COMPUTER LAW & SECURITY REVIEW 35 (2019) 380–397

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

EU GDPR or APEC CBPR? A comparative analysis of the approach of the EU and APEC to cross border data transfers and protection of personal data in the IoT era

Clare Sullivan

Visting Professor, Law Center, Georgetown University, Washington D.C., United States of America

ARTICLE INFO

Keywords:
IoT data
GDPR
CBPR
transborder data flows
data protection
privacy
global standard

ABSTRACT

This article examines the two major international data transfer schemes in existence today – the European Union (EU) model which at present is effectively the General Data Protection Regulation (GDPR), and the Asia-Pacific Economic Cooperation (APEC) Cross Border Privacy Rules system (CBPR), in the context of the Internet of Things (IoT).

While IoT data ostensibly relates to things i.e. products and services, it impacts individuals and their data protection and privacy rights, and raises compliance issues for corporations especially in relation to international data flows. The GDPR regulates the processing of personal data of individuals who are EU data subjects including cross border data transfers. As an EU Regulation, the GDPR applies directly as law to EU member nations. The GDPR also has extensive extraterritorial provisions that apply to processing of personal data outside the EU regardless of place of incorporation and geographical area of operation of the data controller/ processor. There are a number of ways that the GDPR enables lawful international transfer of personal data including schemes that are broadly similar to APEC CBPR.

APEC CBPR is the other major regional framework regulating transfer of personal data between APEC member nations. It is essentially a voluntary accountability scheme that initially requires acceptance at country level, followed by independent certification by an accountability agent of the organization wishing to join the scheme. APEC CBPR is viewed by many in the United States of America (US) as preferable to the EU approach because CBPR is considered more conducive to business than its counterpart schemes under the GDPR, and therefore is regarded as the scheme most likely to prevail.

While there are broad areas of similarity between the EU and APEC approaches to data protection in the context of cross border data transfer, there are also substantial differences. This paper considers the similarities and major differences, and the overall suitability of the two models for the era of the Internet of Things (IoT) in which large amounts of personal data are processed on an on-going basis from connected devices around the world. This is the first time the APEC and GDPR cross-border data schemes have been compared in this

E-mail address: cls268@georgetown.edu

https://doi.org/10.1016/j.clsr.2019.05.004

way. The paper concludes with the author expressing a view as to which scheme is likely to set the global standard.

1. Introduction

The EU model is the most widely adopted personal data protection model in the world, with most countries applying its principles, to varying extents, in their domestic legislation. This is true of both developing and developed nations. Most nations have modeled their legislation on the 1995 Directive, the precursor of the current GDPR that came into operation in 2018. The extent of the adoption varies, with some countries closely following the Directive (and hence now most of the GDPR), while others have adopted key elements. The notable exception is the US which has not generally followed the EU model of data protection.

The reasons for the widespread adoption of the EU model are pragmatic. The EU requires that countries wishing to do business in the EU have equivalent data protection requirements. The 1995 Directive provided an existing model of data protection regulation that could be readily incorporated by other nations into their domestic law.[1] The GDPR which came into operations in 2018 closely follows the 1995 Directive while introducing new elements, ostensibly to update the law for the current digital age including the IoT era. Just as its predecessor set the global standard for data protection, the GDPR can be expected can be expected to set the standard for the new era, particularly for IoT data processing, and to inform law reform outside Europe. There are indications that this is already occurring, with the influence of the GDPR seen in increased protection of personal information and privacy, and higher penalties for noncompliance in the domestic legislation of nations outside Europe.[2] The extraterritorial reach of the GDPR is further increasing its influence, primarily through organizational practice and procedure, as corporations outside the EU realize they have to comply with the GDPR because they are processing the personal data of EU data subjects.

This has raised concerns especially by US multinationals about compliance costs and the need to streamline global compliance strategy and procedures. In the US, the APEC approach using its CBPR scheme is widely considered to be the better model for cross border data transfer, primarily because it is regarded as less prescriptive and restrictive than the GDPR and therefore more conducive to facilitating international data flows.

APEC is a regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific.[3] APEC is loosely modelled on the EU in that it is regional body but APEC does not have the EU's lawmaking powers and governance mechanisms. APEC currently has 21 member economies comprising mostly Asia Pacific countries but also including the US, Canada, Chile, Mexico, and Russia.[4] The stated aim of APEC is "to create greater prosperity for the people of the region by promoting balanced, inclusive, sustainable, innovative and secure growth and by accelerating regional economic integration."[5] In line with this objective, APEC CBPR was established in 2012 as a voluntary regional scheme to facilitate cross border data flows between member economies that met the data protection standards set by the scheme. The CBPR is based on the data protection principles set out in the APEC Privacy Framework (Framework). The CBPR system first requires that an economy join CBPR and establish the necessary legislative and enforcement requirements, then that a corporation that wishes to transfer data under the scheme undergo an independent compliance assessment.[6] In 2012, the U.S. became the first nation to participate in the CBPR scheme and the US Federal Trade Commission (FTC) became the first domestic enforcement authority. FTC and many US corporations are advocates of the scheme.

2. IoT data and communications

This article considers whether the GDPR or the APEC CBPR scheme is most appropriate for cross-border transfers of data, particularly personal data in the IoT era.

IoT as used in this paper is defined in its broadest sense to encompass the wide range of connected devices and applications ranging from industrial and sectorial applications, such as operational monitoring and analysis to optimize efficiency in manufacturing, transportation and logistics, to the connectedness, monitoring and responsiveness that characterize

[1] Australia for example, was one of the first nations outside Europe to implement data protection legislation based on the EU model; and over time Australia updated its Privacy Act 1988 (Cth) to align with the EU required standards.

[2] This has already occurred in Japan and Korea, for example. The Korean Personal Information Protection Act 2011 (PIPPA) is recent example. PIPPA closely follows the EU model, especially the Directive, but now also includes aspects of the GDPR in the increased protection for data subjects and in its enforcement regime. Similar developments have occurred in Japan that has also incorporated aspects of the GDPR into its domestic law. Japan's amended Protection of Personal Information Act (PPIA) also uses the EU adequacy approach in assessing level of data protection provided by a foreign country for cross-border data transfers. Under the amendments to PPIA that came into effect in May 2017, the regulator can warn companies in breach and seek monetary sanctions of up to 300,000 yen and up to six months in prison for offenders.

[3] APEC, "What is Asia-Pacific Economic Cooperation?" at https://www.apec.org/About-Us/About-APEC.

[4] APEC, "Member Economies" at https://www.apec.org/About-Us/About-APEC/Member-Economies.aspx.

[5] APEC, "What is Asia-Pacific Economic Cooperation?" at https://www.apec.org/About-Us/About-APEC.

[6] "By applying this commonly agreed-upon baseline set of rules, the CBPR system bridges across domestic differences that may exist amongst domestic privacy approaches." See, APEC, "APEC Cross-Border Privacy Rules (CBPR) System" at https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.

smart cities. IoT also includes consumer applications. Consumer applications include for example, internet-connected home appliances and devices such as consumer wearables like smart watches, fitness trackers, and connected headsets many of which collect and process personal data on an ongoing, real-time basis, as well as connected cars and other vehicles.[7] Consumer applications also involve commercial IoT when data is collected, transmitted, stored, and analyzed to provide performance and other data to businesses. IoT generally is rapidly converging with OTT services, AI, Deep Learning, and robotics to manage assets and services and generally transform sectors ranging from manufacturing to services, including those which are considered essential, such as utilities, heath care, security, and law enforcement. This convergence coupled with international data flows that unpin IoT data processing, present significant issues for protection of personal data.

One of the most significant technical challenges for the IoT era is the efficient management of an unprecedented volume of IoT data and its varied nature. This also presents legal compliance challenges. IoT devices are designed to monitor and respond, resulting in large amounts of data, including personal data, being processed on a continuous basis. Data is personal if it can directly or indirectly identify an individual, thereby bringing it within the (very similar) definitions of personal data in the GDPR, the APEC CBPR, and domestic legislation that regulates data processing in most jurisdictions. Processing is also typically defined widely. The GDPR for example, defines processing as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." This definition captures all IoT data handling activities.

On-going, fast processing of data[8] including personal data, much of which is sensitive, has an unprecedented impact on individual's personal data protection and privacy. Sensitive personal data or "special category data" as it is now referred to in the GDPR is generally defined as data that can reveal a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person. Data concerning health or data concerning a natural person's sex life or sexual orientation is also classified in this way, typically requiring additional protections. Processing of this personal data is prohibited under data protection legislation in the absence of data subject consent.[9] Data anonymization and pseudonymization whereby data supposedly cannot identify or be associated with an individual, are promoted especially by the GDPR as a way of facilitating the processing of data necessary for IoT. However, both techniques have well-known fallibilities and re-identification presents a significant risk to infringement of individual rights, and to IoT data processors and controllers being found non-compliant.[10]

Consequently, IoT challenges the privacy and data protection principles and assumptions that typically underpin data protection regimes, including the GDPR and the APEC CBPR and much national legislation. IoT data processing is a significant new challenge for law and regulation in balancing business imperatives and the societal benefits of the IoT with protection of personal data and the confidentiality of electronic communications. There is tension between facilitating the public benefits of IoT and protecting the rights of individuals. While both the EU and APEC data transfer regimes attempt to balance competing interests, each has a fundamentally different legal basis, and a different approach to data protection.

It is against this background that this paper examines and compares the two approaches, and given the following of the APEC CBPR in the US, assesses whether the CBPR or the GDPR better balances data protection with facilitation of cross border data flows. The author concludes by positing a view as to whether one scheme is likely to emerge as the dominant global approach.

