidelines that would help to harmonize national privacy legislation and, while upholding such human rights, would prevent interruptions in international flows of data. They represent a consensus on basic privacy principles that can be built into existing national legislation or serve as a basis for legislation in those countries that do not yet have it.

The OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, adopted on September 23, 1980, and revised on September 9, 2013, continue to represent the largest international consensus on general guidance concerning the collection and management of personal information. By articulating core principles, the guidelines play a major role in assisting governments, businesses, and consumer representatives in their efforts to protect privacy and personal data, and in obviating unnecessary restrictions to trans-border data flows, both on- and offline.

The eight national principles set out by the OECD in the revised 2013 OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data are:

1. **Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. **Data Quality Principle:** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

3. **Purpose Specification Principle:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. **Use Limitation Principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except:
    a. with the consent of the data subject; or
    b. by the authority of law.

5. **Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. **Openness Principle:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. **Individual Participation Principle:** An individual should have the right:
    a. to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
    b. to have communicated to him, data relating to him within a reasonable time;
        i. at a charge, if any, that is not excessive;
        ii. in a reasonable manner; and
        iii. in a form that is readily intelligible to him;
    c. to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
    d. to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. **Accountability Principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

The OECD Guidelines acknowledge that countries will include exceptions, and provides that such exceptions "including those relating to national sovereignty, national security and public policy ("order public"), should be: a) as few as possible, and b) made known to the public."

The above eight national principles are further supplemented by the four basic principles on international application:

1. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.
2. Member countries should take all reasonable and appropriate steps to ensure that trans-border flows of personal data, including transit through a Member country, are uninterrupted and secure.
3. A Member country should refrain from restricting trans-border flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.
4. Member countries should avoid developing laws, policies, and practices in the name of the protection of privacy and individual liberties, which would create obstacles to trans-border flows of personal data that would exceed requirements for such protection.

The 2013 Revised OECD Guidelines also introduces several new concepts intended to supplement the original eight principles. These concepts include (i) the obligation to have a

privacy management program in place; (ii) an obligation to be able to demonstrate compliance with the aforementioned privacy management program; and (iii) an obligation to provide good notice to regulators and individuals in the event of a data breach. Since the adoption of the 2013 Revised OECD Guidelines, these concepts have become ubiquitous in new data protection and privacy laws around the world. This is particularly evident in the European General Data Protection Regulation, the California Consumer Privacy Act of 2018, and the draft India Data Protection Bill.

2. Asian-Pacific Economic Cooperation (APEC)

In 2004, the Asian Pacific Economic Cooperation adopted a set of nine privacy principles. Similar to the OECD, the APEC is an organization of 21 member economies. The word "economies" is used to describe APEC members because the APEC cooperative process is predominantly concerned with trade and economic issues, with members engaging with one another as economic entities.

With these goals in mind, the APEC Privacy Framework established nine privacy principles consistent with the OECD's 1980 Privacy Guidelines. These principles are largely the same as the FIPPs with the addition of a harm prevention principle. The harm prevention principle recognizes both the individual's legitimate expectations of privacy and the right to be protected from the misuse of their personal information. Thus, the "remedies for privacy infringements should be designed to prevent harms resulting from the wrongful collection or misuse of personal information, and should be proportionate to the likelihood and severity of any harm threatened by the collection or use of personal information."

The nine APEC principles are:

1. **Preventing harm:** Privacy protections should focus on preventing harm and misuse.

2. **Notice:** Notice of privacy rights should be clear and easily accessible.

3. **Collection limitation:** Collection should be limited to relevant information, in a lawful manner and after notice and consent.

4. **Uses of personal information:** Information should be used for expected and compatibility purposes, with consent or where necessary.

5. **Choice:** Where appropriate, provide clear, accessible opportunities to exercise choice.

6. **Integrity of personal information**: Personal information should be appropriately accurate, complete, and current.

7. **Security safeguards:** Appropriate safeguards to protect against unauthorized access, use, modification, or disclosure.

8. **Access and correction:** Access and correction are important rights with some limitations.

9. **Accountability:** Controllers of personal information are accountable for compliance with all Principles and must use reasonable steps to ensure that recipients of personal information also comply.

