EXPLORING THE RELATIONSHIPS BETWEEN PRIVACY BY DESIGN SCHEMES AND PRIVACY LAWS: A COMPARATIVE ANALYSIS

Atheer Aljeraisy
School of Computer Science and Informatics
Cardiff University, UK
aljeraisya@cardiff.ac.uk

Masoud Barati
Department of Computer and Information Science
Cardiff University, UK
BaratiM@cardiff.ac.uk

Omer Rana
School of Computer Science and Informatics
Cardiff University, UK
RanaOF@cardiff.ac.uk

Charith Perera
School of Computer Science and Informatics
Cardiff University, UK
PereraC@cardiff.ac.uk

July 29, 2020

ABSTRACT

Internet of Things (IoT) applications have the potential to derive sensitive information about individuals. Therefore, developers must exercise due diligence to make sure that data are managed according to the privacy regulations and data protection laws. However, doing so can be a difficult and challenging task. Recent research has revealed that developers typically face difficulties when complying with regulations. One key reason is that, at times, regulations are vague, and could be challenging to extract and enact such legal requirements. In our research paper, we have conducted a systematic analysis of the data protection laws that are used across different continents, namely: (i) General Data Protection Regulations (GDPR), (ii) the Personal Information Protection and Electronic Documents Act (PIPEDA), (iii) the California Consumer Privacy Act (CCPA), (iv) Australian Privacy Principles (APPs), and (v) New Zealand's Privacy Act 1993. In this technical report, we presented the detailed results of the conducted framework analysis method to attain a comprehensive view of different data protection laws and highlighted the disparities, in order to assist developers in adhering to the regulations across different regions, along with creating a Combined Privacy Law Framework (CPLF). After that, we gave an overview of various Privacy by Design (PbD) schemes developed previously by different researchers. Then, the key principles and individuals' rights of the CPLF were mapped with the privacy principles, strategies, guidelines, and patterns of the Privacy by Design (PbD) schemes in order to investigate the gaps in existing schemes.

***K*eywords** Internet of Things, Privacy Laws, Software Design, Security and privacy, Human and societal aspects of security and privacy

1 Report Structure

The technical report contains five sections and is structured as follows: Section 1 presents paper structure. Section 2 presents the key definitions of the selected data protection laws. Section 3 shows the detailed results of the key principles and individuals' rights that resulted from the analysis process (i.e., Combined Privacy Law Framework (CPLF)). Section 3 shows the detailed results of the Combined Privacy Laws Framework (CPLF) using framework analysis. Section 4 presents various Privacy by Design (PbD) schemes (e.g., privacy principles, strategies, guidelines, and patterns) that developed previously by different researchers. In Section 5, the correlation of the principles and rights of the CPLF and the principles, strategies, guidelines, and patterns of the PbD schemes are demonstrated.

2 Key Definitions

This section articulates various definitions of different terms that are used in the regulations of the data protection laws of General Data Protection Regulations (GDPR) [1], the Personal Information Protection and Electronic Documents Act (PIPEDA) [2, 3], California Consumer Privacy Act (CCPA) [4], Australian Privacy Principles (APPs) [5, 6], and the New Zealand Privacy Act (1993) [7, 8].

2.1 Personal Data

- **GDPR:** 'Personal Data' means 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, 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';
- **PIPEDA:** 'Personal Data' is defined under PIPEDA as 'Personal Information' that includes 'any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as: age, name, ID numbers, income, ethnic origin, or blood type; opinions, evaluations, comments, social status, or disciplinary actions; and employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or services, or change jobs)'.
- **CCPA:** 'Personal Data' is defined under CCPA as 'Personal information' that means 'information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household'.
- **APPs:** "Personal Data' is defined under the APPS as 'Personal Information' which means 'any information or an opinion about an identified individual, or an individual who is reasonably identifiable:
  - whether the information or opinion is true or not; and
  - whether the information or opinion is recorded in a material form or not'.
- **New Zealand Privacy Act 1993:** 'Personal Data' is defined under the Privacy Act as 'Personal Information' which means 'information about an identifiable individual'.

2.2 Data Subject

- **GDPR:** 'Data Subject' means 'an identifiable natural person who can be identified directly or indirectly'.
- **PIPEDA:** 'Data Subject' is defined under PIPEDA as 'Individuals'.
- **CCPA:** 'Data Subject' is defined under CCPA as "Consumer" which means 'a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier'.
- **APPs:** 'Data Subject' is defined under APPS as 'Individuals', which means 'a natural person'.
- **New Zealand Privacy Act 1993:** 'Data Subject' is defined under the Privacy Act 1993 as 'Individuals', which means 'a natural person'.

2.3 Processing

- **GDPR:** 'processing' means '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';

- **PIPEDA:** 'Processing' under PIPEDA would include the use, collection, disclosure, alteration, storage or destruction of personal information.
- **CCPA:** 'Processing' is defined under CCPA 'as any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means. These operations would include collection and selling that are defined as:
  - 'Collects,' 'collected,' or 'collection' means buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior.
  - 'Sell, 'selling,' 'sale,' or 'sold,' means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration'.
- **APPs:** 'Processing' under APPS would include 'collection', 'deal', 'use', and 'disclose'.
  - 'Collection' is 'applied broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means'.
  - 'Use' is not defined in the Privacy Act. 'An APP entity 'uses' information where it handles or undertakes an activity with the information, within the entity's effective control'.
  - 'Disclose' is not defined in the Privacy Act. 'An APP entity 'discloses' personal information where it makes it accessible to others outside the entity and releases the subsequent handling of the information from its effective control'.
- **New Zealand Privacy Act 1993:** 'Processing' under The Privacy Act 1993 would include 'collect', 'use', and 'disclose'.

2.4 Controller

- **GDPR:** 'Controller' means '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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law';
- **PIPEDA:** 'Controller' is referred under PIPEDA to 'organizations' which means 'private sector organizations that are not federally regulated. It does not apply to organizations that do not engage in commercial, for-profit activities'.
- **CCPA:** 'Controller' is referred under CCPA to 'business', which means 'a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that does business in the State of California , and that satisfies one or more of the following thresholds:
  1. Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.
  2. Alone or in combination, annually buys, receives for the business' commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.
  3. Derives 50 percent or more of its annual revenues from selling consumers' personal information'.
- **APPs:** 'Controller' is referred under APPS to 'App entity', which defined to be an 'agency' or 'organization' which means 'an individual (including a sole trader), a body corporate, a partnership, any other unincorporated association, or a trust, unless it is a small business operator, registered political party, State or Territory authority or a prescribed instrumentality of a State'.
- **New Zealand Privacy Act 1993:** 'Controller' is referred under The Privacy Act 1993 to 'agency', which means 'any person or body of persons, whether corporate or unincorporated, and whether in the public sector or the private sector; and, for the avoidance of doubt, includes a department'.

2.5 Processor

- **GDPR:** 'processor' means 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller';
- **PIPEDA:** 'Processor' is referred under PIPEDA to 'organizations'.

- **CCPA:** 'Processor' is referred under PIPEDA to 'business'.
- **APPs:** 'Processor' is referred under APPS to 'App entity', which defined to be an "agency" or "organization".
- **New Zealand Privacy Act 1993:** 'Processor' is referred under the Privacy Act 1993 to an 'agency'.

3 Result

This section presents the result of a high-level comparison of various data protection laws, which are: General Data Protection Regulations (GDPR) [1], the Personal Information Protection and Electronic Documents Act (PIPEDA) [2, 3], California Consumer Privacy Act (CCPA) [4], Australian Privacy Principles (APPs) [5, 6], and the New Zealand Privacy Act (1993) [7, 8], through a framework analysis method according to our research paper to attain a comprehensive view of various data protection laws and highlight the disparities. This will assist developers in adhering to the regulations across different regions.. The analysis of the Combined Privacy Laws Framework (CPLF) [1] is based on the principles and rights.

Table 1: Transparency Principle

Definition: *The organisation must provide detailed information on its policies and procedures concerning the management of personal information, and this must be readily available to the public.*

GDPR	Article 5 and Recital 39	*lawfulness, fairness and transparency*
	'Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject', where '(39) The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used'. (39) The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used.	
PIPEDA	Principle 8	*Openness*
	'An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available'.	
CCPA	-	-
	Not mentioned explicitly as a principle or right, but it says in the introduction that: 'Our desire for privacy controls and transparency in data practices is heightened'.	
APPS	App1	*Open and transparent management of personal information*
	'Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy'.	
New Zealand	Principle 3	*Collection of information from subject*
	'Agencies should be open when collecting information.... The best way to do this is usually with a clear privacy statement'.	

[1] Combined Privacy Laws Framework refers to the selected data protection laws for this study.

Table 2: Purpose Limitation Principle

Definition: *The purposes that the personal information is being collected and is used for must be shared by the organization, either prior to or at the time it is collected.*

GDPR	Article 5	*Purpose Limitation*
	'Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes';	
PIPEDA	Principle 2	*Identifying Purposes*
	'The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection'.	
CCPA	1798.100. (b)	-
	'A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section'.	
APPS	App 6	*Use or disclosure of personal information*
	6.12 'The purpose for which an APP entity collects personal information is known as the 'primary purpose' of collection. This is the specific function or activity for which the entity collects the personal information'.	
New Zealand	Principle 1	*Purpose for collection of personal information*
	'Agencies need to carefully consider the purpose for which they collect personal information'.	

Table 3: Limiting Use and Disclosure Principle

Definition: *An organisation may only use or disclose personal information for the purposes for which it was collected.*

GDPR	Article 5	*Purpose limitation*
	'Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes'	
PIPEDA	Principle 5	*Limiting Use, Disclosure, and Retention*
	'Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected'.	
CCPA	1798.100. (b) and 1798.120.(b)	-
	1798.100. (b) 'A business shall not ..... use personal information collected for additional purposes without providing the consumer with notice consistent with this section'. 1798.120.(b) 'A business that sells consumers' personal information to third parties shall provide notice to consumers, pursuant to subdivision (a) of Section 1798.135, that this information may be sold and that consumers have the "right to opt-out" of the sale of their personal information'.	
APPs	App 6	*Use or disclosure of personal information*
	'An APP entity can only use or disclose personal information for a purpose for which it was collected (known as the 'primary purpose'), or for a secondary purpose if an exception applies'.	
New Zealand	Principle10 - 11	*10 + 11: Limits on use and disclosure of personal information*
	P10: 'Agencies must use personal information for the same purpose for which they collected that information'. P11: 'Agencies can only disclose personal information in limited circumstances. One example is where another law requires them to disclose the information'.	

Table 4: Data Minimisation Principle

Definition: *Where personal data is required, it must be relevant, adequate and limited only to what is needed for the purpose stated.*

GDPR	Article 5	*Data Minimisation*
	'Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.	
PIPEDA	Principle 4	*Limiting Collection*
	'The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means'.	
CCPA	1798.100. (b)	-
	'A business shall not collect additional categories of personal information ... for additional purposes without providing the consumer with notice consistent with this section'.	
APPS	App 3	*Collection of solicited personal information*
	'An agency may collect personal information that is 'directly related to' one or more of the agency's functions or activities (APP 3.1). To be 'directly related to', a clear and direct connection must exist between the personal information being collected and an agency function or activity (APP 3.16)'.	
New Zealand	Principle 1	*Purpose for collection of personal information*
	'Personal information must only be collected when: the collection is for a lawful purpose, connected with what the agency does, and it's necessary to collect the information for that purpose'.	