3. Similar but different

There are broad similarities between the APEC CBPR and cross border transfer mechanisms under the EU GDPR. Under the GDPR there are a range of voluntary options for corporations in countries such as the US, that are not considered to have domestic privacy and data protection requirements equivalent to the EU. In addition to the well-known EU /US Privacy Shield (Privacy Shield), other accepted mechanisms include use of standard contractual clauses, approved Codes of Conduct, and certification under the GDPR. This is in contrast to APEC that has one voluntary scheme, CBPR, for its member economies. Most of the transfer mechanisms under GDPR have similarities with CBPR but the latter is most similar in approach to Privacy Shield in that CBPR requires acceptance at country level, followed by an independent certification process for the individual organization wishing to join the scheme.

[7] As National Institute of Standards and Technology, U.S. Department of Commerce (NIST) explains, "[u]biquitous deployment of smart, interconnected devices is estimated to reach 50 billion units by 2020. This exponential increase is fueled by the proliferation of mobile devices (e.g. mobile 163 phones and tablets), smart sensors serving different vertical markets (e.g. smart power grids, autonomous transportation, industrial controls, smart cities, wearables, etc.), wireless sensors and actuators networks. New concepts and technologies are needed to manage this growing fleet of Internet of Things (IoT) devices." See also Michaela Iorga Larry Feldman, Robert Barton, Michael J. Martin, Nedim Goren, Charif Mahmoudi, "The NIST Definition of Fog Computing", NIST Special Publication 800-191 (Draft) 23 24, August 2017 at 1.

[8] Timely analysis is needed for effective management.

[9] There are some limited exceptions. See Article 9 of the GDPR, for example. There are specific rules designed to ensure that consent is fully informed and freely given by the data subject.

[10] See Ohm, P "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" 57 UCLA LAW REVIEW 1701 (2010), 1701, and Article 29 Data Protection Working Party, "Opinion 05/2014 on Anonymisation Techniques", April 2014, 21 where it is noted that "[E]ven if different pseudonymized attributes are used for the same data subject, linkability may still be possible by means of other attributes."

However, although the broad data protection objectives and operation of the APEC CBRP and Privacy Shield schemes are similar, the legal foundation and application of the schemes differ. The CBPR is based on the data protection principles in the APEC Framework which is a basic standard. The APEC Framework, is not as comprehensive, nor as prescriptive as the GDPR and is different in nature. The APEC requirements essentially are a regional data protection standard, whereas the GDPR is an EU Regulation that applies directly as law in the EU[11] and outside the EU through extraterritorial application. Article 3 of the GDPR applies the regulation to organizations processing personal data of EU data subjects[12] regardless of the organization's geographical base and area of operation.[13]

Also, unlike the APEC CBPR, the GDPR is part of a relatively comprehensive suite of regulations intended to address a wide range of issues relevant to the EU in the digital era. The data protection reform package that came into effect in 2018 consists of the GDPR and the Data Protection Directive for Police and Criminal Justice Authorities (DPDPC). This reform package not only updates and replaces the 1995 Data Protection Directive, it reforms the 2008 Framework Decision for the police and criminal justice sector which is designed to facilitate cross-border cooperation to more effectively combat crime and terrorisms. A key part of this reform package is the proposed EU Regulation Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications (ePrivacy Regulation) that will apply to IoT communications. Although originally planned to come into effect at the same time as the GDPR in 2018, the new ePrivacy Regulation is now not expected to become law in the EU until 2019. The proposed ePrivacy Regulation updates and replaces the current ePrivacy Directive that applies to electronic communications. The proposed new regulation substantially changes and extends the existing Directive including extending operation to over-the-top (OTT) services like WhatsApp, Facebook Messenger, and Skype, metadata associated with electronic communications, and to IoT communications. Like the GDPR, the proposed EU ePrivacy Regulation has extraterritorial application and serious consequences for non-compliance but it has a different conceptual basis to the GDPR in that it protects the right to confidentiality and is not limited to protecting individuals. Also, unlike the GDPR, the new ePrivacy Regulation does not generally permit processing based on data subject consent, public interest or legitimate interests of the data controller. While the proposed e-Privacy Regulation is of more limited operation than the GDPR in that it applies to communications, it promises to be more restrictive than the GDPR.

The APEC scheme does not specifically apply to electronic communications and[14] This is not necessarily a deficiency when considering IoT data. A better approach for the EU would be to apply the data protection requirements that are accorded to personal data under the GDPR, rather than also bringing IoT data communications within the proposed new ePrivacy Regulation. However, the overall observation relevant to this discussion is that in comparison to the suite of applicable regulations in the EU, the approach of APEC is much less comprehensive.

The legal foundation of the EU approach is fundamentally different to that of APEC scheme. The EU regulations are based on fundamental human rights, specifically the right to data protection and the right to privacy for the GDPR and in the case of the new ePrivacy Regulation, the right to confidentiality in communications. While the data protection principles in the APEC framework are broadly similar to the basic principles of GDPR, the former is not grounded in human rights-based jurisprudence in the same way, nor to the same extent as the EU regulations. The focus of APEC tends to lean more towards facilitating data transfers within what it considers acceptable data protection parameters. This is evident in one of the stated objectives of the APEC CBPR which is to promote "a policy framework designed to ensure the continued free flow of personal information[15] across borders while establishing

[11] The GDPR, like the 1995 Directive, applies to processing of personal data of an individual who is an E.U. data subject. However, whereas the 1995 Directive established a data protection standard to be incorporated into domestic law but gave discretion to member nations as to how that is done, the GDPR as a regulation, applies directly as law.

[12] Under the GDPR, an EU data subject is a data subject in the EU. A data subject is defined as a natural person who is identified or identifiable by the data pursuant to Article 4 (1) of the GDPR and that term as used in this article has the same general meaning

[13] This is substantially broader than the 1995 Directive which applied to organizations based outside Europe when they did business in the EU Article 3 of the GDPR states: (1). This Regulation applies to the *processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.* (2). "This Regulation applies to the processing of personal data of data subjects who are in the Union *by a controller or processor not established in the Union, where the processing activities are related to:* (a) *the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union;* or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union." (My emphasis)The rationale is explained in the GDPR in Recital (101): "Flows of personal data to and from countries outside the Union and international organizations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organizations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organization to controllers, processors in the same or another third country or international organization. In any event, transfers to third countries and international organizations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor."

[14] The Framework does not purport to cover communications. However, national legislation exists. While establishing minimum standards for regulation of electronic communications in the APEC region may generally be desirable, it is likely to prove a difficult very task politically.

[15] The APEC scheme and some data protection legislation such as the Australian Privacy Act for example, uses personal information instead of personal data. This article refers to information when that terms is used by the applicable scheme and/or legislation. The

meaningful protection for the privacy and security of personal information."[16] The key questions therefore are whether the APEC CBPR appropriately balances trade objectives with adequate protection of personal data and individual privacy; and how does the APEC scheme compare with the EU model in achieving that balance. These questions are explored in this article

4. Overview of the APEC CBPR system

The APEC CBPR is based on the Framework a set of principles and implementation guidelines created in 2005 and updated in 2015.[17] The Framework seeks to balance the free flow of data across borders with the recognized need to provide adequate protection for the personal information[18] and privacy of individual data subjects. Unlike the GDPR and the proposed ePrivacy Regulation which apply as law in EU countries and extraterritorially, the APEC Framework does not apply as law. It is an agreed standard. The Framework, as its title suggests, sets out the basic elements for minimum data protection standards that APEC member economies agree to use in establishing or amending their domestic law. In the absence of domestic legislation or where applicable law provides less protection for data subjects, the Framework provides an agreed minimum level of data protection.[19]

The CBPR system consists of three components: first, the Framework which sets out the baseline data protection requirements; secondly a system for selection and accreditation of the accountability agents which are APEC-recognized independent third parties qualified to assess and certify corporate privacy practices against the Framework; and thirdly a domestic enforcement mechanism.[20]

In order for an APEC member economy to join the system there are specific requirements including existence of a local enforcement authority and local law that allows for the enforcement of the requirements of the Framework as a minimum.[21] The APEC member economy must also endorse the accountability agent who certifies the privacy practices of companies that want to be a part of the system and manage dispute resolution for the certified company so the privacy enforcement authority doesn't have to deal with the majority of complaints.[22] A company wishing to join CBPR then establishes its privacy policy and practices to conform either to the baseline rules in the Framework or to local law, whichever is more privacy protective; and then corporate policy and practice are assessed by the accountability agents for certification under the scheme.[23] Accountability agents such as TrustArc Inc.[24] (TrustArc) in the US for example, typically set out specific certification requirements in more detail, covering additional management requirements to the 50 item Assessment Criteria in the CBPR Program Requirements (CBPR Assessment Criteria).[25] The CBPR assessment and compliance process is comprehensive and time-consuming for both the corporation and for the accountability agent. The cost depends on the organization, its business and operations, and its internal resources but it can be an expensive process. At least in the short term, this generally limits CBPR to organizations that have the necessary funds and resources. In the U.S, for example, the companies who have joined the CBPR scheme are typically large multinationals, mostly technology companies.

definition of information in the applicable legislation and scheme documentation usually includes data, and vice versa.

[16] The focus of APEC is reflected in a stated objective of APEC CBPR as "promoting a policy framework designed to ensure the continued free flow of personal information across borders while establishing meaningful protection for the privacy and security of personal information. See, APEC Cross-Border Privacy Rules System Policies, Rules and Guidelines, 2011, 2 at file:///C:/Users/domin/Downloads/CBPR-PoliciesRulesGuidelines%20(1).pdf

[17] See Preamble Part 1 (8) which states that "The Framework was developed and updated in recognition of the importance of: • Implementing appropriate privacy protections for personal information, particularly from the harmful consequences of intrusions and the misuse of personal information; • The free flow of information to trade, and to economic and social growth in both developed and developing market economies; • Enabling global companies that collect, access, use or process data in APEC member economies to develop and implement uniform approaches within their organizations for global access to and use of personal information; • Empowering Privacy Enforcement Authorities to fulfill their mandate to protect individual privacy; • Advancing international and regional mechanisms, including the APEC Cross Border Privacy Rules (CBPR) system, to promote and enforce privacy and to maintain the continuity of information flows among APEC economies and with their trading partners; • Encouraging organizations to be accountable for all personal information under their control; and • Promoting interoperability between the Framework, and its implementing measures such as the CPEA and CBPR system, and privacy arrangements in other regions."