While focused on cross-border trade and e-commerce in the Asia-Pacific region, the APEC Framework has been implemented through the Cross Border Privacy Rules (CBPR) System as a method to transfer personal information around the world with trust and confidence. Most recently in April, the APEC framework provided the basis to establish the Global CBPR Forum, a venue to promote interoperability and help bridge different regulatory approaches to data protection and privacy.

As in the OECD Guidelines, the APEC Framework provides that "Exceptions to these Principles … including those relating to national sovereignty, national security, public safety and public policy should be: a) limited and proportional to meeting the objectives to which the exceptions relate; and, b) (i) made known to the public; or, (ii)in accordance with law." In an explanatory note, the APEC Framework helpfully expands on this as follows: "Although recognizing the importance of governmental respect for privacy, this Framework is not intended to impede governmental activities authorized by law when taken to protect national security, public safety, national sovereignty or other public policy. Nonetheless, Economies should take into consideration the impact of these activities upon the rights, responsibilities and legitimate interests of individuals and organizations."

3. The General Data Protection Regulation (GDPR)

It should come as no surprise that the most prominent data protection regime also embraces its own version of the FIPPs. In Article 5, the GDPR lays out the following as principles for the processing of personal data:

> Personal data shall be:
>
> ***
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in

the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

C. U.S. Agreements and Frameworks

The U.S. has successfully negotiated agreements using the FIPPs framework in both the law enforcement and national security space and the commercial context.

1. EU - U.S. Passenger Name Records

In December 2011, the Department of Homeland Security signed an *Agreement between the United States of America and the European Union on the use and transfer of Passenger Name Records to the United States Department of Homeland Security*. The purpose of providing Passenger Name Records (PNR) from air carriers operating passenger flights to the U.S. Department of Homeland Security to "ensure security and to protect the life and safety of the public". The Agreement is focused on the export of personal identifying passenger information from EU originating commercial flights into the United States. There are provisions, however, that the terms of the agreement should be reciprocal in the event the EU requests PNR information from U.S. originating flights.

The PNR Agreement substantially tracks the DHS restatement of the FIPPs :

- **Data Minimization** - Article 8 provides specific data retention periods, placing greater restrictions on the use of the data over time, while the Annex specifies the categories of personal data that the agreement is limited to.

- **Transparency** - Article 10 requires DHS provide information to the travelling public regarding its use and processing of PNR and both parties publicize access, correction or rectification, and redress procedures.

- **Individual Participation** - Articles 11, 12, and 13 provide for access, correction and rectification, and redress for individuals.

- **Purpose Specification** - Article 4 and the Recital limit the purpose of data sharing to counterterrorism purposes, serious transnational crimes

- **Data Quality and Integrity** - The Recital recognizes the need to ensure data quality, accuracy, integrity.

- **Security** - Article 5 - obligates DHS to ensure appropriate technical measures are used to safeguard the data including encryption and physical controls, access controls, and incident management procedures.

- **Accountability and Auditing** - Article 14 and the Recital state that various independent offices and entities may exercise oversight including the DHS Privacy Officers, DHS Chief Privacy Officer, DHS Inspector General, the Government Accountability Office, and Congress.

In addition, Article 7 of the agreement adds a new principle, no automated decision-making based on PNR that will affect the legal interests of the individual.

2. EU-U.S. Privacy Shield (2016)

In 2016, the EU and US negotiated a legal framework for regulating transatlantic exchanges of personal data for commercial purposes known as the EU–US Privacy Shield. The primary purpose was to enable US and EU companies to more easily receive personal data from EU entities under the GDPR meant to protect EU residents. Despite the fact, the European Court of Justice declared the EU–US Privacy Shield invalid in 2020, for reasons related to whether the oversight mechanism of data collected the by US the intelligence community was sufficiently effective, the underlying Privacy Shield principles were effectively still valid. In 2022, the US and EU announced that a new data transfer framework called the Trans-Atlantic Data Privacy Framework had been agreed to, replacing Privacy Shield. Based on statements from the EU and US, the new framework will have changes to the oversight of of data collected by US intelligence agencies.

The Privacy Shield Principles are stated by the Department of Commerce as follows:

- **Notice:** Organizations must provide clear and concise notice to individuals including about type of data collected about them, the purpose for which it used, sharing with third parties, and an explanation of their rights.