Table 5: Consent Principle

Definition: *The individual's consent is required for the collection, use, and/or disclosure of their personal information.*

GDPR	Recital 11 - Article 7 – Article 8	*Conditions for consent - Conditions applicable to child's consent ...*
	'consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'; 'Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data'. 'Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child'.	
PIPEDA	Principle 3	*Consent*
	'Organizations are generally required to obtain meaningful consent for the collection, use and disclosure of personal information'. 'To make consent meaningful, people must understand what they are consenting to'. 'Consent and children: Obtain consent from a parent or guardian for any individual unable to provide meaningful consent themselves (the OPC takes the position that, in all but exceptional'	
CCPA	1798.120. (c) - 1798.120. (d)	-
	1798.120. (c) 'A business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited, pursuant to paragraph (4) of subdivision (a) of Section 1798.135, from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information'. 1798.120. (d) 'Notwithstanding subdivision (a), a business shall not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, has affirmatively authorized the sale of the consumer's personal information'.	
APPS	Chapter B	*Key concepts*
	B.35 'Consent means 'express consent or implied consent' (s 6(1)). The four key elements of consent are: the individual is adequately informed before giving consent, the individual gives consent voluntarily, the consent is current and specific, and the individual has the capacity to understand and communicate their consent'. B.48 'An APP entity should generally seek consent from an individual for collection and proposed uses and disclosures of personal information at the time the information is collected'. B.57 'As a general principle, an individual under the age of 18 has capacity to consent when they have sufficient understanding and maturity to understand what is being proposed. In some circumstances, it may be appropriate for a parent or guardian to consent on behalf of a young person'.	
New Zealand	Principle 3	*Collection of information from subject*
	N/A New Zealand's Privacy Act does not require the agency to obtain an individual's consent, however, 'agencies must take reasonable steps to ensure that the person they are collecting information from is aware'.	

Table 6: Lawfulness of processing Principle

Definition: *Personal information must be processed by fair and lawful means.*

GDPR	Article 6	*Lawfulness of Processing*
	'Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by 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'.	
PIPEDA	Principle 4	*Limiting Collection*
	'Information must be collected by fair and lawful means. This requirement is intended to prevent organizations from collecting information by misleading or deceiving about the purpose'.	
CCPA	-	-
	Not mentioned explicitly, but it can be inferred from 1798.105. (d): 'A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to.....: (9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information'.	
APPS	App 3	*Collection of solicited personal information*
	'An APP entity must collect personal information 'only by lawful and fair means' (APP 3.5). This requirement applies to all APP entities'.	
New Zealand	Principle 4	*Manner of collection of personal information*
	'Personal information must not be collected by unlawful means or by means that are unfair or unreasonably intrusive in the circumstances'.	

Table 7: Accuracy Principle

Definition: *Attempts must be made to ensure that personal information is as accurate, complete and up-to-date as possible to ensure it satisfies the purposes for which it will be used.*

GDPR	Article 5	*Accuracy*
	Attempts must be made to ensure that personal information is as accurate, complete and up-to-date as possible to ensure it satisfies the purposes for which it will be used.	
PIPEDA	Principle 6	*Accuracy*
	'Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used'.	
CCPA	-	-
	N/A	
APPS	App 10	*Quality of personal information*
	'An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure'.	
New Zealand	Principle 8	*Accuracy, etc, of personal information to be checked before use*
	'Before it uses or discloses personal information, an agency must take reasonable steps to check that information is accurate, complete, relevant, up to date and not misleading'.	

Table 8: Storage Limitation Principle

Definition: *Personal information must not be stored for longer than necessary once it has met the purposes for which it was collected.*

GDPR	Article 5	*Storage limitation*
	‘Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject’.	
PIPEDA	Principle 5	*Limiting Use, Disclosure, and Retention*
	‘Personal information must only be kept as long as required to serve those purposes. Destroy, erase or anonymise any personal information that your organization no longer needs’.	
CCPA	1798.140.	-
	Not mentioned as a requirement for the businesses, however, Service provider and third party are ‘[prohibited] from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business’.	
APPS	App 11	*Security of personal information*
	11.3 ‘An APP entity must take reasonable steps to destroy or de-identify the personal information it holds once the personal information is no longer needed for any purpose for which the personal information may be used or disclosed under the APPs’.	
New Zealand	Principle 9	*Agency not to keep personal information for longer than necessary*
	‘An agency that holds personal information must not keep that information for longer than is necessary for the purposes for which the information may be lawfully used’.	

Table 9: Security Principle

Definition: *Safeguarding procedures must be in place to protect personal information and prevent its loss, misuse or disclosure.*

GDPR	Article 5 – A 33	*integrity and confidentiality - Notification of a personal data breach ...*
	‘Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. ‘In the case of a personal data breach the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it notify the personal data breach to the supervisory authority’.	
PIPEDA	Principle 7	*Safeguards - What you need to know about mandatory reporting of breaches ...*
	‘Personal information must be protected by appropriate security relative to the sensitivity of the information’. ‘Organizations subject to the (PIPEDA) will be required to: report to the Privacy Commissioner of Canada breaches of security safeguards involving personal information that pose a real risk of significant harm to individuals, notify affected individuals about those breaches, and keep records of all breaches’ [9]	
CCPA	-	-
	Not mentioned explicitly, but it can be inferred from 1798.140. (h) (1) that business that uses deidentified information must have “implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.” Existing law requires a business or person that suffers a breach of security of computerized data that includes personal information, as defined, to disclose that breach, as specified.	
APPS	App 11	*Security of personal information - Australian entities and the EU GDPR*
	‘An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorized access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances’. ‘A notifiable data breaches scheme requires APP entities to provide a statement to the Commissioner notifying of an eligible data breach as soon as practicable after the entity becomes aware of the breach. It also requires entities to notify affected individuals as soon as practicable after preparing the statement for the Commissioner’[10].	
New Zealand	Principle 5	*Storage and security of personal information - Do we have to report data breaches?*
	‘It’s impossible to stop all mistakes. But agencies must ensure that there are reasonable safeguards in place to prevent loss, misuse or disclosure of personal information’. ‘Breach notification is voluntary but that is likely that will change with privacy law reform. The Government has indicated that a mandatory requirement to report data breaches is going to be part of the changes made in a new Privacy Act’ [11].	

Table 10: Accountability Principle

Definition: *An organisation is responsible for complying with all data protection laws concerning the personal information that is under its control, and it must appoint someone to be accountable for complying with the law in this area.*

GDPR	Article 24 - Article 37	*Accountability - Designation of the data protection officer*
	'The controller shall be responsible for, and be able to demonstrate compliance with, [law].' 'The controller and the processor shall designate a data protection officer [in any of the specified cases]'.	
PIPEDA	Principle 1	*Accountability*
	'An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles'. 'The Privacy Officer should establish a program that demonstrates compliance by mapping the program to applicable legislation'.	
CCPA	1798.155. (a)	-
	'Any business or third party may seek the opinion of the Attorney General for guidance on how to comply with the provisions of this title'.	
APPS	App 1	*Open and transparent management of personal information*
	1.4 'An APP entity must take reasonable steps to implement practices, procedures and systems that will ensure it complies with the APPs and any binding registered APP code, and is able to deal with related inquiries and complaints'. 10: 'Privacy Officer: An agency must, at all times, have a designated Privacy Officer. An agency may have more than one Privacy Officer'.	
New Zealand	-	*23 Privacy Officer*
	'It shall be the responsibility of each agency to ensure that there are, within that agency, 1 or more individuals whose responsibilities include: (a) the encouragement of compliance, by the agency, with the information privacy principles. (b) dealing with requests made to the agency pursuant to this Act. (c) working with the Commissioner in relation to investigations conducted pursuant to Part 8 in relation to the agency. (d) otherwise ensuring compliance by the agency with the provisions of this Act'.	

Table 11: Anonymity and Pseudonymity Principle

Definition: *Individuals must be given the option of not identifying themselves, or the choice of using a pseudonym, in relation to certain matters.*

GDPR	Article 32	*Security of processing*
	Not mentioned for the purpose of dealing with an organisation, but mentioned under security of processing: 'the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data'	
PIPEDA	-	-
	Not mentioned for the purpose of dealing with an organisation, but mentioned in the case and principles of storage limitation: 'Destroy, erase or anonymise any personal information that your organization no longer needs'.	
CCPA	1798.140	-
	It is not mentioned clearly, however, the CCPA referred the 'Pseudonymise' or 'Pseudonymisation' to 'the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer'.	
APPS	App 2	*Anonymity and pseudonymity*
	'App2 Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym'.	
New Zealand	-	-
	N/A	

Table 12: Source Principle

Definition: *Unless there is an exception, personal information must be collected from the person the information is about.*

GDPR	Article 14	*Information to be provided where personal data have not been obtained ...*
	2. '. . . , the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject: . . . (f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources';	
PIPEDA	Principle 4	*Limiting Collection*
	'Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information'.	
CCPA	1798.110. (a)	-
	'A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer the following: (2) The categories of sources from which the personal information is collected'.	
APPS	App 3	*Collection of solicited personal information*
	'An organisation must, on request, provide its source for an individual's personal information, unless it is impracticable or unreasonable to do so. APP 3.6 provides that an APP entity 'must collect personal information about an individual only from the individual', unless exceptions apply'.	
New Zealand	Principle 2	*Source of personal information*
	'Personal information must usually be collected from the person the information is about. Collecting information from the person concerned means that people know what is going on and have some control over their information'.	

Table 13: Cross-border Disclosure of Personal Information Principle

Definition: *Individuals' information is expected to be protected and handled appropriately, wherever the processing takes place.*

GDPR	Article 44	*General principle for transfers*
	'All provisions in this Chapter "Chapter V: Transfers of personal data to third countries or international organisations" shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined'.	
PIPEDA	-	*Personal information transferred across borders*
	'Individuals should expect that their information is protected and handled appropriately, regardless of where it's processed'.	
CCPA	-	-
	N/A 1798.145. (a) 'The obligations imposed on businesses by this title shall not restrict a business's ability to: . . . (6) Collect or sell a consumer's personal information if every aspect of that commercial conduct takes place wholly outside of California. For purposes of this title, commercial conduct takes place wholly outside of California if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold. This paragraph shall not permit a business from storing personal information about a consumer when the consumer is in California and then collecting that personal information when the consumer and stored personal information is outside of California'.	
APPS	App 8	*Cross-border disclosure of personal information*
	'Before an APP entity discloses personal information to an overseas recipient, the entity must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information'.	
New Zealand	-	*Does the Privacy Act apply to organisations based overseas?*
	'Any organisation operating in New Zealand is required to comply with the Privacy Act, regardless of where the organisation is based'.	

Table 14: Dealing with Unsolicited Personal Information Principle

Definition: *An organisation must take reasonable steps to manage unsolicited personal information. Unsolicited personal information is 'personal information received by an entity that has not been requested by that entity.'*

GDPR	-	-
	N/A	
PIPEDA	-	-
	N/A	
CCPA	-	-
	N/A	
APPS	App 4	*Dealing with unsolicited personal information*
	4.1 'APP 4 outlines the steps an APP entity must take if it receives unsolicited personal information. Unsolicited personal information is personal information received by an entity that has not been requested by that entity'. 4.2 An APP entity that receives unsolicited personal information must decide whether or not it could have collected the information under APP 3. If not, the entity must destroy or de-identify the information'.	
New Zealand	-	-
	N/A	

Table 15: Adoption, Use or Disclosure of an identifier Principle

Definition: *Adopting, using, or disclosing a unique identifier that was created for an individual for a different purpose should be prohibited.*

GDPR	Article 87	*Processing of the national identification number*
	'Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation'.	
PIPEDA	-	*Guidelines for identification and authentication*
	'It is also important to avoid, where ever possible, using numbers such as a driver's licence number or social insurance number as an identifier as they were created for different purposes'.	
CCPA	-	-
	N/A	
APPS	App 9	*Adoption, Use or Disclosure of an identifier*
	'An organisation must not adopt, use or disclose a government related identifier unless an exception applies'.	
New Zealand	Principle 12	*Unique Identifiers*
	(2) 'An agency shall not assign to an individual a unique identifier that, to that agency's knowledge, has been assigned to that individual by another agency, unless those 2 agencies are associated persons within the meaning of section OD7 of the Income Tax Act 2004'.	