[18] Note that the Framework tends to use "information" whereas GDPR uses "data" but they effectively have the same meaning. This paper uses both terms interchangeably.

[19] Much like the 1995 Directive which is the predecessor of the GDPR in the EU, the APEC Framework which forms the basis of CBPR, sets a minimum data protection standard for domestic legislation for APEC nations.

[20] See APEC Framework Part II Section 12.

[21] To join CBPR, an APEC member must first submit a formal declaration of its intent to participate in the system, demonstrate how the CBPR can be enforced under national law and identify at least one accountability agent. Each participating nation must also have at least one domestic privacy enforcement authority capable of enforcing the minimum standards of the Framework and which participates in the APEC Cross-border Privacy Enforcement Arrangement (CPEA).

[22] Accountability agents must meet rigorous assessment criteria as to their obligations for initial assessment and certification and on-going monitoring of the certified companies, conflict of interests, and the handing of data subject complaints. Accountability agents must be re-approved every year by the participating APEC members.

[23] Companies must apply to an accountability agent that assesses the company's privacy policies and practices against the Framework requirements, requires adjustments and modifications as necessary and certifies the company Certified companies have to be recertified annually. Overlaying the entire CBPR system is a governance and operations structure led by a Joint Oversight Panel that is responsible for approving economy-level participation and for managing recognition of accountability agents.

[24] Formerly TRUSTe Inc.

[25] APEC, "APEC Cross-Border Privacy Rules System Program Requirements" at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx.

As at the time of writing, the USA, Mexico, Japan, Canada and the Republic of Korea have joined CBPR, with Australia announcing its intention to join. While there are similar voluntary schemes under the GDPR, CBPR is generally more appealing to US corporations particularly to large multinationals that can afford the accreditation process. CBPR is considered more attractive from a corporate compliance perspective because it is considered less complex and prescriptive, and more facilitative of cross-border data flows compared to the EU model.[26] Indeed, the focus of the CBPR system differs from the GDPR which is primarily concerned to protect personal data and individual privacy as part of the E.U.'s human rights obligations. CBPR is instead designed primarily to facilitate trans-border data flows and was explicitly established to guide the development of "effective privacy protections that avoid barriers to information flows, and ensure continued trade, and economic growth in the APEC region."[27] US multinationals for example, use CBPR to transfer of personal data from Japan to the US. This reliance is necessary because Japan has not designated the US as a jurisdiction as having adequate data protection by Japanese standards.

5. Overview of GDPR mechanisms

Unlike the APEC CBPR which is one voluntary scheme, the GDPR contains a number of approaches that can be used by organizations transferring personal data across borders. The primary provisions are in Chapter V (Articles 44 through 49) which sets out conditions that must be followed by data controllers and processors. The GDPR states that "[A]ll provisions in this Chapter shall be applied in order to *ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined*."[28] (my emphasis)

The GDPR permits data transfers to countries[29] that the European Commission (EC) considers provide an "adequate" level of personal data protection and Article 45[30] deals with transfers on the basis of an adequacy decision.[31] Recital 104 provides that adequacy essentially equates to equivalency i.e. that the third country or specified entity ensures "an adequate level of protection essentially equivalent to that ensured within the [European] Union."[32] The foreign system when considered as a whole, must be of a standard equivalent to the EU.[33] In determining adequacy, the Commission considers a range of factors including specific processing activities, international human rights norms, the general and sectoral law of the country, legislation concerning public security, defense and national security, public order, and criminal law.[34] The EC considers "an adequacy decision, including a partial or sector-specific one, is the best avenue to build mutual trust, guaranteeing uninhibited flow of personal data, and thus facilitate commercial exchanges involving transfers of personal data."[35] The widespread adoption of the EU data protection model, including its human rights foundations, by countries outside the EU may lead to more transfers proceeding on the basis of adequacy.

[26] Note however that the EU is moving towards greater transparency for data that is non-personal. EU Regulation 2018/1807 which provides a framework for the free flow of non-personal data in the EU will apply to EU Member States in May 2019. The main purpose of this new Regulation is to facilitate movement of non-personal data across borders.

[27] APEC, APEC Privacy Framework, 2015, Forward, 2.

[28] Article 44.

[29] Chapter V covers transfer of personal data to third countries or international organisations. If the personal data of an EU data subject is transferred to a country outside the EU, the Articles in this Chapter apply

[30] Article 45 provides that:" (1) A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation. (2) When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements: (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred; the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data."

[31] Whereas only approved third countries could receive personal data transfers outside the EU member states under the 1995 Directive, the GDPR permits transfers third countries, and to a territory or a specified sector within a third country, or to an international organization, provided they have been given the Commission's adequacy designation. The designation binds all EU member states.

[32] See also, Judgment of the Court of Justice of the EU of 6 October 2015 in Case C-362/14, *Maximillian Schrems v Data Protection Commissioner,* points 73, 74 and 96.

[33] See, Judgment of the Court of Justice of the EU of 6 October 2015 in Case C-362/14, *Maximillian Schrems v Data Protection Commissioner,* point 74 which confirms that the adequacy standard is substantive and does not require a point-to-point replication of the EU rules.

[34] Recital 107 states that adequacy decisions are also subject to periodic review to determine whether the entity still ensures an adequate level of data protection. Recital 108 provides that the Commission consult with the entity, and consider relevant developments in the entity and information from other relevant sources such as the findings of the European Parliament or Council.

[35] European Commission, Communication from the Commission to the European Parliament and the Council, "Exchanging and Protecting Personal Data in a Globalised World", Brussels, 10.1.2017 COM (2017) 7 final, 9.

In the absence of an adequacy decision, transfers are permitted under the GDPR if the controller or processor utilizes other safeguards which under Article 49 include:

- Legally binding and enforceable instrument between public authorities or bodies
- Binding Corporate Rules (BCRs) under Article 47
- Standard data protection contractual clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2).
- Standard data protection contractual clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure referred to in Article 93(2).
- An approved code of conduct under Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.
- An approved certification mechanism under Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights

The EU does not consider the laws of the US provide adequate data protection. To address this issue and facilitate data flows between the EU and US Privacy Shield was agreed in 2016 in the wake of the finding that its predecessor, the EU-US Safe Harbor Framework under the 1995 Directive was inadequate.[36] Privacy Shield applies the data protection standards required by the EU through a voluntary op-in scheme that is very similar to CBPR.[37] A US organization that wants to process the personal data of an E.U. data subject can voluntarily commit to the EU-US Privacy Shield Framework and is then bound by it. Privacy Shield includes assurances by the US government preventing access to data, as well as for a U.S.-based compliance and enforcement regime. The US Department of Commerce (DoC) monitors compliance and the FTC is responsible for enforcement.[38] A data privacy ombudsman within the U.S. State Department is the contact for EU citizens for complaints in relation to how their personal data is processed under Privacy Shield. US organizations participating in Privacy Shield must comply with mandatory deadlines for dealing with individual complaints and EU data subjects have access to alternative dispute resolution. Additionally, the EU member States' Data Protection Authorities (DPAs) can refer complaints directly to the DoC and the FTC. The Privacy Shield arrangements are reviewed annually to ensure that they meet EU privacy standards. Compliance is monitored by the E.C. as part of the annual review.[39] It should be noted, however, that like its predecessor, Privacy Shield can be challenged as not providing an adequate level of protection; and questions have been referred to the European Court of Justice (ECJ) that could impact the future of Privacy Shield.[40]

Of the other options under Article 49, the most relevant to a U.S. corporation are standard contractual clauses which under the GDPR can include model clauses[41] (although currently there are no EU-processor to non-EU processor clauses), BCRs which under the GDPR extend beyond a corporate group to unrelated businesses involved in common enterprise,[42] approved codes of conduct, and certification. The GDPR removes some of the red tape that applied under the 1995 Directive. For example, under the GDPR standard contractual clauses[43] and BCRs can be used without prior notice and approval of a DPA.[44] The new regulation places greater emphasis on these mechanisms, includes more detailed guidance, and integrates them into the GDPR's compliance and enforcement regime. Unlike the Directive, the GDPR specifically includes BCRs as an appropriate safeguard in Article 46 and provides detailed conditions for transfers by way of BCRs in Article 47. The GDPR sets out the minimum content of BCRs including information about the data and transfer processes, how the general data protection principles, are applied, structure and contact details for the concerned corporation/s, complaint procedures,

[36] This was the result of the decision of the Court of Justice of the European Union (CJEU) in *Schrems v Data Protection Commissioner* Case C-362/14 in October 2015. Schrems brought the action against the Irish data protection authority regarding his concerns about the transfer of his Facebook data from Ireland to the US. The decision largely turned on the finding that the protections provided under the framework did not meet the EU standards because the safe harbor framework did not provide adequate independent oversight and redress for EU data subjects. On 3 February 2016, the EU and US agreed in principal to a new framework to replace safe harbor and following months of negotiation and revision, the EU-US Privacy Shield was signed on July 12th, 2016.

[37] Privacy Shield attempts to address the concerns of the highly influential E.U. Article 29 Working Party (Working Party) in April 2016 but there are still concerns about the effectiveness of the current framework and that Privacy Shield could be the subject of a challenge.

[38] A key feature of the agreement is a guarantee by the US Director of National Intelligence (DNI) that the US government will use EU personal data only for purposes that are necessary and proportionate for national security.