- **Choice:** An organization must offer individuals the opportunity to choose whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.

- **Accountability for Onward Transfer:** Organizations that share data with a third party must 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 Principles and will notify the organization if it makes a determination that it can no longer meet this obligation.

- **Security:** Organizations must take reasonable and appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

- **Data Integrity and Purpose Limitation:** Personal information must be limited to the information that is relevant for the purposes of processing and an organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current. An organization must adhere to the Principles for as long as it retains such information.

- **Access:** Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles, except 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 persons other than the individual would be violated.

- **Recourse, Enforcement and Liability:** Effective privacy protection must 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.

3. EU-U.S. Data Protection and Privacy Agreement (the "Umbrella Agreement")

In 2016, after more than six years of negotiation, the EU and the U.S. signed the EU-US agreement on personal data protection (better known as the "Umbrella Agreement") that implemented a comprehensive data protection framework for criminal law enforcement cooperation.

The Umbrella Agreement covers all personal data (e.g., names, addresses, criminal records, etc.) exchanged between police and criminal justice authorities of the EU Member States and the U.S. federal authorities for preventing, investigating, detecting and prosecuting criminal offenses, including terrorism. This Umbrella agreement created a framework for future agreements between the EU-US and Member State law enforcement authorities based on the following principles:

- **Clear limitations on data use –** Personal data may only be used for the purpose of preventing, investigating, detecting or prosecuting criminal offences, and may not be processed beyond compatible purposes.

- **Onward transfer –** Any onward transfer to a non-US, non-EU country or international organisation must be subject to the prior consent of the competent authority of the country which had originally transferred personal data.

- **Retention periods -** Individuals' personal data may not be retained for longer than necessary or appropriate. These retention periods will have to be published or otherwise

made publicly available. The decision on what is an acceptable duration must take into account the impact on people's rights and interests.

- **Right to access and rectification** - Individuals are entitled to access their personal data – subject to certain conditions, given the law enforcement context – and will be able to request the data be corrected if it is inaccurate.

- **Notification of data security breaches –** Notification mechanisms to ensure notification of data security breaches to the competent authority and, where appropriate, the data subject.

- **Judicial redress and enforceability of rights -** EU and U.S. citizens have the right to seek judicial redress if authorities deny access or rectification, or unlawfully disclose their personal data.

4. The United States-Mexico-Canada Agreement (USMCA)

In November 2018, the U.S. signed an agreement with Mexico and Canada in the renegotiation of the North American Free Trade Agreement (NAFTA). The new United States-Mexico-Canada Agreement (USMCA) includes a chapter on Digital Trade. The USMCA can come into effect following the completion of U.S. Trade Promotion Authority procedures, including a Congressional vote on an implementing bill.

The USMCA Chapter on Digital Trade specifically endorsed APEC and OECD privacy principles (noted above) and noting the key principles based on the FIPPs: limitation on collection; choice; data quality; purpose specification; use limitation; security safeguards; transparency; individual participation; and accountability. In addition, the the USMCA noted:

- Restrictions on cross-border flows of personal information should be necessary and proportionate to the risks presented;
- The Parties should adopt non-discriminatory practices in the use of personal information;
- The Parties shall publish information on the personal information a natural person can pursue a remedy; and an enterprise can comply with legal requirements;
- The Parties shall develop mechanisms to promote compatibility between their different regimes.

Possibly the most significant development to come out of the USMCA is the prohibition on data localization:

> *No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.*

This prohibition on data localization is the first active step taken by the U.S. Government to counteract the growing trend of foreign governments that are imposing positive obligations to store data physically within their borders. The reasons for these data localization laws are varied, but the impact has been to prevent access to markets.

D. Conclusion

From their inception in the early 1970s, the FIPPs have been a framework for privacy and data protection laws around the world. The US has successfully used this framework to negotiate cross-border data-sharing arrangements in both the law enforcement and national security context, and in the commercial context. Further, the FIPPs framework has proved critical to creating multi-lateral frameworks with the OECD and APEC, as well as in the trade context with Canada and Mexico. After decades of success, it seems as if the FIPPs could be the basis to support even more cross-border data sharing while protecting privacy.