Table 16: Right of Individuals to Exercise their Rights

Definition: *Individuals shall have the right to exercise their data protection rights.*

GDPR	Article 12	*Transparent information, communication and modalities ...*
	'The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights'.	
PIPEDA	Principle 9	*Individual Access*
	'Help people prepare their request for access to personal information.' 'Respond to the request as quickly as possible, and no later than 30 days after receiving it'.	
CCPA	1798.130. (a)	-
	'A business shall: (1) Make available to consumers two or more designated methods for submitting requests for information required to be disclosed pursuant to Sections 1798.110 and 1798.115, including, at a minimum, a toll-free telephone number, and if the business maintains an Internet Web site, a Web site address. (2) Disclose and deliver the required information to a consumer free of charge within 45 days of receiving a verifiable request from the consumer.'	
APPS	Your Privacy Rights – App 12	*Access your personal information - Access to personal information*
	'An organisation or agency must be satisfied the request came from you or a person you authorised'. 'An agency must respond to a request for access to/ [correct] personal information within 30 days'. 'an entity cannot require an individual to follow a particular procedure, use a designated form or explain the reason for making the request. Any recommended procedure should be regularly reviewed to ensure that it is flexible and facilitates rather than hinders access'.	
New Zealand	Principle 6	*Access to personal information*
	'When an agency receives a request for access or correction, it has to do various things. It has to: decide whether it agrees to the request; if so, decide how it will provide access or correction; The agency has to make these decisions and let the requester know as soon as it can. The longest the agency can usually take is 20 working days from the date it receives the request.'	

Table 17: Right to be Informed

Definition: *Individuals must be informed about the collection, use and/or disclosure of their personal information.*

GDPR	Article 13 - 14	*Information to be provided where personal data are collected/ not obtained ...*
	'Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the [specified] information', such as information about the controller, the purpose of processing, the recipients of the personal data, and the rights of the data subject...etc. 'Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the [specified] information.'	
PIPEDA	Principle 3	*Consent*
	'The knowledge of the individual is required for the collection, use, or disclosure of personal information'.	
CCPA	1798.100 (b)	-
	'A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used'.	
APPS	App 5	*Notification of the collection of personal information*
	'An APP entity that collects personal information about an individual must take reasonable steps either to notify the individual of certain matters or to ensure the individual is aware of those matters'.	
New Zealand	Principle 3	*Collection of information from subject*
	'When an agency collects personal information from the person the information is about, it has to take reasonable steps to make sure that person knows things like: - why it's being collected - who will get the information - whether the person has to give the information or whether this is voluntary ... etc.'.	

Table 18: Right of Individuals Access

Definition: *Individuals have the right to access the personal information which an organisation is holding about them.*

GDPR	Article 15	*Right of access by the data subject*
	'The data subject shall have the right to access to the personal data', and provide information about the processing, such as 'purposes of processing, categories of personal data concerned, recipients, etc.)'.	
PIPEDA	Principle 9	*Individual Access*
	'Individuals have a right to access the personal information that an organization holds about them'. 'When asked, advise people about the personal information about them your organization holds. Explain how that information is or has been used and to whom it has been disclosed. Give people access to their information at minimal or no cost or explain your reasons for not providing access. Providing access can take different forms. For example, you may provide a written or electronic copy of the information or allow the individual to view the information or listen to a recording of the information'.	
CCPA	1798.100. (d)	-
	'A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer ... the categories and specific pieces of personal information the business has collected'.	
APPS	App 12	*Access to personal information*
	'APP 12 requires an APP entity that holds personal information about an individual to give the individual access to that information on request' 'The manner of access may, for example, be by email, by phone, in person, hard copy, or an electronic record'. 'An agency cannot impose upon an individual any charge for providing access to personal information'.	
New Zealand	Principle 6	*Access to personal information*
	'People usually have a right to ask for access to personal information that identifies them' '... a public sector agency shall not require the payment, by or on behalf of any individual who wishes to make an information privacy request'.	

Table 19: Right to Rectification

Definition: *Individuals shall have the right to ask for correction of their personal data.*

GDPR	Article 16	*Right to rectification*
	'The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her'.	
PIPEDA	Principle 9	*Individual Access*
	'Individuals have the right to challenge the accuracy and completeness of the information, and have that information amended as appropriate'.	
CCPA	-	-
	N/A	
APPS	App 13	*Correction of personal information*
	'Australian privacy law gives you the right to correct the personal information an organization or agency holds about you if it is: inaccurate, out of date, incomplete, irrelevant, misleading'.	
New Zealand	Principle 7	*Correction of personal information*
	'People have a right to ask the agency to correct information about themselves, if they think it is wrong'.	

Table 20: Right to Erasure

Definition: *Individuals shall have the right to ask for deletion of their personal data.*

GDPR	Article 17	*Right to erasure ('right to be forgotten')*
	'The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where [one of the specified grounds applies]'.	
PIPEDA	Principle 5 - Principle 6	*Principle 5 - Limiting Use, Disclosure, and Retention Principle 6- Accuracy*
	'Destroy, erase or anonymise any personal information that your organization no longer needs'. 'When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information'[12] .	
CCPA	1798.105. (a)	-
	'A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer'.	
APPS	-	*Australian entities and the EU General Data Protection Regulation (GDPR)*
	'There is no equivalent 'right to erasure' under the Privacy Act, however APP 11.2 requires an APP entity that holds personal information to take reasonable steps to destroy the information or to ensure it is de-identified if the information is no longer needed for any purpose permitted under the Privacy Act' [10].	
New Zealand	Principle 9	*Agency not to keep personal information for longer than necessary*
	There is no equivalent 'right to erasure' under the New Zealand's Privacy Act, however, 'an agency that holds personal information must not keep that information for longer than is necessary for the purposes for which the information may be lawfully used'.	

Table 21: Right to Restriction of Processing

Definition: *Individuals shall have the right to restrict the processing of their personal data.*

GDPR	Article 18	*Right to restriction of processing*
	'The data subject shall have the right to obtain from the controller restriction of processing where [one of the specified cases applies]'.	
PIPEDA	-	-
	N/A	
CCPA	-	-
	N/A	
APPS	-	-
	N/A	
New Zealand	-	-
	N/A	

Table 22: Right to Object

Definition: *Individuals shall have the right to object to the processing of their personal data.*

GDPR	Article 21	*Right to Object*
	'The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her'.	
PIPEDA	Principle 3	*Consent*
	There is no specific right to object to processing under the PIPEDA, but it can be inferred from principle 3 that 'individuals can withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice, and organizations must inform individual of the implications of withdrawal'.	
CCPA	1798.120. (a)	-
	'A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt out'.	
APPS	Chapter B	*B.51 Key concepts*
	There is no specific right to object to processing under the APPs, but 'An individual may withdraw their consent at any time' [3]	
New Zealand	-	*When does a privacy waiver expire?*
	N/A The New Zealand's Privacy Act does not contain an equivalent right to 'right to object'. However, 'an individual might at any point withdraw that consent and the agency has to respond accordingly'.	

Table 23: Right to Object to Marketing

Definition: *Individuals shall have the right to reject the processing of their personal data for direct marketing purposes.*

GDPR	Article 21	*Right to object*
	2. 'Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing'. 3. 'Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes'.	
PIPEDA	-	-
	N/A	
CCPA	1798.120. (c)	-
	It is not mentioned explicitly but could be inferred from 1798.120. (c), 'a business that has received direction from a consumer not to sell the consumer's personal information or, in the case of a minor consumer's personal information has not received consent to sell the minor consumer's personal information shall be prohibited, pursuant to paragraph (4) of subdivision (a) of Section 1798.135, from selling the consumer's personal information after its receipt of the consumer's direction, unless the consumer subsequently provides express authorization for the sale of the consumer's personal information'.	
APPS	App 7	*Direct marketing*
	"An organisation must not use or disclose the personal information that it holds about an individual for the purpose of direct marketing (APP 7.1) 7.2 and 7.3 require an organisation to provide a simple means by which an individual can request not to receive direct marketing communications (also known as 'opting out')."	
New Zealand	-	-
	N/A	

Table 24: Right to Data Portability

Definition: *Individuals shall have the right to receive their personal data in a readily useable format that allows the Individual to transmit the information to another organisation.*

GDPR	Article 20	*Right to data Portability*
	'The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided'.	
PIPEDA	-	-
	N/A	
CCPA	1798.100. (d)	-
	'A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance'.	
APPS	-	*Australian entities and the EU General Data Protection Regulation (GDPR)*
	N/A 'The Privacy Act does not include an equivalent right to 'data portability' or 'right to object'. However, individuals do have a right to request access to, and correction of, their personal information under APPs 12 and 13. In giving access under APP 12, where reasonable and practicable, an entity must give access in the manner requested by the individual. For more information, see Chapters 12 and 13 of the APP guidelines' [10].	
New Zealand	-	-
	N/A	

Table 25: Right to Object to Automated Decision-Making

Definition: *Individuals must have the right to object to a decision that is based solely on automated processing.*

GDPR	Article 22	*Automated individual decision-making, including profiling*
	'The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'.	
PIPEDA	-	-
	N/A	
CCPA	-	-
	N/A	
APPS	-	-
	N/A	
New Zealand	-	-
	N/A	

Table 26: Right to Withdraw Consent

Definition: *Individuals shall have the right to withdraw consent at any time.*

GDPR	Article 7	*Conditions for consent*
	'The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent'.	
PIPEDA	Principle 3	*Consent*
	'Individuals can withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice, and you must inform individual of the implications of withdrawal'.	
CCPA	1798.120. (a)	-
	'A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt out'.	
APPS	Chapter B	*B.51 Key concepts*
	'An individual may withdraw their consent at any time, and this should be an easy and accessible process. Once an individual has withdrawn consent, an APP entity can no longer rely on that past consent for any future use or disclosure of the individual's personal information' [13]	
New Zealand	-	*When does a privacy waiver expire?*
	'An individual might at any point withdraw that consent and the agency has to respond accordingly' [14].	

Table 27: Right to Complain

Definition: *Every data subject shall have the right to lodge a complaint.*

GDPR	Article 14	*Transparent information, communication and modalities for the exercise of the rights ...*
	'If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy'.	
PIPEDA	Principle 10	*Challenging Compliance - File a formal privacy complaint*
	'An individual must be able to challenge your organization's compliance with the fair information principles. They should address their challenge to the person in your organization who is accountable for compliance with PIPEDA'. 'If you can't resolve the issue directly with the organization, you may decide to file a formal complaint'.	
CCPA	1798.150. (a)	-
	'(1) Any consumer whose nonencrypted or nonredacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of [specified conditions]'. ..... '(2) A consumer bringing an action as defined in paragraph (1) of subdivision (c) shall notify the Attorney General within 30 days that the action has been filed. (3) The Attorney General, upon receiving such notice shall, within 30 days, do one of the specified steps'.	
APPS	-	*Lodge a privacy complaint with us*
	'If you're concerned your personal information has been mishandled, you first need to complain to the organisation or agency you think has mishandled it. If they don't respond to your complaint within 30 days or you're not happy with their response, you can lodge a complaint with us'.	
New Zealand	Your Rights	*Making a complaint*
	'If you're unable to resolve a privacy dispute, you can make a complaint to us. But, before you make a complaint to us, contact the agency and let it know what the problem is. Agencies can often sort out problems more quickly without the need for us to get involved'.	

Table 28: Right of individuals not to be Discriminated

Definition: *A business shall not discriminate against a consumer because the consumer exercised any of their rights.*

GDPR	-	-
	N/A	
PIPEDA	-	-
	N/A	
CCPA	1798.130. (a)	-
	"1798.125. (a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title."	
APPS	-	-
	N/A	
New Zealand	-	-
	N/A	

4 Privacy by Design Schemes

This section presents various Privacy by Design (PbD) schemes (e.g., privacy principles, strategies, guidelines, and patterns) that developed previously by different researchers.