[39] The E.C. considers that the following criteria (i) the extent of the EU's (actual or potential) commercial relations with the third country, including the existence of a free trade agreement or ongoing negotiations; (ii) the extent of personal data flows from the EU, reflecting geographical and/or cultural ties; (iii) the pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region; and (iv) the overall political relationship with the third country, in particular with respect to the promotion of common values and shared objectives at international level. The E.C. has also indicated that adequacy will be considered on a sectorial basis rather than country-wide, where appropriate. See Article 45.

[40] On April 12, 2018, the Irish High Court in the matter of the Data Protection Commissioner v Facebook Corporation and Maximillian Schrems (2016 No:4089P) referred a number of questions to the ECJ, including where it references Privacy Shield. See Data Protection Commissioner v Facebook Corporation and Maximillian Schrems (2016 No:4089P) at http://www.europe-v-facebook.org/sh2/ref.pdf.

[41] See Article 46.

[42] See Articles 46(2)(b) and 47, and recital 110.

[43] Ad hoc contractual clauses can also be used but are subject to prior supervisory authority approval.

[44] See Article 46(2).

and compliance mechanisms. As such BCR's have similarities with CBPR.[45]

Approved Codes of Conduct and certification area also applicable. As explained by the EC, "[n]on EU-controllers will be able to adhere to an EU code of conduct or certification mechanism by making binding and enforceable commitments, via contractual or other legally binding commitments, to apply the data protection safeguards contained in those instruments."[46] A code of conduct can address many aspects of the GDPR including international data transfers. The GDPR refers to codes of conduct as "binding and enforceable" in relation to cross-border transfers. Controllers adopting BCRs must demonstrate that they are binding in that they constitute compliance obligations for subsidiaries and employees, establish third party beneficiary rights for data subjects, show accepting liability and submitting to DPA jurisdiction, and confirming sufficient assets to pay damages for a breach While it is not clear exactly how this will operate in practice, it is likely to be similar to the use of BCRs. Adherence to codes of conduct by controllers or processors not otherwise subject to the GDPR but involved in the transfer of personal data outside the E.U. assists a regulated controller in demonstrating GDPR compliance.

Articles 40 and 41 of the GDPR authorize the use of code of conduct which can be created by the regulator; or "associations or other bodies representing controllers or processors," to implement the requirements of the GDPR.[47] Recital 99 encourages private associations preparing codes of conduct to "consult relevant stakeholders, including data subjects where feasible, and have regard to submissions received and views expressed in response to such consultations." A draft code must be submitted to the appropriate supervisory authority to determine whether it provides "sufficient appropriate safeguards." Approved codes of conduct must enable "the mandatory monitoring of compliance with its provisions;" and the monitoring body must be accredited by the competent supervisory authority, after demonstrating "an appropriate level of expertise in relation to the subject-matter of the code."[48] An accredited and competent body may monitor compliance.[49] Adherence to an approved code of conduct can be used by both data controllers[50] and processors[51] to demonstrate that the required safeguards and procedures are followed[52] for personal data transfers to third countries.[53] The accredited body shall "take appropriate action" when a controller or processor "infringes" the code of conduct, including suspending or excluding the infringing party from the code. Under Article 83(4)(c), an accredited monitoring body faces fines up to 10,000,000 EUR for failing to "take appropriate action" when a controller or processor infringes a code of conduct. Notably, the action of the accredited body does not displace the action that can be taken by the regulator for non-compliance. The monitoring body must notify the supervising authority which can also take enforcement action.[54]

The new certification procedure under the GDPR is of particular relevance to U.S. corporations processing and transferring personal data. Certification covers obligations under to Article 25 of the GDPR, which governs data protection by design and by default. Article 25(2) requires a controller "shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed." The GDPR expressly recognizes certifications (as well as seals and marks) as a means of demonstrating compliance by controllers and processors.[55] Only certification under the GDPR can be used to demonstrate compliance with Article 25 under which data controllers are obliged to implement "appropriate technical and organisational measures, such as pseudonymization" to "integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects." However, despite known fallibilities of anonymization

[45] See for example, in relation to BCRs under the 1995 Directive, "Joint work between experts from the Article 29 Working Party and from APEC Economies, on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross Border Privacy Rules submitted to APEC CBPR Accountability Agents" at file:///C:/Users/domin/Downloads/20140307_Referential-BCR-CBPR-reqs%20(4).pdf.

[46] European Commission, Communication from the Commission to the European Parliament and the Council, "Exchanging and Protecting Personal Data in a Globalised World", Brussels, 10.1.2017 COM (2017) 7 final, 5.

[47] Under Article 83(2)(j) a supervisory authority can consider adherence to an approved code of conduct (and certification) as a mitigating factor in assessing an administrative fine.

[48] To be accredited, the body must show that it (a) demonstrates "its independence and expertise in relation to the subject-matter of the code to the satisfaction of the competent supervisory authority"; (b) "has established procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation"; (c) "has established procedures and structures to deal with complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make these procedures and structures transparent to data subjects and the public"; and (d) "demonstrates to the satisfaction of the competent supervisory authority that its tasks and duties do not result in a conflict of interests." See Article 41(2).

[49] See, Article 41(1).

[50] Article 24 sets out the controller's primary responsibilities with regard to processing personal data, and expressly encourages codes of conduct to demonstrate GDPR compliance.

[51] Article 28 and Recital 81 expressly provide that adherence to an approved code of conduct by a processor is "an element to demonstrate compliance" with the controller's obligations.

[52] Article 32 (3) further expressly acknowledges adherence to an approved code of conduct as a means of demonstrating compliance with the Regulation's data security obligations.

[53] Recital 77 of the GDPR encourages use of approved codes of conduct by both controllers and processors These codes may demonstrate that a controller or processor has identified any risk related to data processing; assessed the origin, nature, likelihood, and severity of the risk; and determined how best to mitigate the risk

[54] Enforcement by the accredited body is "without prejudice to the tasks and powers of the supervisory authority." Article 41(1).

[55] Article 42(1) provides that Member States, supervisory authorities, the Board, and the Commission shall all "encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors."

and pseudonymization techniques,[56] the GDPR does not contain a saving provision that protects an organization from exposure to liability under the regulation or more generally, should data subject identification or re-identification occur.[57]

Like the codes of conduct, certification is available to controllers and processors outside the EU if they can show willingness to adhere to the mandated data protection safeguards through contracts or other binding legal instruments. Certifications covering general GDPR compliance as well as the obligations under Article 25 may be issued by either an accredited certification body,[58] "the competent supervisory authority", or by the European Data Protection Board,[59] which may create a "common certification—the European Data Protection Seal."[60] The body doing the certification must conduct a "proper assessment" leading to granting certification, and its withdrawal in the event of noncompliance. The body must inform the supervisory authority, and provide reasons, when it grants or withdraws certification from a controller or processor. Accredited certification bodies that violate their duties under the GDPR are subject to penalties up to 10,000,000 EUR.

Certification is for a maximum of three years. It can be renewed if the conditions and requirements are met. certifications are voluntary, must be "via a process that is transparent," and do not "reduce the responsibility of the controller or the processor for compliance" with the GDPR.[61] As with codes of conduct, non-E.U. controllers and processors must also make "binding and enforceable commitments, via contractual or other legally binding instruments, to apply those appropriate safeguards, including as regards data subjects' rights." Article 46(f), further provides that compliant cross-border data transfers may involve an approved certification mechanism but must also involve binding and enforceable commitments "in the third country." Like codes of conduct, certification by an accredited body is taken into account in assessing an administrative fine under Article 83(2)(j) for non-compliance by a controller or processor.

Derogation or exception to the general prohibition on transferring personal data outside the EU without adequate protections are permitted but only in limited circumstances. The derogations in the GDPR[62] are generally the same as those in the Directive, but there is a new derogation for acceptable transfers for the "compelling legitimate interests" of the controller.

Derogation is permitted when:

- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.
- The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
- The transfer is made from a register that, according to E.U. or member state law, is intended to provide information to the public and that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

[56] Anonymization means that the data subject/s cannot, or can no longer, be identified or identifiable. As stated in Recital 26, anonymization takes the processing outside the scope of the GDPR, obviating the need for compliance with its requirements. Pseudonymization is defined in Article 4 (5) of the GDPR as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." Article 6 (4) (e) of the GDPR permits the processing of pseudonymized data for uses beyond the purpose for which the data was originally collected and Recital 78 and Article 25 also list pseudonymization as a method to show GDPR compliance.

[57] For further discussion of this point see, Clare Sullivan, GDPR Regulation of AI and Deep Learning in the Context of IoT Data Processing—A Risky Strategy, (2018) Vol 22 Issue 6 Journal of Internet Law 7. See also Recital 9 of the new EU Regulation 2018/1807 on a framework for the free flow of non-personal data in the EU which also confirms that data that is de-anonymized is personal data. Recital 9 which applies to IoT data recognizes "[T]he expanding Internet of Things, artificial intelligence and machine learning, represent major sources of non-personal data, for example as a result of their deployment in automated industrial production processes. Specific examples of non-personal data include aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines. *If technological developments make it possible to turn anonymised data into personal data, such data are to be treated as personal data,* and Regulation (EU) 2016/679 is to apply accordingly." (my emphasis)

[58] In the US, TRUSTe is an example of an organization that conducts certification assessments of U.S corporations in relation to compliance under the 1995 Directive, self-certification required by the US Department of Commerce, and APEC certification. TRUSTe is currently the only accredited Accountability Agent in the US under APEC CBPR). In Europe, EuroPriSe seal has been the principal European certification body for the 1955 Directive.

[59] The European Data Protection Board is also empowered to accredit certification bodies and maintain a register of accredited bodies. The GDPR directs the Board to "collect all certification mechanisms and data protection seals and marks in a register and … make them publicly available through any appropriate means." Article 42(8). Accreditation can be up to five years and may be renewed.

