Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective

ATHEER ALJERAISY, Cardiff University, UK
MASOUD BARATI, Cardiff University, UK
OMER RANA, Cardiff University, UK
CHARITH PERERA, Cardiff University, UK

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 this paper, we have conducted a systematic analysis of the privacy and 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. Then, we used framework analysis method to attain a comprehensive view of different privacy and 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, the key principles and individuals' rights of the CPLF were mapped with Privacy by Design (PbD) schemes (e.g., privacy principles, strategies, guidelines, and patterns) developed previously by different researchers in order to investigate the gaps in existing schemes. Subsequently, we have demonstrated how to apply and map privacy patterns into IoT architectures at the design stage, and have also highlighted the complexity of doing such mapping. Finally, we have identified the major challenges that should be addressed and potential research directions in order to take the burden off software developers when applying privacy-preserving techniques that comply with privacy and data protection laws. We have released a companion technical report [3] that comprises all definitions, detailed steps on how we developed the CPLF, and detailed mappings between CPLF, and PbD schemes.

CCS Concepts: • **Human-centered computing → Ubiquitous and mobile computing**; • **Security and privacy → Human and societal aspects of security and privacy**.

Additional Key Words and Phrases: Internet of Things, Privacy by Design, Privacy Law, Programming Environment, Human-centered Design, Software Engineering

ACM Reference Format:
Atheer Aljeraisy, Masoud Barati, Omer Rana, and Charith Perera. 2020. Privacy Laws and Privacy by Design Schemes for the Internet of Things: A Developer's Perspective. *ACM Comput. Surv.* 1, 1, Article 1990 (December 2020), 38 pages. https://doi.org/00.0000/000000.00000

Authors' addresses: Atheer Aljeraisy, aljeraisya@cardiff.ac.uk, Cardiff University, Cardiff, UK, CF10 3AT; Masoud Barati, Cardiff University, Cardiff, UK, baratim@cardiff.ac.uk; Omer Rana, Cardiff University, Cardiff, UK, ranaof@cardiff.ac.uk; Charith Perera, Cardiff University, Cardiff, UK, PereraC@cardiff.ac.uk.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
© 2020 Association for Computing Machinery.
0360-0300/2020/12-ART1990 $15.00
https://doi.org/00.0000/000000.00000

1 INTRODUCTION

Due to the potential of Internet of Things (IoT) applications to derive sensitive information about individuals [49], developers[1] must exercise due diligence so that users' privacy is protected in accordance with the regulations of privacy 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 when they are vague, and where it is difficult to extract and enact such legal requirements [6]. It is essential to note that developers often do not put privacy first [2, 7, 31], as well as having a lack of understanding of the necessity of putting it in place for data privacy and protection purposes [22]. There is, moreover, a lack of practical guidance that considers the technical domain for developers to build a-privacy-aware IoT application [29].

Building an IoT application is a complex process compared to desktop, mobile, or web applications [14]. This is due to the IoT containing various physical objects or nodes of different computing, sensing, and actuation capabilities, along with being able to communicate between each other and other systems in order to gather and exchange data [49]. The heterogeneous nature of IoT necessitates that both software and hardware should work together, for example sensors and actuators, across a variety of nodes, including mobile phones and cloud platforms, due to them having varying capabilities depending on different conditions [48]. The complexity of IoT architecture results in a lack of integrated development stacks, with different software engineering specialists collaborating to support end-to-end IoT applications [47].

Privacy concerns are not always properly considered due to engineering complexities, even though there may be isolated solutions [65, 67] for software processes during the design and development of IoT applications. In addition, studies have revealed that developers with various backgrounds tend to lack the skills to effectively implement privacy management [8, 63], and the difficulties around complying with regulations are likely to increase in the future [7]. Even though guidelines are available, they usually focus on legal aspects, and not technical requirements, leaving them disconnected from the environment that developers work in, as well as the tools they use to build applications. Thus, developers face the problem of relating the guidance provided to actual technical considerations, such as ensuring a specific design or its implementation properly meets privacy requirements.