4.1 Privacy Principles

4.1.1 Privacy by Design Principles by Cate (2010) Fair Information Practice Principles (FIPPs) [15]:

01. Notice / Awareness Consumers should be given notice of an entity's information practices before any personal information is collected from them. This requires that companies explicitly notify some or all of the following:

- Identification of the entity collecting the data;
- Identification of the uses to which the data will be put;
- Identification of any potential recipients of the data;
- The nature of the data collected and the means by which it is collected;
- Whether the provision of the requested data is voluntary or required;
- The steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.

02. Choice / Consent Choice and consent in an on-line information-gathering sense means giving consumers options to control how their data is used. Specifically, choice relates to secondary uses of information beyond the immediate needs of the information collector to complete the consumer's transaction. The two typical types of choice models are 'opt- in' or 'opt-out.' The 'opt-in' method requires that consumers affirmatively give permission for their information to be used for other purposes. Without the consumer taking these affirmative steps in an 'opt-in' system, the information gatherer assumes that it cannot use the information for any other purpose. The 'opt-out' method requires consumers to affirmatively decline permission for other uses. Without the consumer taking these affirmative steps in an 'opt-out' system, the information gatherer assumes that it can use the consumer's information for other purposes. Each of these systems can be designed to allow an individual consumer to tailor the information gatherer's use of the information to fit their preferences by checking boxes to grant or deny permission for specific purposes rather than using a simple "all or nothing" method.

03. Access / Participation Access as defined in the Fair Information Practice Principles includes not only a consumer's ability to view the data collected, but also to verify and contest its accuracy. This access must be inexpensive and timely in order to be useful to the consumer.

04. Integrity / Security Information collectors should ensure that the data they collect is accurate and secure. They can improve the integrity of data by cross-referencing it with only reputable databases and by providing access for the consumer to verify it. Information collectors can keep their data secure by protecting against both internal and external security threats. They can limit access within their company to only necessary employees to protect against internal threats, and they can use encryption and other computer-based security systems to stop outside threats

05. Enforcement / Redress In order to ensure that companies follow the Fair Information Practice Principles, there must be enforcement measures. The FTC identified three types of enforcement measures: self-regulation by the information collectors or an appointed regulatory body; private remedies that give civil causes of action for individuals whose information has been misused to sue violators; and government enforcement that can include civil and criminal penalties levied by the government.

4.1.2 Privacy by Design Principles by Ann Cavoukian

Cavoukian (2010) has proposed seven Privacy by Design foundation principles [16]:

01. Proactive not Reactive; Preventative not Remedial The Privacy by Design (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred - it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.

02.Privacy as the Default Setting We can all be certain of one thing - the default rules! Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy - it is built into the system, by default. 03. Privacy Embedded into Design Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

03.Privacy Embedded into Design Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

04. Full Functionality-Positive - Sum, not Zero-Sum Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

05. End-to-End Security - Full Lifecycle Protection Privacy by Design, having been em- bedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved - strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

06. Visibility and Transparency - Keep it Open Privacy by Design seeks to assure all stake- holders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

07. Respect for User Privacy - Keep it User-Centric Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

4.1.3 ISO 29100 Privacy framework

ISO 29100 has proposed 11 privacy principles [17]:

01. Consent and choice Adhering to the consent principle means:

- presenting to the PII principal the choice whether or not to allow the processing of their PII except where the PII principal cannot freely withhold consent or where applicable law specifically allows the processing of PII without the natural personâĂŹs consent. The PII principal's choice must be given freely, specific and on a knowledgeable basis;

- obtaining the opt-in consent of the PII principal for collecting or otherwise processing sensitive PII except where applicable law allows the processing of sensitive PII without the natural personâĂŹs consent;
- informing PII principals, before obtaining consent, about their rights under the individual participation and access principle;
- providing PII principals, before obtaining consent, with the information indicated by the openness, transparency and notice principle; and
- explaining to PII principals the implications of granting or withholding consent.

02. Purpose legitimacy and specification Adhering to the purpose legitimacy and specification principle means:

- ensuring that the purpose(s) complies with applicable law and relies on a permissible legal basis;
- communicating the purpose(s) to the PII principal before the time the information is collected or used for the first time for a new purpose;
- using language for this specification which is both clear and appropriately adapted to the circumstances; and
- if applicable, giving sufficient explanations for the need to process sensitive PII.

03. Collection limitation Adhering to the collection limitation principle means:

- limiting the collection of PII to that which is within the bounds of applicable law and strictly necessary for the specified purpose(s).

04. Data minimisation Adhering to the Data Minimisation principle means designing and implementing data processing procedures and ICT systems in such a way as to:

- minimise the PII which is processed and the number of privacy stakeholders and people to whom PII is disclosed or who have access to it;
- ensure adoption of a âĂIJneed-to-knowâĂİ principle, i.e. one should be given access only to the PII which is necessary for the conduct of his/her official duties in the framework of the legitimate purpose of the PII processing;
- use or offer as default options, wherever possible, interactions and transactions which do not involve the identification of PII principals, reduce the observability of their behaviour and limit the linkability of the PII collected; and
- delete and dispose of PII whenever the purpose for PII processing has expired, there are no legal requirements to keep the PII or whenever it is practical to do so.

05. Use, retention and disclosure limitation Adhering to the use, retention and disclosure limitation principle means:

- Limiting the use, retention and disclosure (including transfer) of PII to that which is necessary in order to fulfil specific, explicit and legitimate purposes;
- Limiting the use of PII to the purposes specified by the PII controller prior to collection, unless a different purpose is explicitly required by applicable law;
- Retaining PII only as long as necessary to fulfil the stated purposes, and thereafter securely destroying or anonymising it; and
- Locking (i.e. archiving, securing and exempting the PII from further processing) any PII when and for as long as the stated purposes have expired, but where retention is required by applicable laws.

06. Accuracy and quality Adhering to the accuracy and quality principle means:

- ensuring that the PII processed is accurate, complete, up-to-date (unless there is a legitimate basis for keeping outdated data), adequate and relevant for the purpose of use;
- ensuring the reliability of PII collected from a source other than from the PII principal before it is processed;
- verifying, through appropriate means, the validity and correctness of the claims made by the PII principal prior to making any changes to the PII (in order to ensure that the changes are properly authorized), where it is appropriate to do so;

- establishing PII collection procedures to help ensure accuracy and quality; and
- establishing control mechanisms to periodically check the accuracy and quality of collected and stored PII.

07. Openness, transparency and notice Adhering to the openness, transparency and notice principle means:

- providing PII principals with clear and easily accessible information about the PII controller âĂŹs policies, procedures and practices with respect to the processing of PII;
- including in notices the fact that PII is being processed, the purpose for which this is done, the types of privacy stakeholders to whom the PII might be disclosed, and the identity of the PII controller including information on how to contact the PII controller;
- disclosing the choices and means offered by the PII controller to PII principals for the purposes of limiting the processing of, and for accessing, correcting and removing their information; and
- giving notice to the PII principals when major changes in the PII handling procedures occur.

08. Individual participation and access; Adhering to the individual participation and access principle means:

- giving PII principals the ability to access and review their PII, provided their identity is first authenticated with an appropriate level of assurance and such access is not prohibited by applicable law;
- allowing PII principals to challenge the accuracy and completeness of the PII and have it amended, corrected or removed as appropriate and possible in the specific context;
- providing any amendment, correction or removal to PII processors and third parties to whom personal data had been disclosed, where they are known; and
- establishing procedures to enable PII principals to exercise these rights in a simple, fast and efficient way, which does not entail undue delay or cost.

09. Accountability The processing of PII entails a duty of care and the adoption of concrete and practical measures for its protection. Adhering to the accountability principle means:

- documenting and communicating as appropriate all privacy-related policies, procedures and practices;
- assigning to a specified individual within the organization (who might in turn delegate to others in the organization as appropriate) the task of implementing the privacy-related policies, procedures and practices;
- when transferring PII to third parties, ensuring that the third party recipient will be bound to provide an equivalent level of privacy protection through contractual or other means such as mandatory internal policies (applicable law can contain additional requirements regarding international data transfers);
- providing suitable training for the personnel of the PII controller who will have access to PII;
- setting up efficient internal complaint handling and redress procedures for use by PII principals;
- informing PII principals about privacy breaches that can lead to substantial damage to them (unless prohibited, e.g., while working with law enforcement) as well as the measures taken for resolution;
- notifying all relevant privacy stakeholders about privacy breaches as required in some jurisdictions (e.g., the data protection authorities) and depending on the level of risk;
- allowing an aggrieved PII principal access to appropriate and effective sanctions and/or remedies, such as rectification, expungement or restitution if a privacy breach has occurred; and
- considering procedures for compensation for situations in which it will be difficult or impossible to bring the natural person âĂŹs privacy status back to a position as if nothing had occurred.

10. Information security Adhering to the information security principle means:

- protecting PII under its authority with appropriate controls at the operational, functional and strategic level to ensure the integrity, confidentiality and availability of the PII, and protect it against risks such as unauthorized access, destruction, use, modification, disclosure or loss throughout the whole of its life cycle;
- choosing PII processors that provide sufficient guarantees with regard to organizational, physical and technical controls for the processing of PII and ensuring compliance with these controls;
- basing these controls on applicable legal requirements, security standards, the results of systematic security risk assessments as described in ISO 31000, and the results of a cost/benefit analysis;

- implementing controls in proportion to the likelihood and severity of the potential consequences, the sensitivity of the PII, the number of PII principals that might be affected, and the context in which it is held;
- limiting access to PII to those individuals who require such access to perform their duties, and limit the access those individuals have to only that PII which they require access to in order to perform their duties;
- resolving risks and vulnerabilities that are discovered through privacy risk assessments and audit processes; and
- subjecting the controls to periodic review and reassessment in an ongoing security risk management process.

11. Privacy compliance Adhering to the privacy compliance principle means:

- verifying and demonstrating that the processing meets data protection and privacy safeguarding requirements by periodically conducting audits using internal auditors or trusted third-party auditors;
- having appropriate internal controls and independent supervision mechanisms in place that assure compliance with relevant privacy law and with their security, data protection and privacy policies and procedures; and
- developing and maintaining privacy risk assessments in order to evaluate whether program and service delivery initiatives involving PII processing comply with data protection and privacy requirements.

4.1.4 Privacy by Design Principles for Big Data by Ann Cavoukian and Jeff Jonas

Cavoukian and Jonas (2010) has extended the Cavoukian's privacy principle [16] as follows [18] :

01. Full Attribution Every observation (record) needs to know from where it came and when. There cannot be merge/purge data survivorship processing whereby some observations or fields are discarded.

02. Data Tethering Adds, changes and deletes occurring in systems of record must be accounted for, in real time, in sub-seconds.

03. Analytics on Anonymised Data The ability to perform advanced analytics (including some fuzzy matching) over cryptographically altered data means organizations can anonymise more data before information sharing.

04. Tamper-Resistant Audit Logs Every user search should be logged in a tamper-resistant manner-even the database administrator should not be able to alter the evidence contained in this audit log.

05. False Negative Favouring Methods The capability to more strongly favour false negatives is of critical importance in systems that could be used to affect someone's civil liberties.

06. Self-Correcting False Positives With every new data point presented, prior assertions are re-evaluated to ensure they are still correct, and if no longer correct, these earlier assertions can often be repaired in real time.

07. Information Transfer Accounting Every secondary transfer of data, whether to human eyeball or a tertiary system, can be recorded to allow stakeholders (e.g., data custodians or the consumers themselves) to understand how their data is flowing.