[60] Article 42(5).

[61] Article 42(7) and (3).

[62] See, Article 49.

A final derogation is also available but only in very limited circumstances. Where it cannot be based on standard contractual clauses, BRCs, or any of the other derogations, a transfer to a third country or an international organization may take place only if the transfer is "not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data."[63]

In line with the transparency requirements under the EU model, Article 13 of the GDPR requires controllers to provide information to data subjects when their information is obtained, that includes that the controller intends to transfer personal data to a third country or international organization. The notice must state that the transfer is either pursuant to an adequacy decision by the EC or refer to the appropriate or suitable safeguards and the means for the data subject to obtain them. This information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language as required by Article 12.

As to enforcement, violations of the data transfer provisions in Articles 44–49 of the GDPR may result in "administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher."[64] The factors considered in determining the fine include the nature, gravity and duration of the infringement, the intentional character of the infringement, actions taken to mitigate the damage suffered, degree of responsibility or any relevant previous infringements, the manner in which the infringement became known to the supervisory authority, compliance with measures ordered against the controller or processor, adherence to a code of conduct and any other aggravating or mitigating factor.[65]

6. Comparison of the models

This comparison focuses on the key provisions of the GDPR for the EU data transfer scheme and the Framework as the seminal document for CBPR. While the CBPR Assessment Criteria[66] and program requirements required by accountability agents such as Relevant Program Requirements of TrustArc in the US for example,[67] provide more detail as to practical implementation, the focus of the Framework as is discussed in the following sections of this article, is clearly evident in those criteria and in the implementation requirements.

Key aspects of the Framework and the GDPR especially in the context of IoT data, will be examined and compared in more detail the following sections. However, initial overall observations are that:

- The APEC Framework and the GDPR both apply to the processing of personal data by private and public sector organizations.[68] A stated objective of the GDPR is to update data protection for a new era which includes IoT, Big Data, and AI. The Framework on the other hand, which was updated in 2015, refers to technological development,[69] and the Preamble notes the impact of mobile technology, but does not specifically address the aspects covered by the GDPR.
- Both APEC and the EU models aim to facilitate data flows and protect personal data[70] which is defined in substantially the same terms under both the GDPR and the Framework. The facilitation of transborder flows whilst providing appropriate protection is particularly important for IoT data but each scheme has a different conceptual foundation that results in different emphasis. The emphasis in the GDPR is on protection of fundamental rights and freedoms of natural persons, particularly their right to the protection of personal data.[71] This is in line with the EU focus on protecting fundamental rights, whereas the APEC Framework is designed to facilitate transborder data flows, in line with the overarching objective to encourage trade amongst APEC members.[72] This different conceptual basis is reflected in the framing of the APEC data protection standards in terms of reasonableness and/or risk of harm to an individual, akin to a quasi-tortious approach,[73] whereas

[63] See Recital 113 and Article 49 (1).
[64] Article 83(5).
[65] Article 83(2).
[66] APEC Cross-Border Privacy Rules System Program Requirements
[67] TRUSTe, APEC CBPR Program Requirements Map at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx. TrustArc was formerly Trustee.
[68] The Framework has very limited application to what it terms as "publicly available information" which is defined to be information which an individual has made public or permitted to be public and which is legally obtained from public records. See Part II Section 11.
[69] See for example, Preamble Part 1 (2) but also note Part 1 (8) which does not specifically mention technological advances.
[70] See Article 1(1) of the GDPR and Preamble Part 1 (1) of the APEC Framework.
[71] See Article 1(1) of the GDPR.
[72] See APEC, APEC Privacy Framework, Description at https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015) which states that the APEC Privacy Framework "aims at promoting electronic commerce throughout the Asia Pacific region, is consistent with the core values of the OECD's Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (OECD Guidelines), and reaffirms the value of privacy to individuals and to the information society. The previous version of the Framework (2005) was modelled upon the OECD Guidelines (1980) which at that time represented the international consensus on what constitutes fair and trustworthy treatment of personal information. The updated Framework (2015) draws upon concepts introduced into the OECD Guidelines (2013) with due consideration for the different legal features and context of the APEC region."
[73] See APEC Framework Part III Section 20. In this respect the APEC Framework appears to be importing a tortious notion of privacy based on the common law as it applies in a number of APEC jurisdictions. A common law tort of privacy has not historically been recognized, with the tort of confidentiality being invoked (somewhat artificially) in some circumstances to protect individual privacy but there are signs that a new common law tort of privacy is emerging. See, *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 1999, and *Grosse v Purvis* (2003) QDC 751, *Grosse v Purvis* (2003) QDC 751,

the GDPR is based on protection of fundamental human rights. In the EU, mere violation of the human right is all that is required; and the ere is no requirement to prove harm in the traditional tortious sense. The violation of an individual's rights to data protection and/or privacy is itself harm.

- Most of the CBPR Requirements are expressed in terms what is "reasonable,"[74] many are framed in terms of what is "appropriate"[75] (a term also widely used in the GDPR), and some depend on the risk, and type, of harm[76] to the individual. Specific examples are discussed in the following sections of this article, but as a preliminary point it should be noted that there is limited guidance[77] in the Framework, CBPR Assessment Criteria, and Requirements as to the factors to be taken into account when determining reasonableness, appropriateness, and risk. This approach allows for flexibility and scope in interpretation but it can also result in uncertainty and a lack of clarity as to level of protection provided to personal information and individual privacy under CBPR.
- Consideration of basic elements of the GDPR and CBPR as they apply to processing IoT data, clearly reveal that the APEC model is not as comprehensive, nor as detailed as the GDPR.
- Unlike the Framework which is a minimum data protection standard to which organizations are required to adhere to be certified for CBPR, the GDPR is relatively more detailed, and clear, as to specific requirements and those requirements apply directly as law.[78]

The impact of these broad differences between the two models and how they manifest in key elements of relevant to cross border data transfer and the protection of personal data and data subject rights are discussed in the following sections.

6.1. *Personal data*

The E.U. and APEC schemes define personal data broadly and similarly. Both the GDPR, the APEC Privacy Framework basically define personal data as any data about an identified or identifiable individual but the GDPR definition is more detailed, including examples of identifying data as including "in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" A similar definition in the 1995 Directive has been interpreted in the E.U. as applying to data from disparate sources, if when considered collectively, it is capable of identifying natural person.[79] As a consequence, data from a connected IoT device owned by, or provided to, a consumer for example, can readily come within the definition of personal data under the GDPR, thereby attracting protections for individuals and consequential compliance obligations for organizations.

The definitions in both the GDPR and the APEC Framework are however, capable of being interpreted in a more pragmatic way so as to exclude IoT data, unless it is clearly personal data that should be protected. An APEC member nation provides an example of how this can be achieved. In Australia there has been recent narrowing of the broad approach to determining whether information is capable of directly or indirectly identifying a natural person so as to constitute personal information. The Full Court of the Federal Court of Australia has confirmed that information will only be regulated as "personal information" under the federal Privacy Act 1988 (Cth) (Privacy Act) if there is a sufficient connection between the information and an individual so that the information can be said to be about that person.[80] This is a major judicial development of relevance to IoT data and communications that has implications beyond Australia.

The Australian Privacy Act largely follows the EU data protection model and like the GDPR only applies to personal information that is defined on the basis of whether a person is identified or identifiable from the data. Until recently, it has been assumed in Australia, as in the EU and in other nations

[74] TRUSTe APEC CBPR Program Requirements Map, pages 2, 5, 12-14, 24-30, 32, 34, 35, 38, 39, 45, 47, 48 and 50 at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx.

[75] TRUSTe APEC CBPR Program Requirements Map, pages 25, 29, 31, 39, 40, 45-47 and 50 at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx.

[76] TRUSTe APEC CBPR Program Requirements Map, pages 11, 13-15, 18, 30-33 at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx.

[77] Some requirements include more detail. For example, in relation to providing a data subject with access to personal data, the TrustArc requirements state that a "[p]articipant is not required to permit Individual access to Personally Identifiable Information to the extent that: • Such access would prejudice the confidentiality necessary to comply with regulatory requirements, or breach Participant's confidential information or the confidential information of others; • The burden or cost of providing access would be disproportionate or the legitimate rights or interests of others would be violated. However, Participant may not deny access on the basis of cost if the Individual offers to pay the costs of access; or • The requested PII is derived from public records or is Publicly Available Information and is not combined with non-public record or non-publicly available information." See, TRUSTe APEC CBPR Program Requirements Map, page 41 at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx.

[78] This is acknowledged in the TrustArc CBPR program requirements where a participant is asked to acknowledge that "it understands that it has an independent duty to comply with any and all laws and regulations." See TRUSTe APEC CBPR Program Requirements Map, page 41 at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx.

[79] In *Lindqvist v Sweden* [2003] ECRI-12971, ¶ 24 for example, the CJEU provided guidance about what constitutes personal data under the 1995 Directive, the Court stated that personal information "… undoubtedly covers the name of a person in conjunction with telephone coordinates or information about his working conditions or hobbies." In general, the more detail provided, the greater the likelihood that the data will identify a data subject and be considered personal data under the Regulation.

[80] To understand this distinction, the situation outlined by the Deputy President of the Administrative Appeals Tribunal (which heard the case at first instance and who identified the point which eventually decided the case) is instructive. The Deputy President referred to service records for a car she purchased. The information in the records was about the car, and repairs that had been carried out on the car, but was not information about the Deputy President, even though the records may have referred to the registration number of the car and even her name. See also Article 29 Data Protection Working Party Opinion 4/2007.

that have used the EU model, that as long as a person can be identified from data from a range of sources, the data will be considered to be personal for the purposes of the Act. However, the decision of the Full Court of the Federal Court of Australia has rolled back that assumption. In the first significant judicial decision on the meaning of "personal information" in the Act,[81] the Federal Court in *Privacy Commissioner v Telstra Corporation Limited*[82] in a unanimous decision held that data is only personal if a person is the subject the information.[83] The Court rejected the proposition that information from which an individual's identity can reasonably be ascertained is always be personal information, stating that interpretation would make the requirement that the information be "about an individual," redundant. The Court held that the concept of personal information in the Act whilst broad, was "constrained" by the requirements of the definition that the information that must be "about" the individual and that the identity of the individual be apparent, or reasonably ascertainable from the information. The Court gave the example of the color of an individual's mobile phone color and network type (3 G) as being information that the Court did not consider was "about" the data subject. However, the Court noted that "[i]n other circumstances, the conclusion might be different", making it clear that each case will turn on its circumstances.