Privacy by Design (PbD) [27] is a fairly new system that works to embed privacy practice more deeply and effectively into the development process [30, 59]. REGULATION (EU) 2016/679 General Data Protection Regulation (GDPR) [1] confirms the importance of this and is applicable to all systems that manage personal data processing - a common feature of IoT applications. The contribution of this paper is as follows:

- An analysis of various privacy and data protection laws, which are: General Data Protection Regulations (GDPR), the Personal Information Protection and Electronic Documents Act (PIPEDA), California Consumer Privacy Act (CCPA), Australian Privacy Principles (APPs), and New Zealand's Privacy Act 1993, through the framework analysis method [60] used to attain a comprehensive view of various privacy and data protection laws and highlight the disparities. This will assist developers in adhering to the regulations across different regions. Subsequently, a Combined Privacy Law Framework (CPLF) was created which was then used for the following tasks (CPLF is presented in Section 4 and the detailed results are presented in the Technical Report [3]). **The reason we created CPLF is that we noticed most of the well known Privacy and Data Protection Laws are based on very similar principles and rights. Therefore, instead of analysing each privacy and data protection law framework separately, we combined all the privacy and data protection law frameworks into**

[1]In this paper, the terms software developers, developers, or software engineers are used interchangeability.

a single Combined Privacy Law Framework (CPLF). By doing so, we eliminated the duplication of analysis and clarity.

- The key principles and individuals' right of the CPLF were mapped with the well-known Privacy by Design (PbD) schemes (e.g., privacy principles, strategies, guidelines, and patterns) developed by different researchers in the past in order to investigate the gaps in existing schemes.
- Furthermore, we provide an insight into how to apply privacy patterns to the IoT architecture during the software design phase. Several different case scenarios were used to demonstrate how developers could use privacy patterns to comply with privacy and data protection laws. Finally, the research challenges and opportunities were also identified.

Paper Structure. The paper contains nine sections and is structured as follows: Section 1 presents the introduction, contributions, and paper structure. Section 2 gives an overview of privacy and data protection laws. Section 3 presents the analysis process for the privacy and data protection laws of various countries using framework analysis. Section 4 presents an overview of the key principles and individuals' rights that resulted from the analysis process (i.e., Combined Privacy Law Framework (CPLF)). Section 5 discusses the results of the analysis of the various privacy and data protection laws. Section 6 presents an overview of Privacy by Design (PbD) and correlates the principles and rights of the CPLF and the principles, strategies, guidelines, and patterns of the PbD schemes. In Section 7, the IoT architectures of two scenarios are presented, and the position of the privacy patterns are demonstrated in these IoT architectures. Section 8 discusses the research challenges and opportunities. Finally, Section 9 sets out the conclusion.

2 OVERVIEW OF THE PRIVACY AND DATA PROTECTION LAWS

This section presents an overview of various privacy and data protection laws with their key principles and rights, which are: General Data Protection Regulations (GDPR), the Personal Information Protection and Electronic Documents Act (PIPEDA), California Consumer Privacy Act (CCPA), Australian Privacy Principles (APPs), and the New Zealand Privacy Act (1993) to present a comprehensive view of some of the privacy and data protection laws of key countries around the world, and to highlight any disparities, in order to assist developers in adhering to the regulations across different regions. It is important to understand each of these major privacy and data protection laws individually, before moving on to analyse them together in the subsequent sections. We acknowledge that there are many other laws around the world, such as the Cybersecurity Law of the People's Republic of China (CSL) [33] and the Protection of Personal Information Act of South Africa (POPIA) [50]. While the CSL provides data protection requirements for network operators, the POPIA sets out a general information protection mechanism for organizations in the public and private sectors. However, due to the limitation of space, we have chosen the most popular privacy and data protection laws from around the world, as approved by consulted privacy lawyers.