4.1.5 Wright and Raab Privacy Principles [19]:

01. Right to dignity, i.e., freedom from infringements upon the person or his / her reputation.

02. Right to be let alone (privacy of the home, etc.).

03. Right to anonymity, including the right to express oneâĂŹs views anonymously.

04. Right to autonomy, to freedom of thought and action, without being surveilled.

05. Right to individuality and uniqueness of identity.

06. Right to assemble or associate with others without being surveilled.

07. Right to confidentiality and secrecy of communications.

08. Right to travel (in physical or cyber space) without being tracked.

09. People should not have to pay in order to exercise their rights of privacy (subject to any justifiable exceptions), nor be denied goods or services or offered them on a less preferential basis.

4.1.6 Fisk et al. (2015) Principles [20]:

01. Principle of Least Disclosure Systems should strive to disclose as little to others as possible, while still sharing.

02. Principle of Qualitative Evaluation One must balance (subjectively) costs and benefits for privacy and progress.

03. Principle of Forward Progress Organizations must not become paralyzed by Least Disclosure and Qualitative Evaluation.

4.2 Privacy Strategies

4.2.1 Privacy Strategies by Rost and Bock

Rost and Bock (2011) has suggested six privacy strategies [21]:

01. Availability

02. Integrity

03. Confidentiality

04. Transparency

05. Unlinkability

06. Ability to intervene

4.2.2 Privacy Strategies by Hoepman

Hoepman (2014) has proposed eight privacy design strategies [22]:

01. Minimise The most basic privacy design strategy is MINIMISE, which states that the amount of personal data that is processed should be restricted to the minimal amount possible.

02. Hide Any personal data, and their interrelationships, should be hidden from plain view.

03. Separate Personal data should be processed in a distributed fashion, in separate compartments whenever possible.

04. Aggregate Personal data should be processed at the highest level of aggregation and with the least possible detail in which it is (still) useful.

05. Inform Data subjects should be adequately informed whenever personal data is processed.

06. Control Data subjects should be provided agency over the processing of their personal data.

07. Enforce A privacy policy compatible with legal requirements should be in place and should be enforced.

08. Demonstrate Be able to demonstrate compliance with the privacy policy and any applicable legal requirements

4.3 Privacy Guidelines

4.3.1 Privacy Guidelines by O'Leary (1995) [23]:

01. Collection limitation Data should be obtained lawfully and fairly, while some very sensitive data should not be held at all.

02. Data quality Data should be relevant to the stated purposes, accurate, complete and up-to- date: proper precautions should be taken to ensure this accuracy.

03. Purpose specification The purposes for which data will be used should be identified, and the data should be destroyed if it no longer serves the given purpose.

04. Use limitation Use of data for purposes other than specified is forbidden, except with the consent of the data subject or by authority of the law.

05. Security safeguards Agencies should establish procedures to guard against loss. corruption, destruction, or misuse of data.

06. Openness It must be possible to acquire information about the collection, storage, and use of personal data.

07. Individual participation The data subject has a right to access and challenge the data related to him or her.

08. Accountability A data controller should be accountable for complying with measures giving effect to all these principles.

4.3.2 Privacy Guidelines by Perera et al. (2019) [24]:

01. Minimise data acquisition This guideline suggests to minimise the amount of data collected or requested by an IoT platform or application. Minimisation includes:

- Minimising data types (e.g., energy consumption, water consumption, temperature)
- Minimum duration (e.g., hours, days, weeks, months)
- Minimum frequency (e.g., sampling rate: one second, 30 seconds, minutes)
- Minimum amount of data (e.g., kilobytes, megabytes, gigabytes)

02. Minimise number of data sources This guideline suggests to minimise the number of data sources used by an IoT platform or application. Depending on the task at hand, it may be required to collect data from different sources. Multiple data sources may hold pieces of information about an individual (e.g., An activity tracking service may hold an individual's activity data while a hospital may hold his health records). Aggregation of data from multiple sources allow malicious parties to identify sensitive personal information of an individual that that could lead to privacy violations.

03. Minimise raw data intake Whenever possible, IoT applications should reduce the amount of raw1 data intake. Raw data could lead to secondary usage and privacy violation. Therefore, IoT platforms should consider converting (or transforming) raw data into secondary context data. For example, IoT applications can extract orientation (e.g. sitting, standing, walking) by processing accelerometer data and store only the results (i.e. secondary context) and delete the raw accelerometer data.

04. Minimise knowledge discovery This guideline suggests to minimise the amount of knowledge discovered within an IoT application. IoT applications should only discover the knowledge necessary to achieve their primary objectives. For example, if the objective is to recommend food plans, it should not attempt to infer users' health status without their explicit permission.

05. Minimise data storage This guideline suggests to minimise the amount of data (i.e. primary or secondary) stored by an IoT application. Any piece of data that is not required to perform a certain task should be deleted. For example, raw data can be deleted once secondary contexts are derived. Further, personally identifiable data may be deleted without storing.

06. Minimise data retention period This guideline suggests to minimise the duration for which data is stored (i.e. avoid retaining data for longer than needed). Long retention periods provide more time for malicious parties to attempt accessing the data in unauthorized manner. Privacy risks are also increased because long retention periods could lead to unconsented secondary usage.

07. Hidden data routing In IoT, data is generated within sensing devices. The data analysis typically happens within cloud servers. Therefore, data is expected to travel between different types of computational nodes before arriving at the processing cloud servers. This type of routing could reveal user locations and usage from anyone conducting network surveillance or traffic analysis. To make it more difficult for Internet activities to be traced back to the users, this guideline suggests that IoT applications should support and employ anonymous routing mechanism (e.g., torproject.org).

08. Data anonymisation This guideline suggests to remove personally identifiable information before the data gets used by IoT applications so that the people described by the data remain anonymous. Removal of personally identifiable information reduces the risk of unintended disclosure and privacy violations.

09. Encrypted data communication This guideline suggests that different components in an IoT application should consider encrypted data communication wherever possible. Encrypted data communication would reduce the potential privacy risks due to unauthorised access during data transfer between components. There are multiple data communication approaches based on the components involved in an IoT application, namely, 1) device-to-device, 2) device-to-gateway, 3) device-to-cloud, and 4)gateway-to-cloud. Sensor data communication can be encrypted using symmetric encryption AES 256 in the application layer. Typically, device- to-device communications are encrypted at the link layer using special electronic hardware included in the radio modules. Gateway-to-cloud communication is typically secured through HTTPS using Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

10. Encrypted data processing This guideline suggests to process data while encrypted. Encryption is the process of encoding data in such a way that only authorised parties can read it. However, sometimes, the party who is responsible for processing data should not be allowed to read data. In such circumstances, it is important to process data while they are in encrypted form. For example, homomorphic encryption is a form of encryption that allows computations to be

carried out on cipher-text, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plain-text.

11. Encrypted data storage This guideline suggests that IoT applications should store data in encrypted form. Encrypted data storage reduces any privacy violations due to malicious attacks and unauthorised access. Data encryption can be applied in different levels from sensors to the cloud. Depending on the circumstances, data can be encrypted using both hardware and software technologies.

12. Reduce data granularity The granularity is the level of depth represented by the data. High granularity refers to atomic grade of detail and low granularity zooms out into a summary view of data. For example, dissemination of location can be considered as coarse- grained and full address can be considered as fine-grained. Therefore, releasing fine grained information always has more privacy risks than coarse-grained data as they contain more information. Data granularity has a direct impact on the quality of the data as well as the accuracy of the results produced by processing such data. IoT applications should request the minimum level of granularity that is required to perform their primary tasks. Higher level of granularity could lead to secondary data usage and eventually privacy violations.

13. Query answering This guideline suggests to release high-level answers to the query when dissemination without releasing raw data. For example, a sample query would be 'how energy efficient a particular household is?' where the answer would be in 0-5 scale. Raw data can always lead to privacy violations due to secondary usage. One such implementation is openPDS/SafeAnswers where it allows users to collect, store, and give high level answers to the queries while protecting their privacy.

14. Repeated query blocking This guideline goes hand-in-hand with the Query answering guideline. When answering queries, IoT applications need to make sure that they block any malicious attempts to discover knowledge that violates user privacy through repeated queries (e.g, analysing intersections of multiple results).

15. Distributed data processing This guideline suggests that an IoT application should process data in a distributed manner. Similar, approaches are widely used in traditional wireless sensor network domain. Distributed processing avoids centralised large-scale data gathering. As a result, it deters any unauthorised data access attempts.

16. Distributed data storage This guideline recommends storing data in a distributed manner. Distributed data storage reduces any privacy violation due to malicious attacks and unauthorised access. It also reduces privacy risks due to unconsented secondary knowledge discovery.

17. Knowledge discovery based aggregation Aggregation of information over groups of attributes or groups of individuals, restricts the amount of detail in the personal data that remains. This guideline suggests to discover knowledge though aggregation and replace raw data with discovered new knowledge. For example, 'majority of people who visited the park on [particular date] were young students' is an aggregated result that is sufficient (once collected over a time period) to perform further time series based sales performance analysis of a near-by shop. Exact timings of the crowd movements are not necessary to achieve this objective.

18. Geography based aggregation This guideline recommends to aggregate data using geographical boundaries. For example, a query would be 'how many electric vehicles used in each city in UK'. The results to this query would be an aggregated number unique to the each city. It is not required to collect or store detailed about individual electric vehicle.

19. Chain aggregation This guideline suggests to perform aggregation on-the-go while moving data from one node to another. For example, if the query requires a count or average, it can be done without pulling all the data items to a centralised location. Data will be sent from one node to another until all the nodes get a chance to respond. Similar techniques are successfully used in wireless sensor networks. This type of technique reduces the amount of data gathered by a centralised node (e.g. cloud server). Further, such aggregation also eliminates raw data from the results by reducing the risk of secondary data usage.

20. Time-Period based aggregation This guideline suggests to aggregate data over time (e.g. days, week, months). Aggregation reduces the granularity of data and also reduces the secondary usage that could lead to privacy violations. For example, energy consumption of a given house can be acquired and represented in aggregated form as 160 kWh per month instead of gathering energy consumption on daily or hourly basis.

21. Category based aggregation Categorisation based aggregation approaches can be used to reduce the granularity of the raw data. For example, instead of using exact value (e.g. 160 kWh per month), energy consumption of a given house can be represented as 150-200 kWh per month. Time-Period based and category based aggregation can be combined together to reduce data granularity.

22. Information Disclosure This guideline suggests that data subjects should be adequately informed whenever data they own is acquired, processed, and disseminated. Inform can take place at any stage of the data life cycle. Further,

inform can be broadly divided into two categories: pre-inform and post-inform. Pre-inform takes place before data enters to a given data life cycle phase. Post-inform takes place soon after data leaves a given data life cycle phase.

- Consent and Data Acquisition: what is the purpose of the data acquisition?, What types of data are requested?, What is the level of granularity?, What are the rights of the data subjects?
- Data Pre-Processing: what data will be taken into the platform?, what data will be thrown out?, what kind of pre-processing technique will be employed?, what are the purposes of pre-processing data?, what techniques will be used to protect user privacy?
- Data Processing and Analysis: what type of data will be analysed?, what knowledge will be discovered?, what techniques will be used?.
- Data Storage: what data items will be stored? how long they will be stored? what technologies are used to store data (e.g. encryption techniques)? is it centralised or distributed storage? will there be any back up processes?
- Data Dissemination: with whom the data will be shared? what rights will receivers have? what rights will data subjects have?

23. Control This guideline recommends providing privacy control mechanisms for data subjects. Control mechanisms will allow data owners to manage data based on their preference. There are different aspects that the data owner may like to control. However, controlling is a time consuming task and not every data owner will have the expertise to make such decisions. Therefore, it is a software architect's responsibility to carefully go through the following list of possibilities and determine what kind of controls are useful and relevant to data owners in a given IoT application context. Further, it is important to provide some kind of default set of options for data owners to choose from, specially in the cases where data subjects do not have sufficient knowledge. Some potential aspects that a data owner may like to control are 1) data granularity, 2) anonymisation technique, 3) data retention period, 4) data dissemination.