The decision sets an historic legal precedent in Australia that may influence the interpretation of the definition of personal data in other jurisdictions, to limit the scope of the definition of personal information and hence the application of data protection legislation like the Australian Privacy Act. That Act, like most legislation of its kind in the world, closely follows the EU data protection model including its definitions. The decision means that the Privacy Act will not necessarily extend to information that has no substantive relation to an individual, even if could potentially be traced back to that person. This decision surprised many in Australia especially considering the pro-privacy culture that is now ingrained in that nation, and the long-held view that all information from which an individual's identity can reasonably be ascertained was personal information. While the decision did not specifically concern IoT data, it can be viewed as a pragmatic response to a new era. The broad relevance of this interpretation to the IoT era, is that data that identifies an individual but is not about that individual, would not necessarily be regarded as personal information so as to attract restrictions on processing in legislation like the GDPR, including extraterritorial processing. The advantage is that is this approach does not ensnare all IoT data and could be a first step to developing more considered judicial criteria for achieving an acceptable balance between individual interests and IoT that moves beyond legitimate interest and public interest as the primary legislative grounds of for lawful processing in the absence of data subject consent.

6.2. *Data processing*

The definition of processing in the GDPR covers a wide range of operations and applications including collection, recording, disclosure by transmission and erasure, and specifically includes processing wholly or partly by automated means which is significant for context of IoT. Processing is undefined in the APEC Framework. However, the definition of "personal information controller" in the Framework refers to specific processing activities i.e. "collection, holding, processing, use, disclosure or transfer of personal information." This is a more limited list than those specified in the GDPR in the definition of "processing."

The Unlike the GDPR, the APEC Privacy Framework also generally does not protect personal data that is publicly available,[84] and not collected directly from the data subject.[85] The Framework specifically states that "it may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information"[86] and this approach is reflected in the CBPR Assessment Criteria. This is a very different approach to the GDPR. Article 14 of the GDPR for example, requires that specified information be provided to a data subject when personal information has not been obtained from that person.

The GDPR generally requires under Article 5 (b) that personal data be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[87] Both the GDPR and the Framework have exceptions that permit processing, such as with consent of the data subject, and when necessary to provide a service or product requested by the individual.[88] However, the basic requirements under the Framework are generally less than the GDPR, with the Framework specifying only that collection "be obtained by lawful and fair means, and

[81] The Act currently defines personal information as "information or an opinion, whether true or not, and whether recorded in a material form or not, *about an identified individual,* or *an individual who is reasonably identifiable*." (my emphasis) The definition considered by the Court was the definition prior to the 2014 amendments, so it was "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion."

[82] [2017] FCAFC 4.

[83] The Court did not, however, determine on whether any of the particular information requested which including metadata retained by Telstra, was "personal information" because this issue was not included as specific ground of appeal.

[84] Part 11 defines "publicly available information" to mean "personal information about an individual that the individual knowingly makes or permits to be made available to the public, or that is legally obtained be made and accessed from: a) government records that are available to the public; b) journalistic reports; orc) information required by law to available to the public." The GDPR does not have a similar definition.

[85] See Part 11. Note also however, that 'the GDPR does contain some exceptions such as processing of special categories of personal data that relates to personal data "which are manifestly made public by the data subject" under Article 9 (2) (e).

[86] Part 23.

[87] Article 5(c).

[88] In part 25 c) the Framework specifies another exception to enable collection "by the authority of law and other legal instruments, proclamations and pronouncements of legal effect." If this refers only to public law as seems to be so, this exception is in-line with the approach of the GDPR.

where appropriate, with notice to, or consent of, the data subject."[89] As to data use, the Framework specifies that "personal information collected should be used only to fulfill the purposes of collection *and other compatible or related purposes*."[90] (my emphasis) The commentary indicates that the scope of part 25[91] covers disclosure to a third party and further use. That processing can also be permitted under the GDPR as being necessary for the legitimate interests of a controller but is subject to "the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."[92]

Both the Framework and GDPR cover access and correction. The Framework states that an individual should be able to obtain confirmation from the controller as to personal information held, have access to that information, and be able to challenge its accuracy, and request rectification, additions, amendments and deletions. These rights are subject to a balancing of the burden or expense of compliance, legal or security reasons, protection of commercial information, and protection of the privacy rights of other persons.[93] However in a notable departure from the GDPR and the usual approach under the EU model, the Framework provides that "[t]he details of the procedures by which the ability to access and correct information is provided may differ depending on the nature of the information and other interests. For this reason, in certain circumstances, *it may be impossible, impracticable or unnecessary to change, suppress or delete records*."[94] (my emphasis) The Relevant Program Requirements are broadly reflective of the Framework in that they require that a CBPR participant "implement reasonable and appropriate mechanisms" for data correction, updating, and deletion or a request by the data subject that the collected data no longer be used.[95]

The GDPR also provides for confirmation and access to personal information and for erasure and rectification of the personal data but does so by expressing them as rights of the data subject. Although there is some weighing of the relative interests of controller, processor, and data subject in the GDPR, the Regulation does not express these rights in terms of "reasonableness" in the same way, nor to the extent of the Relevant Program Requirements, for example.[96] The GDPR also provides for access to information about processing including: what categories of data are processed, the recipients of the data, the right to lodge a complaint with a DPA as well as other information specified in Article 41 (2).That other information includes the rights of the data subject, the source of the data, whether the data was subject to automated profiling and if so, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.[97] A detailed discussion of the ramifications of the information required by Article 41 (2) in relation automated processing is outside the scope of this paper, but it is clearly problematical. While information about processing is generally desirable, the requirements in relation to automated processing present compliance difficulties in relation to IoT data processing using AI because of AI's inherently opaque nature. That aspect aside however, the GDPR generally requires provision of more information about data processing and about data subject rights than the Framework, CBPR Assessment Criteria, and the Relevant Program Requirements.

6.3. *Data subject notice and consent*

The APEC Framework has a similar but less strict requirement compared to the GDPR, that data controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information. For example, the language used by the Framework in relation to choice notice, is that "where appropriate", individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal data.[98] There is a provisothat it may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.[99] The Framework states that all reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information, and then provides that, otherwise the notice should be provided as soon after as is practicable.[100] The Relevant Program Requirements reflect this approach, by prefacing the requirement that a Privacy statement be available when the individual engages with the participant with "[a]s reasonable."[101] This approach leaves a lot of scope for uncertainty in practical application. It provides flexibility for data controllers but is not necessarily conducive to fairness and transparency, requirements required under Article 5 of the GDPR as guiding principles for processing of personal data.

The Framework refers to consent but does not contain any further detail or guidance, whereas the GDPR is detailed and prescriptive. Under Article 4 (11) the GDPR, "consent" of the data subject means any freely given, specific, informed and

[89] Part 24.
[90] Part 25. Several exceptions ae listed which generally follow the same approach as the GDPR.
[91] The commentary states: "The use of personal information for "compatible or related purposes" would extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls *by a third party*; or, the use of information collected by an organization for *the purpose of granting credit* for the subsequent purpose of collecting debt owed to that organization." (my emphasis)
[92] Article 6 (1) (f).
[93] Part 30.
[94] See, commentary to part 31 regarding the handling a request by a data subject.
[95] See, for example, TRUSTe APEC CBPR Program Requirements Map, pages 5 and 25 at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx.
[96] See above.
[97] Article 41(1) and (2).
[98] Part 26.
[99] Part 26.
[100] Part 22.
[101] The Relevant Program Requirements state: "As reasonable, Privacy statement must be available when the Individual engages with the Participant, such as through an application, Website homepage or landing page." See, TRUSTe APEC CBPR Program Requirements Map, page 2 at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx.

unambiguous indication of the data subject's wishes by which he or she, by statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[102] The GDPR clarifies that consent will not considered to be freely given if the data subject has no genuine and free choice; or is unable to refuse or withdraw consent without detriment; and where there is a clear imbalance between the data subject and the controller, particularly in relation to a public authority.[103] Relating this to IoT, consent is unlikely to be regarded as freely given if the performance of a contract including the provision of a service, is conditional on the data subject's consent to certain data processing activities which are not necessary for the performance of that contract.[104] Consent also must relate to specific processing operations and should cover all processing activities. The latter requirement can be particularly problematical for IoT devices and data. If the processing has multiple purposes, the consent must be for all those purposes which presents similar difficulties in the IoT context.[105] Consent is presumed to not be freely given if separate consents are not permitted for different data processing when separate consents would be appropriate.[106]

The GDPR further provides that consent "should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement."[107] In a much more prescriptive approach compared to the Framework, the GDPR states that "[S]ilence, pre-ticked boxes, or inactivity should not therefore constitute consent."[108] Pre-formulated consent declarations are required to be accessible and clear and not contain unfair terms;[109] and electronic requests for consents must be clear, concise and not unnecessarily disruptive to the use of the services for which they are provided.[110] Article 7 also states that if consent is given in the context of a written declaration which also concerns other matters, the request for consent must be clearly distinguishable from the other matters, and presented in accessible form, using clear and plain language. While these requirements generally reflect good corporate practice especially when dealing with consumers, under the GDPR a data subject also has the right to withdraw consent at any time[111] which can be challenging from a business management perspective especially in relation to IoT data.[112]

Specific requirements are also laid down by the GDPR for consent in relation to processing special categories of personal data, that are not in the Framework. The Framework does not define this type of data although the term sensitive data is mentioned in the context of "credit card numbers, bank account information or other sensitive personal information."[113] This is a very different approach from the GDPR that defines special categories of personal data, and with limited exceptions, generally prohibits its processing without explicit consent of the data subject unless processing can be justified on one of the other specified lawful grounds. The GDPR definition refers to data consisting of "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation."[114] Explicit consent under the GDPR, requires that the data subject be clearly informed of the use of the data and take an affirmative action to demonstrate consent. The other lawful ground apart from consent is processing in the public interest; and depending on the circumstances, that could apply to IoT data processing.[115] There is also an exception where the data is "manifestly made public by the data subject"[116] which could be applicable in some scenarios.