24. Logging This guideline suggests to log events during all phases. It allows both internal and external parties to examine what has happened in the past to make sure a given system has performed as promised. Logging could include but not limited to event traces, performance parameters, timestamps, sequences of operations performed over data, any human interventions. For example, a log may include the timestamps of data arrival, operations performed in order to anonymise data, aggregation techniques performed, and so on.

25. Auditing This guideline suggests to perform systematic and independent examinations of logs, procedures, processes, hardware and software specifications, and so on. The logs above could play a significant role in this processes. Non-disclosure agreements may be helpful to allow auditing some parts of the classified data analytics processes.

26. Open Source Making source code of an IoT application open allows any external party to review code. Such reviews can be used as a form of compliance demonstration. This allows external parties to examine the code bases to verify and determine whether a given application or platform has taken all measures to protect user privacy.

27. Data Flow Data flow diagrams (e.g. Data Flow Diagrams used by Unified Modelling Language) allow interested parties to understand how data flows within a given IoT application and how data is being treated. Therefore, DFDs can be used as a form of a compliance demonstration.

28. Certification In this context, certification refers to the confirmation of certain characteristics of an system and process. Typically, certifications are given by a neutral authority. Certification will add trustworthiness to IoT applications. TRUSTe (truste.com) Privacy Seal is one example, even though none of the existing certifications are explicitly designed to certify IoT applications.

29. Standardisation This guideline suggests to follow standard practices as a way to demonstrate privacy protection capabilities. Industry wide standards (e.g. AllJoyn allseenalliance.org) typically inherit security measures that would reduce some privacy risks as well. This refers to the process of implementing and developing technical standards. Standardisation can help to maximise compatibility, interoperability, safety, repeatability, or quality. Standardisation will help external parties to easily understand the inner workings of a given IoT application.

30. Compliance Based on the country and region, there are number of policies, laws and regulations that need to be adhered to. It is important for IoT applications to respect guidelines. Some regulatory efforts are ISO 29100 Privacy framework, OECD privacy principles, and European Commission Protection of personal data.

4.4 Privacy Patterns

This section presents the existing privacy patterns which are gathered from [25, 26].

1. Protection against Tracking
2. Location Granularity
3. Minimal Information Asymmetry
4. Informed Secure Passwords
5. Awareness Feed
6. Encryption with user-managed keys
7. Federated Privacy Impact Assessment
8. Use of dummies
9. Who's Listening
10. Privacy Policy Display
11. Layered Policy Design
12. Discouraging blanket strategies
13. Reciprocity
14. Asynchronous notice
15. Abridged Terms and Conditions
16. Policy Matching Display
17. Incentivized Participation
18. Outsourcing [with consent]
19. Ambient Notice
20. Dynamic Privacy Policy Display
21. Privacy Labels
22. Data Breach Notification Pattern
23. Pseudonymous Messaging
24. Onion Routing
25. Strip Invisible Metadata
26. Pseudonymous Identity
27. Personal Data Store
28. Trust Evaluation of Services Sides
29. Aggregation Gateway
30. Privacy icons
31. Privacy-Aware Network Client
32. Sign an Agreement to Solve Lack of Trust on the Use of Private Data Context
33. Single Point of Contact
34. Informed Implicit Consent
35. Enable/Disable Functions
36. Privacy Colour Coding
37. Appropriate Privacy Icons
38. User data confinement pattern
39. Icons for Privacy Policies

40. Obtaining Explicit Consent
41. Privacy Mirrors
42. Appropriate Privacy Feedback
43. Impactful Information and Feedback
44. Decoupling [content] and location information visibility
45. Platform for Privacy Preferences
46. Access control
47. Pay Back
48. Privacy dashboard
49. Preventing mistakes or reducing their impact
50. Obligation Management
51. Informed Credential Selection
52. Anonymous Reputation-based Blacklisting
53. Negotiation of Privacy Policy
54. Reasonable Level of Control
55. Masquerade
56. Buddy List
57. Privacy Awareness Panel
58. Lawful Consent
59. Privacy Aware Wording
60. Sticky Policies
61. Personal Data Table
62. Informed Consent for Web-based Transactions
63. Added-noise measurement Obfuscation
64. Increasing awareness of information aggregation
65. Attribute Based Credentials
66. Trustworthy Privacy Plug-in
67. [Support] Selective Disclosure
68. Private link
69. Anonymity Set
70. Active broadcast of presence
71. Unusual Activities
72. Identity Federation Do Not Track Pattern
73. Dynamic Location Granularity

5 Mapping between the Combined Privacy Laws Framework and Privacy by Design Schemes

5.0.1 Mapping between the Combined Privacy Laws Framework and Privacy by Design Principles

In this section, the objective is to correlate the principles of the Privacy by Design (PbD) schemes with the key principles and individuals' rights of the CPLF. According to Table 29, Cate [15] has proposed five principles (Section 4.1.1),

Cavoukian [16] has suggested seven privacy principles (Section 4.1.2), and ISO/IEC 29100 [17] has issued 11 principles (Section 4.1.3). According to Table 30, Cavoukian and Jonas [18] have proposed 7 principles (Section 4.1.4), Wright and Raab [19] have created nine principles (Section 4.1.5), and three principles have been issued by Fisk et al. [20] (Section 4.1.6).

- - Begin of Table

Table 29: Mapping between the Combined Privacy Laws Framework and Privacy by Design Principles (Cate 2011, Cavoukian 2009, and ISO/IEC 29100 2011) *(shortened form of the terminologies - see Section 4 for the full form of PbD principles and Section 3 for the full form of the CPLF)*

Principles	Principles by Cate (2011) [15]					Principles by Cavoukian (2010) [16]							Principles by ISO/IEC 29100 (2011) [17]									
Privacy Laws/ Rights	0.1 Notice / Awareness ...	0.2 Choice / Consent	0.3 Access / Participation	0.4 Integrity / Security ...	0.5 Enforcement / Redress...	01. Proactive not Reactive; ...	02. Privacy as the ...	03. Privacy Embedded ...	04. Full Functionality-...	05. End-to-End ...	06. Visibility and Transparency - ...	07. Respect for User ...	01. Consent and choice	02. Purpose legitimacy and ...	03. Collection limitation	04. Data minimisation	05. Use, retention, and ...	06. Accuracy and quality	07. Openness, transparency, ...	08. Individual participation ...	09. Accountability	10. Information Security	11. Privacy Compliance
Transparency	✓										✓		✓	✓					✓				
Purpose Limitation						✓	✓							✓									
Limiting Use, Disclosure				✓		✓	✓	✓								✓	✓						
Data Minimisation						✓	✓	✓							✓	✓							
Consent						✓		✓				✓	✓										
Lawfulness of Processing						✓		✓				✓	✓										
Accuracy			✓	✓		✓												✓		✓			
Storage Limitation						✓	✓	✓								✓	✓						
Security				✓		✓	✓	✓		✓												✓	
Accountability					✓	✓	✓	✓	✓											✓	✓		✓
Anonymity ...						✓	✓	✓		✓						✓							
Source								✓															
Cross-border Disclousure ..						✓	✓																
Dealing ... Data						✓	✓																
Adoption, .. identifier							✓	✓															
.. Exercise Rights			✓									✓								✓	✓		
Right to be informed	✓										✓	✓	✓	✓					✓				
Right of .. Access			✓									✓								✓			
Right to Rectification			✓			✓						✓								✓			

- - Continuation of Table

Principles	Principles by Cate (2011) [15]					Principles by Cavoukian (2010) [16]							Principles by ISO/IEC 29100 (2011) [17]										
Privacy Laws/ Rights	0.1 Notice / Awareness ...	0.2 Choice / Consent	0.3 Access / Participation	0.4 Integrity / Security ...	0.5 Enforcement / Redress...	01. Proactive not Reactive; ...	02. Privacy as the ...	03. Privacy Embedded ...	04. Full Functionality-...	05. End-to-End ...	06. Visibility and Transparency - ...	07. Respect for User ...	01. Consent and choice	02. Purpose legitimacy and ...	03. Collection limitation	04. Data minimisation	05. Use, retention, and ...	06. Accuracy and quality	07. Openness, transparency, ...	08. Individual participation ...	09. Accountability	10. Information Security	11. Privacy Compliance
Right to Erasure												✓								✓			
.. Restriction of Processing						✓						✓											
Right to Object						✓						✓											
.. Object to Marketing						✓						✓											
Right to Data Portability												✓											
.. Automated Decision ..						✓						✓											
.. Withdraw Consent		✓				✓						✓	✓										
Right to Complain												✓									✓		
.. Discriminated												✓											

End of Table

Regarding the relationship between the CPLF and the Privacy by Design (PbD) principles of Cate [15], Cavoukian [16], and ISO/IEC [17], Table 29 shows that most of the principles and rights of the CPLF are associated with many of these PbD principles. Interestingly, the principles of Cavoukian [16] tend to cover all the principles and rights of the CPLF compared to Cate [15], and ISO/IEC [17] principles. Cavoukian [16], furthermore, takes into consideration the interests of the individual under the principle of – **Respect for User Privacy; Keep it User-Centric** – as this principle achieves all the rights of the CPLF. This could simply return to the reason that Cavoukian [16] who first developed the concept of Privacy by Design. In contrast, **Consent, Lawfulness of processing, Storage limitation, and Anonymity and pseudonymity** principles of the CPLF are not covered by the principles of Cate [15]. In addition, neither Cate [15] nor ISO/IEC [17] consider the following principles of the CPLF: **Source, Cross-Border Disclosure of Personal Information, Dealing with Unsolicited Personal Data, and Adoption Use or Disclosure of an Identifier**. With regard to the rights, while Cavoukian [16] covers all the rights of the CPLF, Cate [15] and ISO/IEC [17] have missed most of these rights.

- - Begin of Table

Table 30: Mapping between the Combined Privacy Laws Framework and Privacy by Design Principles (Cavoukian et al. 2012, Wright et al. 2014, and Fisk et al. 2015) *(shortened form of the terminologies; see Section 4 for the full form of PbD principles and Section 3 for the full form of the CPLF)*

Principles	Principles by Cavoukian and Jonas (2012) [18]							Principles by Wright and Raab (2014) [19]								Principles by Fisk et al. (2015) [20]		
Privacy Laws/ Rights	1. Full Attribution	2. Data Tethering	3. Analytics on Anonymised ...	4. Tamper-Resistant ...	5. False Negative ...	6. Self-Correcting False ...	7. Information Transfer ...	01. Right to dignity	02. Right to be let alone	03. Right to anonymity	04. Right to autonomy	05. Right to individuality ...	06. Right to assemble or associate ...	07. Right to confidentiality and ...	08. Right to travel ...	09. People should not ...	Principle of Least ...	Principle of Qualitative ...	Principle of Forward Progress
Transparency							✓								✓				
Purpose Limitation																			
Limiting Use and Disclosure															✓		✓		✓
Data Minimisation					✓				✓	✓	✓	✓	✓						
Consent								✓	✓		✓	✓		✓	✓				
Lawfulness of Processing								✓	✓		✓	✓		✓	✓				
Accuracy	✓	✓				✓													
Storage Limitation																	✓		
Security			✓	✓										✓					
Accountability							✓											✓	✓
Anonymity and Pseudonymity			✓						✓	✓	✓	✓	✓						
Source																			
Cross-border Disclousure ...																			
Dealing with Unsolicited Data																			
Adoption ... an identifier																			
Right ... Exercise their Rights																✓			
Right to be informed							✓												
Right of Individuals Access																			
Right to Rectification	✓	✓				✓													
Right to Erasure																			
Right to Restriction of Processing																			
Right to Object															✓				
Right to Object to Marketing																			
Right to Data Portability																			
Right to object to Automated ...																			

- - Continuation of Table

Principles	Principles by Cavoukian and Jonas (2012) [18]							Principles by Wright and Raab (2014) [19]									Principles by Fisk et al. (2015) [20]		
Privacy Laws/ Rights	1. Full Attribution	2. Data Tethering	3. Analytics on Anonymised ...	4. Tamper-Resistant ...	5. False Negative ...	6. Self-Correcting False ...	7. Information Transfer ...	01. Right to dignity	02. Right to be let alone	03. Right to anonymity	04. Right to autonomy	05. Right to individuality ...	06. Right to assemble or associate ...	07. Right to confidentiality and ...	08. Right to travel ...	09. People should not ...	Principle of Least ...	Principle of Qualitative ...	Principle of Forward Progress
Right to Withdraw Consent																			
Right to Complain																			
Right ... not to be Discriminated																✓			

End of Table

According to Table 30, it seems that the principles of Cavoukian and Joans [18], Wright and Raab [19], and Fisk et al. [20] do not cover many of the CPLF's principles. This could be due to the nature of these principles, as the principles of Cavoukian and Joans are concerned with directing technical outcomes. While these principles move consumer privacy issues away from a policy or compliance issue towards a business imperative [18], the principles and rights of the CPLF tend to be legal requirements rather than technical requirements. As a result, only some – **Transparency, Accuracy, Security, Accountability** and **Anonymity and pseudonymity** – of the CPLF principles are achieved. **Right to be Informed**, and **Right to Rectification** – are also covered. With regard to the principles of Wright and Raab [19], they do not aim at creating principles that cover all the privacy issues, but aim to identify further privacy principles for the existing privacy principles that could be applied to different types of privacy with consideration of the risks and harms of different types of privacy policies [19]. Accordingly, seven out of 15 CPLF principles have been achieved, as shown in Table 4, and only two of the CPLF rights are covered – **Right of Individuals to Exercise their Rights**, and **Right to Object**. Fisk et al. [20], in contrast, define three principles that focus on sharing security information between organisations [20]. This results in achieving only three of the principles – **Limiting Use and Disclosure, Storage Limitation**, and **Accountability** – of the CPLF and missing all of its rights.

5.0.2 Mapping between the Combined Privacy Laws Framework and Privacy by Design Strategies

This section aims at correlating the strategies of Privacy by Design (PbD) and the key principles and individuals' rights of the CPLF. According to Table 31, while six privacy strategies have been issued by Rost and Bock [21] (Section 4.2.1), Hoepman [22] has created eight privacy strategies (see Section 4.2.2).

- - Begin of Table

Table 31: Mapping between Privacy Laws and Privacy by Design Strategies (Rost et al. 2011, and Hoepman 2014)
((shorten form of the terminologies; see Section 3 for the full form of the CPLF)

Strategies	Strategies by Rost and Bock (2011) [21]						Strategies by Hoepman (2014) [22]							
Privacy Laws/ Rights	01. Availability	02. Integrity	03. Confidentiality	04. Transparency	05. Unlinkability	06. Ability to intervene	01. Minimise	02. Hide	03. Separate	04. Aggregate	05. Inform	06. Control	07. Enforce	08. Demonstrate
Transparency				✓							✓			
Purpose Limitation					✓								✓	

- - Continuation of Table

Strategies	Strategies by Rost and Bock (2011) [21]						Strategies by Hoepman (2014) [22]							
Continuation of Privacy Laws/ Rights	01. Availability	02. Integrity	03. Confidentiality	04. Transparency	05. Unlinkability	06. Ability to intervene	01. Minimise	02. Hide	03. Separate	04. Aggregate	05. Inform	06. Control	07. Enforce	08. Demonstrate
Limiting Use and Disclosure							✓							
Data Minimisation							✓	✓		✓				
Consent						✓						✓		
Lawfulness of Processing						✓						✓		
Accuracy		✓												
Storage Limitation							✓							
Security			✓					✓	✓	✓				
Accountability	✓			✓	✓	✓							✓	✓
Anonymity and Pseudonymity							✓	✓						
Source														
Cross-border Disclousure ...														
Dealing with Unsolicited Data														
Adoption, Use ... of an Identifier														
Right ... to exercise their Rights						✓						✓		
Right to be informed											✓			
Right of Individuals Access						✓						✓		
Right to Rectification						✓						✓		
Right to Erasure						✓						✓		
Right to Restriction of Processing						✓						✓		
Right to Object						✓						✓		
Right to Object to Marketing						✓						✓		
Right to Data Portability						✓						✓		
Right to object to Automated Decision-Making						✓						✓		
Right to Withdraw Consent						✓						✓		
Right to Complain														
Right ... not to be Discriminated														

End of Table

According to Table 31, Rost and Bock [21] have formulated new data protection goals which are classified in this paper under the strategy of PbD schemes as it has an equivalent meaning, where strategy achieves a certain design goal. Hoepman [22] also defines eight PbD strategies from the perspective of an IT system, and considers legal requirements to be the point of departure. Accordingly, most of the principles and rights of the CPLF are covered by these strategies. More precisely, as shown in Table 31, these PbD strategies tend to cover more of the rights of the CPLF compared to the principles of CPLF. However, both strategies do not take into consideration the following principles of the CPLF: – **Source, Cross-border Disclosure of Personal Data, Dealing with Unsolicited Personal Data,** and **Adoption, Use, Disclosure of an Identifier**. While three strategies of Hoepman [22] cover the principle of – **Data Minimisation** – , none of Rost and Bock's [21] strategies are concerned about the **Data Minimisation** principle. In addition, neither the – **Limiting Use and Disclosure** – nor – **Storage Limitation** – and – **Anonymity and Pseudonymity** – of the CPLF are achieved by Rost and Bock's [21] strategies. This could simply refer to the perspective of Rost and Bock [21] as they

claim that their strategies do not stand alone but should be combined together with the privacy by design principles to be a comprehensive and universally accepted concept [21]. By contrast, while Rost's and Bock's [21] strategies achieve the **Accuracy** principle, Hoepman's [22] strategies do not.

5.0.3 Mapping between the Combined Privacy Laws Framework and Privacy by Design Guidelines

In this section, the guidelines by O'Leary [23] (Section 4.3.1) the guidelines by Perera et al.[24] (see Section 4.3.2) are mapped to the key principles and individuals' rights in the CPLF, as demonstrated in Tables 32 and 33.

- - Begin of Table

Table 32: Mapping between the Combined Privacy Laws Framework and Privacy by Design Guidelines (O'Leary 1995) [23] *(shortened form of the terminologies; see Section 3 for the full form of the CPLF)*

Guidelines	Guidelines by O'Leary (1995) [23]							
Privacy Laws/ Rights	01. Collection limitation	02. Data quality	03. Purpose specification	04. Use limitation	05. Security safeguards	06. Openness	07. Individual participation	08. Accountability
Transparency						✓		
Purpose Limitation			✓					
Limiting Use and Disclosure				✓				
Data Minimisation	✓							
Consent								
Lawfulness of Processing	✓							
Accuracy		✓						
Storage Limitation			✓					
Security					✓			
Accountability								✓
Anonymity and Pseudonymity								
Source								
Cross-border Disclousure of Personal Infomation								
Dealing with Unsolicited Data								
Adoption, Use or Disclosure of an identifier								
Right of individuals to exercise their rights							✓	
Right to be informed						✓		
Right of Individuals Access							✓	
Right to Rectification							✓	
Right to Erasure							✓	
Right to Restriction of Processing							✓	
Right to Object							✓	
Right to Object to Marketing							✓	
Right to Data Portability								
Right to object to Automated Decision-Making							✓	
Right to Withdraw Consent								
Right to Complain								
Right ... not to be Discriminated								

End of Table

With regard to the correlation of the CPLF and PbD guidelines by O'Leary [23], Table 32 shows that O'Leary's guidelines cover most of the principles and rights of the CPLF. Considering the right of the CPLF, as seen in Table 32, all the rights of the CPLF are achieved by O'Leary [23] except the – **Right to Data Portability**, **Right to Withdraw Consent**, **Right to Complain**, and **Right of Individuals not to be Discriminated**. According to the principles of the CPLF, O'Leary's [23] guidelines cover many of these principles: –**Transparency**, **Purpose Limitation**, **Limiting Use and Disclosure**, **Data Minimisation**, **Lawfulness of processing**, **Accuracy**, **Storage Limitation**, **Security**, and **Accountability**.

- - Begin of Table

Table 33: Mapping between the Combined Privacy Laws Framework and Privacy by Design Guidelines (Perera et al. 2019) *(shortened form of the terminologies; see Section 3 for the full form of the CPLF)*

Guidelines	Guidelines by Perera et al. (2019) [24]																														
Privacy Laws/ Rights	01. Minimise data acquisition	02. Minimise number of ...	03. Minimise raw data ...	04. Minimise knowledge ...	05. Minimise data storage	06. Minimise data retention ...	07. Hidden data routing	08. Data anonymisation	09. Encrypted data communication	10. Encrypted data processing	11. Encrypted data storage	12. Reduce data granularity	13. Query answering	14. Repeated query blocking	15. Distributed data processing	16. Distributed data storage	17. Knowledge discovery based ...	18. Geography based aggregation	19. Chain aggregation	20. Time-Period based ...	21. Category based aggregation	22. Information Disclosure	23. Control	24. Logging	25. Auditing	26. Open Source	27. Data Flow	28. Certification	29. Standardisation	30. Compliance
Transparency																															
Purpose Limitation				✓																											
Limiting Use ..			✓	✓								✓	✓				✓		✓	✓	✓										
Data Minimisation	✓	✓	✓		✓							✓	✓				✓	✓	✓		✓										
Consent																															
Lawfulness of Processing																															
Accuracy																															
Storage Limitation			✓			✓																									
Security							✓		✓	✓	✓			✓	✓	✓			✓													
Accountability																								✓	✓	✓	✓	✓	✓	✓	
Anonymity and Pseudonymity								✓																							
Source																															
Cross-border Disclosure ..																															
Dealing with Unsolicited Data																															
Adoption ... an identifier																															
Right ... to exercise their rights																							✓								

- - Continuation of Table

Guidelines	Guidelines by Perera et al. (2019) [24]																											
Privacy Laws/ Rights	01. Minimise data acquisition	02. Minimise number of ...	03. Minimise raw data ...	04. Minimise knowledge ...	05. Minimise data storage	06. Minimise data retention ...	07. Hidden data routing	08. Data anonymisation	09. Encrypted data communication	10. Encrypted data processing	11. Encrypted data storage	12. Reduce data granularity	13. Query answering	14. Repeated query blocking	15. Distributed data processing	16. Distributed data storage	17. Knowledge discovery based ...	18. Geography based aggregation	19. Chain aggregation	20. Time-Period based ...	21. Category based aggregation	22. Information Disclosure	23. Control	24. Logging	25. Auditing	26. Open Source	27. Data Flow	28. Certification	29. Standardisation	30. Compliance
Right to be informed																						✓								
Right of Individuals Access																							✓							
Right to Rectification																							✓							
Right to Erasure																							✓							
Right to Restriction ...																							✓							
Right to Object																							✓							
Right to Object to Marketing																							✓							
Right to Data Portability																							✓							
Right to ... Automated ...																							✓							
Right to Withdraw Consent																														
Right to Complain																														
Right .. Discriminated																														

End of Table

Table 33 shows the correlation between the Privacy by Design (PbD) guidelines by Perera et al. [24] and the CPLF. These 30 guidelines are inspired by Hoepman's strategies and have been developed for the IoT domain specifically to help software engineers develop and assess IoT applications [24]. As seen in Table 33, various principles and rights of the CPLF are achieved by Perera et al.'s [24] guidelines. Nevertheless, these guidelines tend to focus on achieving some of the CPLF's principles through several of the guidelines, rather than covering all the principles of the CPLF. For example, the – **Data Minimisation** – principle of the CPLF is covered by ten of Perera et al.'s [24] guidelines, while the – **Transparency**– principle is not covered by any of these guidelines. With regards to the rights of the CPLF, interestingly, all of these rights are covered by Perera et al.'s [24] guidelines except, **Right to Withdraw Consent**, **Right to Complain**, and **Right of Individuals not to be Discriminated**.