The Framework does not have equivalent, or even similar, requirements for special categories of personal data nor for explicit consent. The Relevant Program Requirements do refer to "express consent," though that term is not defined and the conditions under which consent is express are not set out. The Requirements base the need for express consent on risk of harm. Establishing what seems to be a relatively high bar of "likely" harm, the Requirements state, for example, that "[e]xpress Consent must be obtained from the Individual prior to the transfer of PII[117] to Third Parties other than Service Providers if an unauthorized use or disclosure or that information would be likely to cause financial, physical, or reputational harm to an Individual."[118] Otherwise controls and processes to protect and manage personal data under the Requirements are to be "[a]ppropriate to the size of the Participant's business; and [a]ppropriate to the level of sensitivity of the data collected and stored." These requirements are expressed jointly apparently taking into account both factors. The obvious point is that business size should not dictate responsibility for data protection; and especially not for protection of what the GDPR defines as special categories of personal data.

6.4. *Data controllers and processors*

Both the GDPR and Framework make the data controller primarily responsible for compliance. The APEC Framework

[102] Unlike the 1995 Directive, the GDPR now specifically addresses consent of child, especially for "information society services" which are defined as any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. See GDPR Articles 8 and 4, and Article 1(1) of EU Directive 2015/1535.
[103] Recitals 42 and 43.
[104] Article 7(4) and Recital 43.
[105] See Recital 32.
[106] Recital 43.
[107] Recital 32
[108] Recital 32.
[109] See, Article 7(2) and Recital 42.
[110] See Recital 32 and Article 7(3
[111] Article 7(3).
[112] Article 7(3). Note that processing remans lawful until consent is withdrawn.
[113] Part 24 which deals with collection limitation.
[114] Article 9(1).
[115] See, Article 9.
[116] Article 9(2) (e).
[117] PII is used by TrustArc in Required Program Requirements to refer to Personally Identifiable Information. PII is the term commonly used in the U.S. to refer to what the EU model including the GDPR and this article refers to as personal data or information.
[118] See, TRUSTe APEC CBPR Program Requirements Map, page 15 at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx.

defines a controller in terms of control of data processing and excludes a natural or legal person who acts under the instructions of another person or organization.[119] The definition of controller in the GDPR is similar but more comprehensive in that it includes joint control and specifically applies to persons and organizations processing the data on behalf of the controller. A controller is defined in the GDPR as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[120] Unlike the Framework, the GDPR also extends accountability to a processor defined as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller,"[121] and sets out responsibilities to protect personal data in accordance with the data protection principles.

There is a fundamental difference in approach to the discharge of responsibilities by controllers (and processors) under the Framework and GDPR that is especially apparent in relation to data transfers that are especially important for IoT data processing. The Framework requires that the controller undertake due diligence if personal information is to be transferred to another person or organization, domestically or internationally. In the absence of data subject consent,[122] the controller is to "exercise due diligence and take reasonable steps" to ensure that the recipient will protect the information consistently with the principles in the Framework.[123] The accompanying commentary, however, makes the point that "[t]here are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between the personal information controller and the third party to whom the information is disclosed." This is reflected in the Relevant Program Requirements which set out basic responsibilities of a CBPR participant to take "reasonable steps to ensure that Service Providers" abide by applicable privacy policies.[124] In contrast, the GDPR requires processing in accordance with the data protection principles in Article 5, none of which are couched in terms of reasonableness. Additionally, as discussed earlier, generally in the absence of consent of the data subject, personal data can only be transferred to another country under an adequacy decision, or using compliance mechanisms that under the GDPR include standard contractual clauses, BCRs, binding agreements combined with an approved code of conduct, and certification.

6.5. *Data protection and security*

Both the Framework and the GDPR adopt a risk-based approach to data protection and security, however they are fundamentally different. The differences are important for IoT data processing.

The stated purpose of the Framework is to "prevent misuse" of personal data. Misuse is not defined but the objective is that considering "the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information."[125] The Framework states that controllers should protect personal information with appropriate safeguards against risks like loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. This is expressed in the Relevant Program Requirements as: "[t]he Participant must implement *reasonable* procedures to protect PII *within its control* from unauthorized access, use, alteration, disclosure, or distribution."[126] (my emphasis)

"Reasonableness" is evident throughout the Requirements. Another example is that a Participant must "implement *reasonable procedures to protect PII within its control* from unauthorized access, use, alteration, disclosure, or distribution."[127] (my emphasis) The questions are- reasonable to whom or what; and judged under what criteria? In addition to reasonableness, the Requirements use a risk-based/ harm approach that generally reflects the Framework. For example, the Requirements state that Participants are required to "[u]se *reasonable* encryption methods for transmission of information across wireless networks, and storage of information *if the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual*." (my emphasis) The requirement for a Participant to "utilize encryption such as Secure Socket Layer for the transmission of information" is couched in terms of risk i.e. if "*the inappropriate use or disclosure of that information could cause financial, physical, or reputational harm to an individual*."[128] Even the requirement that access "to PII or Third Party PII retained by Participant must be at least restricted by username and password, is subject to the proviso"if the inappropriate use or disclosure of that information

[119] The definition includes a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf, but excludes a person or organization who performs such functions as instructed by another person or organization.

[120] Article 4 (7).

[121] Article 4 (8).

[122] The Relevant Program Requirements in relation to Criteria 10, 11 and 12 state that "[e]xpress Consent must be obtained from the Individual prior to the transfer of PII to Third Parties other than Service Providers *if an unauthorized use or disclosure or that information would be likely to cause financial, physical, or reputational harm to an Individual*." (my emphasis)

[123] Part 32. See also commentary in relation to part 10. This reasonableness requirement is reflected in the Relevant Program Requirements. In relation to Criteria 33 for example, the Requirements state that a "[p]articipant must implement *reasonable* procedures to protect PII within its control from unauthorized access, use, alteration, disclosure, or distribution." (my emphasis)

[124] See for example, TRUSTe APEC CBPR Program Requirements Map, page 27 at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx.

[125] Part 20.

[126] See, for example TRUSTe APEC CBPR Program Requirements Map, page 29 at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx.

[127] See, TRUSTe, APEC CBPR Program Requirements Map page 29 at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx.

[128] See, TRUSTe, APEC CBPR Program Requirements Map page 30 at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx.

could cause financial, physical, or reputational harm to an individual."[129] This approach is in stark contrast to the GDPR.

The GDPR similarly requires that personal data be protected but specifically requires the use of "appropriate technical or organizational measures," to protect against "unauthorized or unlawful processing and against accidental loss, destruction or damage."[130] This is a broader requirement than the Framework, Assessment Criteria and the Requirements. The GDPR does contain limitations based on reasonableness, or harm. The GDPR also sets out a list of the type of risks involved in processing personal data which go beyond what would usually be considered misuse as used in the Framework.

Like the Framework, the GDPR requires that controller implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk but the GDPR also extends this requirement to processors and this is an important distinction, especially for IoT data. The GDPR requires that controllers and processors take into account "the state of the art", the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.[131] The factors to be considered by the controller and processor specifically include pseudonymizing and encryption of personal data; ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and the process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the data processing.[132] Article 32 (3) requires that controller and processor "take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process (the data) except on instructions from the controller…"[133] The GDPR also requires the appointment of a "data protection officer" i.e. "a person with expert knowledge of data protection law and practices to assist the controller or processor to monitor internal compliance. The Framework in the commentary regarding Accountability merely states that "[a] useful means for a personal information controller to help ensure accountability for the personal information it holds, is to have in place a privacy management programme."[134]

Overall the Framework is much less detailed and prescriptive; and is generally less comprehensive in managing and protecting personal data and individual privacy than the GDPR. Unlike the Framework, the GDPR frames security in terms of risk to data subjects and their rights, not just risk to the data.

6.6. *Data breaches*

There is substantial divergence between the Framework and GDPR in relation to a personal data breach and this is significant for IoT data processing considering the high-degree of connectiveness that characterizes the IoT era and hence the heightened risk for harm to individuals in the event of a data breach.