5.1 Mapping Privacy Laws and Privacy Patterns

This section correlates the privacy patterns and the principles and rights of the CPLF. These privacy patterns are gathered from [25, 26], as many common patterns are shared between these two resources. The principles and the rights of the CPLF are usually aimed at the legal domain and not the technical domain due to remaining disconnected from developers' tools and the environment required for building applications. Therefore, mapping the principles and the rights of the CPLF with the privacy patterns is essential to facilitate developers building a privacy-aware application and complying with the law. Typically, patterns are more reliable and it is possible to explain their use in a particular context, compared to guidelines, strategies or principles for PbD schemes, which is highlighted in Table 29, Table 30, Table 31, Table 32, and Table 33. The following criteria are followed in order to map between the privacy laws and the privacy patterns:

●	Direct relationship: If a specific pattern can achieve a law (principle/right) directly (a direct law).
○	Indirect relationship: If a specific law can achieve a specific pattern through a direct law.

Table 34: Mapping between the Combined Privacy Laws Framework and Privacy by Design Patterns *(shortened form of the terminologies; see Section 4.4 for the full form of privacy patterns and Section 3 for the full form of the CPLF)*

- - Begin of Table

Privacy Patterns	Transparency	Purpose Limitation	Limiting Use and Disclosure	Data Minimisation	Consent	Lawfulness of Processing	Accuracy	Storage Limitation	Security	Accountability	Anonymity and Pseudonymity	Source	Cross-border Disclosure ...	Dealing with Unsolicited Data	Adoption ... an identifier	Right ... to exercise their rights	Right to be informed	Right of Individuals Access	Right to Rectification	Right to Erasure	Right to Restriction ...	Right to Object	Right to Object to Marketing	Right to Data Portability	Right to object to Automated ...	Right to Withdraw Consent	Right to Complain	Right ... not to be Discriminated
1. Protection against ...		○						●	○	○	●																	
2. Location Granularity		○	●	●						○																		
3. Minimal Information ...	●	○		●						○							●											
4. Informed Secure Passwords									●	○																		
5. Awareness Feed	●									○							●											
6. Encryption ...									●	○																		
7. Federated Privacy ...										●																		
8. Use of Dummies									○	○	●																	
9. Who's Listening										○							●											
10. Privacy Policy Display	●									○							●											
11. Layered Policy Design	●									○							●											
12. Discouraging Blanket ...																												
13. Reciporcity																												
14. Asynchronous Notice										○							●											
15. Abridged Terms ...	●									○							●											
16. Policy Matching Display																												
17. Incentivized Participation																												
18. Outsourcing [with consent]		○	●		●	●				○																		
19. Ambient Notice	●									○							●											
20. Dynamic Privacy Policy ...	●									○							●											
21. Privacy Labels	●									○							●											
22. Data Breach Notification ...									●	●																		
23. Pseudonymous Messaging									●	○	●																	

- - Continuation of Table

Privacy Patterns	Transparency	Purpose Limitation	Limiting Use and Disclosure	Data minimisation	Consent	Lawfulness of Processing	Accuracy	Storage Limitation	Security	Accountability	Anonymity and Pseudonymity	Source	Cross-border Disclosure ...	Dealing with Unsolicited Data	Adoption ... an identifier	Right ... to exercise their rights	Right to be informed	Right of Individuals Access	Right to Rectification	Right to Erasure	Right to Restriction ...	Right to Object	Right to Object to Marketing	Right to Data Portability	Right to object to Automated ...	Right to Withdraw Consent	Right to Complain	Right ... not to be Discriminated
24. Onion Routing									●	○	●																	
25. Strip Invisible Metadata		○	●	●						○																		
26. Pseudonymous Identitiy									○	○	●																	
27. Personal Data Store																												
28. Trust Evaluation ...	●									●							●											
29. Aggregation Gateway				○					●	○																		
30. Privacy icons	●									○							●											
31. Privacy-Aware Network ...	●									○							●											
32. Sign an Agreement ...					●	●				○																		
33. Single Point of ...									●	○																		
34. Informed Implicit ...	●				●	○				○							●											
35. Enable/Disable Function	●				●	○				○							●											
36. Privacy Color Coding	●									○							●											
37. Appropriate Privacy Icons	●									○							●											
38. User Data Confinement ...		○		●						○																		
39. Icons for Privacy Policies	●									○							●											
40. Obtaining Explicit Consent					●	●				○																		
41. Privacy Mirrors										○							●	●										
42. Appropriate Privacy ...	●									○							●											
43. Impactful Information ...										○							●											
44. Decoupling [content] ...									●	○																		
45. Platform for Privacy ...	●									○							●											
46. Selective Access									●	○																		
47. Pay Back																												
48. Privacy Dashboard	●									○						●	●	●	●	●	●	●	●		●	●		
49. Preventing Mistakes ...		○	●		○	○				○							●											
50. Obligation Management		○		●				●		●							●											
51. Informed Credential ...	●	○		●						○							●											
52. Anonymous Reputation ...									●	○	●																	
53. Negotiation of ... Policy																												
54. Reasonable Level of ...		○	●							○																		
55. Masquerade		○	●							○																		
56. Buddy List		○	●							○																		
57. Privacy Awareness Panel	●									○							●											
58. Lawful Consent		●			●	●				○																		

- - Continuation of Table

Privacy Patterns	Transparency	Purpose Limitation	Limiting Use and Disclosure	Data minimisation	Consent	Lawfulness of Processing	Accuracy	Storage Limitation	Security	Accountability	Anonymity and Pseudonymity	Source	Cross-border Disclosure ...	Dealing with Unsolicited Data	Adoption ... an identifier	Right ... to exercise their rights	Right to be informed	Right of Individuals Access	Right to Rectification	Right to Erasure	Right to Restriction ...	Right to Object	Right to Object to Marketing	Right to Data Portability	Right to object to Automated ...	Right to Withdraw Consent	Right to Complain	Right ... not to be Discriminated
59. Privacy Aware Wording	●									○							○											
60. Sticky Policies		○		●				●		●							●											
61. Personal Data Table	●									○						●		●										
62. Informed Consent ...					●	●				○																		
63. Added-noise ...		○	●							○																		
64. Increasing Awareness ...	●				○					○							●											
65. Attribute Based ...		○		●					○	○	●																	
66. Trustworthy Privacy ...		○		●																								
67. [Support] Selective ...		○	●	●					○	○	●																	
68. Private Link		○	●							○																		
69. Anonymity Set									○	○	●																	
70. Active Broadcast of ...		○	●		●	○				○																		
71. Unusual Activities									●	○							●											
72. Identity Federation ...										●																		
73. Dynamic Location ...		○		●					○	○	●																	

End of Table

In the initial move towards correlating the privacy patterns and the CPLF, it is useful to construct criteria showing the capability of the privacy patterns to apply various principles and rights of the CPLF. Table 6 aims at correlating the privacy patterns and the principles and rights of the CPLF, which will enable thorough and efficient compliance with the main principles and rights of the CPLF of the various data protection laws. Two criteria have been identified: the (●) in the various cells determines a direct relationship, and the (○) shows an indirect relationship between the privacy patterns and the CPLF. Underlining the relationship between the privacy patterns and among the various principles and rights of privacy laws, the criteria indicates that most of the privacy patterns are associated with more than one principle or right, except the following patterns: **Discouraging Blanket Strategies**, **Reciprocity**, **Policy Matching Display**, **Incentivised Participation**, **Personal Data Store**, **Pay Back**, and **Negotiation of Privacy Policy**. This might be due to the nature of the privacy patterns as they are more specific than the principles or rights of the CPLF. Nevertheless, some of the principles and rights of the CPLF have not been associated with any of the privacy patterns, as seen in Table 6. These are the following principles: **Source**, **Cross-border Disclosure of Personal Data**, **Dealing with Unsolicited Data**, and **Adoption, Use or Disclosure of an identifier**. However, these principles of the CPLF are only limited to Australia's and New Zealand's data protection laws. With Regard to the rights of the CPLF, **Right to Data Portability**, **Right to Complain**, and **Right of Individuals not to be Discriminated** are not achieved by any of the privacy patterns. This could be due to the nature of the law as being largely disconnected from the technical domain. Some of the provisions of laws, furthermore, require organisations to comply with the provisions rather than implementing them in the development phase. Therefore, it cannot be implemented in the technical domain.

References

[1] the European Commission. L_2016119EN.01000101.xml, 2016.

[2] Office of the Privacy Commissioner of Canada. PIPEDA fair information principles - Office of the Privacy Commissioner of Canada, 2019.

[3] Office of the Privacy Commissioner of Canada. Businesses and your personal information - Office of the Privacy Commissioner of Canada, 2016.

[4] California State Legislature. Bill Text - AB-375 Privacy: personal information: businesses., 2018.

[5] Office of the Australian Information Commissioner. Australian Privacy Principles quick reference — OAIC, 2014.

[6] Office of the Australian Information Commissioner. Rights and responsibilities — OAIC, 2014.

[7] Office of the Privacy Commissioner of Canada. Office of the Privacy Commissioner |Commissioner of the privacy principles, 2016.

[8] Office of the Privacy Commissioner of Canada. Office of the Privacy Commissioner | Your Right To Know - an OPC advice sheet, 2013.

[9] Office of the Privacy Commissioner of Canada. What you need to know about mandatory reporting of breaches of security safeguards - Office of the Privacy Commissioner of Canada, 2018.

[10] Office of the Australian Information Commissioner. Australian entities and the EU General Data Protection Regulation (GDPR) — OAIC, 2018.

[11] Office of the Privacy Commissioner of Canada. AskUs | Article | Do we have to report data breaches? | Office of the Privacy Commissioner, 2013.

[12] Office of the Australian Information Commissioner. Interpretation Bulletin: Accuracy - Office of the Privacy Commissioner of Canada, 2013.

[13] Office of the Australian Information Commissioner. Chapter B: Key concepts — OAIC, 2019.

[14] Office of the Privacy Commissioner. AskUs | Article | When does a privacy waiver expire? | Office of the Privacy Commissioner, 2013.

[15] Fred H Cate. The Failure of Fair Information Practice Principles. *Consumer Protection in the Age of the 'Information Economy'*, pages 341–377, 2006.

[16] Ann Cavoukian. Privac y by Design. *Identity in the Information Society*, 3(2):1–12, 2010.

[17] the European Commission. INTERNATIONAL STANDARD ISO / IEC: Information technology — Security techniques — Guidelines for cybersecurity. 2012:58, 2012.

[18] Ann Cavoukian and Jeff Jonas. Privacy by Design in the Age of Big Data. *Information and Privacy Commisioner*, (June):1–17, 2012.

[19] David Wright and Charles Raab. Privacy principles, risks and harms. *International Review of Law, Computers and Technology*, 28(3):277–298, 2014.

[20] Gina Fisk, Calvin Ardi, Neale Pickett, John Heidemann, Mike Fisk, and Christos Papadopoulos. Privacy principles for sharing cyber security data. *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, pages 193–197, 2015.

[21] Martin Rost and Kirsten Bock. Privacy by Design and the New Protection Goals. *DuD, January*, (November 2009):1–9, 2011.

[22] Jaap-henk Hoepman. IFIP AICT 428 - Privacy Design Strategies. pages 446–459, 2014.

[23] Daniel E. O'leary. Some Privacy Issues in Knowledge Discovery: The OECD Personal Privacy Guidelines. *IEEE Expert-Intelligent Systems and their Applications*, 10(2):48–59, 1995.

[24] Charith Perera, Mahmoud Barhamgi, Arosha K. Bandara, Muhammad Ajmal, Blaine Price, and Bashar Nuseibeh. Designing Privacy-aware Internet of Things Applications. 2019.

[25] privacypatterns.org. Patterns - Privacy Patterns.

[26] privacypatterns.org. privacypatterns.eu - collecting patterns for better privacy.