While neither the Framework, the CBPR Assessment Criteria, nor the Relative Program Requirements contain a definition, the GDPR states that a personal data breach means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed."[135] The GDPR requires assessment of data incidents and clear notification "without undue delay" of breach to data subjects when there is a high risk to the rights and freedoms of natural persons.[136] Notification to data subjects is not required if the controller has implemented appropriate technical and organizational protection measures, and those measures were applied to the data affected by the personal data breach. The GDPR specifically refers to measures that render the data unintelligible to any person who is not authorized to access it such as encryption; and when the controller has taken subsequent measures which ensure that the high risk for the rights and freedoms of data subjects is no longer likely to materialize; or it would involve disproportionate effort.[137] In such a case, however there must be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.[138] Notification of supervisory authorities within 72 h is required when the breach is likely to result in a risk to the rights and freedoms of natural persons.[139]

The APEC framework in its primary principles relating to controllers does not specifically address data breaches. Only the commentary on part 20 relating to "Preventing Harm" states that, "[w]here there has been a significant security breach affecting personal information, *it may help* to reduce the risk of harmful consequences to the individuals concerned to give notice to Privacy Enforcement Authorities and/or the individuals concerned." (my emphasis). The CBPR Assessment Criteria requires that personal information processors, agents, contractors, or other service providers to whom personal information is transferred, promptly notify the data controller of a data breach.[140] The Relevant Program Requirements

[129] See above.
[130] Article 32(1).
[131] See, Article 32.
[132] Article 32 (1). Article 32 (3) provides that "[a]dherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance."
[133] Unless he or she is required to do so by Union or Member State law.
[134] Part 32.
[135] Article 4 (12).
[136] Article 34 (1) and (2).
[137] See, Article 34 (3).
[138] See, Article 34 (3) (c).
[139] Article 33(1).
[140] See, APEC Cross-Border Privacy Rules System Program Requirements, 35 a). Question 35.c) however does ask if immediate steps are taken to correct/address the security failure which caused the privacy or security breach. The Requirements state that "[t]he Accountability Agent must verify that the Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is

contain a general requirement that a CBPR participant "take reasonable steps to ensure" that its Service Providers with whom it shares personal information abide by privacy policy; and "abide by the rights and obligations attached to the PII by the Participant regarding the security, confidentiality, integrity, use, and disclosure of the PII." The US Accountability Agent, TrustArc, further requires that equivalent obligations also be imposed on third party service providers, and that third-party service providers provide notice to the Participant of "any data breach, including leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information."[141] Although the latter is a step in the right direction, overall these requirements are nowhere near those of the GDPR and are not adequate.

The CBPR also does not require that member countries impose mandatory notification breach to privacy enforcement authorities or data subjects, requiring only that member nations impose rules that data controllers contractually require notification by data processors, agents, contractors and other service providers to the data controller. This is a major deficiency in any event but it can be especially impactful when IoT data is involved.

In the section in the Framework under "Guidance for Domestic Implementation" the guidance is very general i.e. that a member economy "should *consider encouraging or requiring* personal information controllers to provide notice, *as appropriate, to Privacy Enforcement Authorities and/or other relevant authorities in the event of a significant security breach* affecting personal information under its control. *Where it is reasonable to believe that the breach is likely to affect individuals, timely notification directly to affected individuals should be encouraged or required, where feasible and reasonable.*"[142] (my emphasis).

Overall in relation to data breaches, the APEC Framework, CBPR Assessment Criteria, and the Relevant Program Requirements are out of step with the GDPR, and with what is generally regarded as good practice, specifically the need to assess and mitigate damage in the event of a breach, and to promptly notify affected data subjects and the authorities.

6.7. Summary

Review of the EU and APEC models in relation to aspects pertinent to IoT data processing reveals that while there are similarities in terminology and in general approach, basic objectives and standards differ. Comparison shows that the APEC Framework lacks the particularity, clarity, and guidance required for a standard of this nature; and that it does not generally meet the standard set by GDPR.

As even a minimum standard, the Framework, CBPR Assessment Criteria and the Relevant Program Requirements collectively, do not accord with widely- accepted good practice in not directly applying to data processors, and in not requiring the appointment of a Data Protection Officer. The Framework is notably deficient in the lack of specificity as to collection practices particularly what constitutes free and informed consent, in not addressing the need to provide additional protection to what the GDPR defines as special categories of personal data especially health data, genetic data and biometric data; and in relation to security and breach mitigation and notification. While corporations certified under CBPR can include these aspects to comply with domestic law, as part of their internal governance standards and procedures, or to meet additional management standards independently required by an Accountability Agent, the point is that the Framework, Assessment Criteria and Requirements which collectively constitute the regional standard and the basis of CBPR, are lacking in these important respects. In many respects neither the Framework, the CBPR Assessment Criteria nor the Relevant Program Principles provide the level of data and privacy protection required under the EU regulations; and in some respects, such as for encryption for example, the approach adopted is markedly out of alignment with the GDPR and usual practice.

Of course, proponents of CBPR assert that the EU approach is too focused on data protection and privacy to the point where compliance risks stymying cross border data flows and hence the development of IoT devices, data processing, and communications. While there is no doubt that the EU is concerned to protect personal data and individual privacy, a human rights foundation and approach generally provides conceptually sound basis for balancing competing interests. The need to weigh individual rights with the broader societal impact is an inherent part of human rights law and its application. While the ePrivacy Regulation as currently does potentially presents difficulty for IoT data communications, the GDPR can be interpreted and applied proposed so as to effectively balance competing interests and it contains a range of data transfer mechanisms that can be employed to transfer data, including IoT data, whilst also adequately protecting individual rights and interests.

7. Conclusion

The IoT era highlights the need for effective mechanisms to facilitate international data flows, whilst protecting personal data. Although IoT offers many benefits for individuals and businesses, there are clearly concomitant data protection and individual privacy risks, especially when data is transferred across borders. Given the concern by corporations that process data around the world, to streamline compliance, the threshold question explored in this article is which scheme more effectively achieves this balance particularly in the context of the IoT data processing.

---

transferred, to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness."

[141] In relation to Assessment Criteria 35. In relation to Criteria 35, the Requirements state that "Participant must take reasonable steps to ensure that it's Service Providers with whom it shares PII either: o Abide by Participant's privacy policies as reflected in Participant's Privacy Statement; or o Abide by privacy policies that are substantially equivalent to Participant's privacy policies as reflected in Participant's Privacy Statement; and o Abide by the rights and obligations attached to the PII by the Participant regarding the security, confidentiality, integrity, use, and disclosure of the PII." See, TRUSTe APEC CBPR Program Requirements Map, page 36 at http://www.cbprs.org/GeneralPages/APECCBPRSystemDocuments.aspx.

[142] Part 54.

As discussed, the are some broad similarities but there are also notable differences conceptual basis and in objectives, guidance, and requirements. There is significant difference in the overall standard of data protection and individual privacy under the two schemes.

CBPR is a mechanism that facilitates trade within the APEC region. Japan for instance, automatically permits international transfers by corporations that have CBPR approval whereas other corporations must first obtain consent under the Act on the Protection of Personal Information 2003 (PPIA). However, it is questionable whether the Framework lives up to the intention set out in Part 1 (7) i.e. "….to provide clear guidance and direction to businesses and government entities in APEC economies on common privacy issues and the impact of privacy issues upon the way legitimate business practice and government functions are to be conducted." The Framework goes on to state that "[i]t does so by highlighting the reasonable privacy expectations of the modern consumer,"[143] but this is doubtful. As examination of the scheme reveals, there are key areas where the Framework does not provide clear and sufficient guidance and does not reflect what is presently considered good practice.

In comparison, the EU model has a relatively high degree of particularity and guidance. Some aspects of the GDPR are concerning, such as the technical and legal implications of reliance on data anonymization and pseudonymization when they are not yet capable of providing the necessary protection from identification or re-identification of data subjects. Overall though, the basic approach to data protection is sound; and the GDPR provides a range of mechanisms which can be adapted to a variety of data transfer situations applicable to IoT data and communications.

The APEC scheme facilitates data flows amongst APEC members including the US which is not considered to have domestic data protection law that satisfies the EU adequacy requirements. It is questionable whether the Framework strikes the right balance between trade objectives and adequate personal data and individual privacy protection at this time. In comparison with the Framework, CBPR Assessment Criteria and the Relevant Program Requirements, the EU regulations that make up the suite of data protection requirements, are more focused on ensuring adequate protection of personal information and the rights of the individual data subject. This is sometimes at the expense of the business imperatives, which is perhaps most apparent in the proposed ePrivacy Regulation in its application to IoT data communications; and in the GDPR in relation to automated decisions, and the right of data subjects to withdraw consent at any time. In comparison, however, the Framework, Assessment Criteria and the Requirements are basic, indeed too basic to ensure protection to the standard required by the GDPR, nor in some respects, to generally accepted business standards.

As to whether one model is likely to prevail, while both the GDPR and the Framework have the potential to better balance business and trade objectives with individual rights though pragmatic interpretation and application, the GDPR is generally better positioned to do so for the IoT era. The GDPR compliance mechanisms enable processing of personal data as part of IoT operations by organizations while providing a high standard of protection to personal data and privacy. The EU will likely continue to set the international model for data protection legislation. There are already indications of changes similar to those in the GDPR being incorporated into the domestic legislation of nations outside the EU. Nations are likely to implement similar data protection requirements, extraterritorial reach, data transfer mechanisms, and adequacy requirements which over time will lead to greater convergence in national data protection standards including in APEC member nations[144] and increased opportunity for mutual recognition of adequacy.

Even for a country like the US where enactment of equivalent domestic data protection legislation is unlikely in the short term, the extraterritorial reach of the GDPR is resulting in US organizations especially those likely to be caught by the GDPR, incorporating GDPR requirements and standards into their global corporate compliance policy and procedures. As a consequence, whether by law or through practice, the EU model especially the GDPR will in the author's view continue to set the international data protection standard.

Acknowledgement

This material is based upon work supported by the National Science Foundation under Grant no. IIP-1362046 and the industry affiliates of the Security and Software Engineering Research Center (S2ERC). The views and analysis provided are entirely our own and not attributable to any other party. Support for this work includes funding from the S2ERC affiliate Cisco Systems Inc. Payments are made to Georgetown University and the funds are used to cover the expenses of the study and related academic and research activities of the institution. The author also acknowledges the assistance provided the U.S Department of Commerce and TrustArc Inc in providing background information for this article.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.clsr.2019.05.004.

[143] See above. The statement continues: "Businesses and member economies should respect individuals' privacy interests in a way that is consistent with the Principles outlined in the Framework."

[144] As mentioned earlier in this article, this is being observed in some APEC nations such as Japan and South Korea for example.