2.1 The General Data Protection Regulation (GDPR)

These regulations have applied since the 25th of May 2018, although they were entered into force on the 24th of May 2016. Their applicability under the General Data Protection Regulations means that there is a single set of data protection rules that all companies operating within the EU must adhere to. These regulations have strengthened the rights of individuals in accordance with the current digital age, along with providing clarity to businesses and public bodies operating within the single digital market of the EU. The key principles and rights of the GDPR are as follows [1]: **Key Principles:** (1) *Lawfulness, fairness and transparency*, (2) *Purpose limitation*, (3) *Data minimisation*, (4) *Accuracy*, (5) *Storage limitation, Disclosure, and Retention*, (6) *Integrity and*

confidentiality (security), and (7) *Accountability*; **Individuals' Rights:** (1)*The right of individuals to exercise their rights*, (2) *The right to be informed*, (3) *The right of access*, (4) *The right to rectification*, (5) *The right to erasure*, (6) *The right to restrict processing*, (7) *The right to data portability*, (8)*The right to object*, and (9) *The rights in relation to automated decision making and profiling.*

2.2 The Personal Information Protection and Electronic Documents Act (PIPEDA)

The Personal Information Protection and Electronic Documents Act (PIPEDA) was introduced in Canada and became law on the 13th of April 2000; it addresses federal privacy law for organisations in the private sector. The ground rules for how businesses should deal with personal information as part of their commercial activities, are set out. The act gives individuals more control over how the private sector handles their personal information [45]. The key principles [44] and rights [40] of the PIPEDA are as follows: **Key Principles:** (1) *Accountability*, (2) *Identifying Purposes*, (3) *Consent*, (4) *Limiting Collection*, (5) *Limiting Use, Disclosure, and Retention*, (6) *Accuracy*, (7) *Safeguards*, (8) *Openness*, (9) *Individual Access*, and (10) *Challenging Compliance*; **Individuals' Rights:** PIPEDA states that (1) *Private sector organisations must gather, and use or disclose, personal information using appropriate fair and lawful means, including gaining consent, and for reasonable and clear purposes,* (2) *Organisations must protect people's personal information by implementing effective security measures, and this data must be destroyed once it is no longer needed,* (3) *The individual has the right to expect that any personal information an organisation has about them is accurate and up to date,* (4) *The person has the right to see it, and if it is inaccurate, request that corrections are made,* and (5) *The person also has the right to withdraw their consent at any time, in accordance with legal or contractual restrictions and following reasonable notice.*

2.3 California Consumer Privacy Act (CCPA)

The right of privacy for Californians is granted by the California Constitution, which provides consumers with an effective way of controlling their personal information through upholding specific rights. This bill enacts the California Consumer Privacy Act of 2018, starting on January 1st, 2020. **Key Principles:** the CCPA grants Californians rights rather than principles [28]. **Individuals' Rights:** (1) *Californians have the right to know what personal information an organisation is collecting about them*, (2) *Californians have the right to know if their personal information has been sold or disclosed, and to who*, (3) *Californians have the right to refuse the sale of their personal information*, (4) *Californians have the right to gain access to their personal information*, and (5) *Californians have the right to equal services and prices, including if they decide to exercise these privacy rights.*

2.4 Australian Privacy Principles (APPs)

Australian Privacy Principles (APPs) provide the main privacy protection framework in the Privacy Act 1988 (Privacy Act), and they are applicable to all organisations and agencies that the Privacy Act covers. This gives the organisation or agency the flexibility to design their practices on personal information for inclusion in their business model to meet the varied needs of individuals [34]. The key principles [35] and rights [36] of the Privacy Act are as follows: **Key Principles:** (1) *Open and transparent management of personal information*, *(*2) *Anonymity and pseudonymity*, (3) *Collection of solicited personal information*, (4) *Dealing with unsolicited personal information*, (5) *Notification of the collection of personal information*, (6) *Use or disclosure of personal information*, (7) *Direct marketing*, (8) *Cross-border disclosure of personal information*, (9) *Adoption, Use or Disclosure of an identifier*, (10) *Quality of personal information*, (11) *Security of personal information* (12) *Access to personal information*, and (13) *Correction of personal information*; **Individuals' Rights:** the Privacy Act gives individuals more control over the way their personal information is managed, as it allows the person to: (1) *Find out why their personal information is being collected, and how it will be used,*

as well as who it will be disclosed to, (2) *The option of not being identified or using a pseudonym if possible*, (3) Request access to their personal information, including health information, (4) *Stop being sent unwanted direct marketing material*, (5) *Request that any personal information that is incorrect is corrected*, and (6) *Put in a complaint about an organisation or agency that the Privacy Act covers if they believe that their personal information has been handled inappropriately.*

2.5 New Zealand's Privacy Act 1993

The Privacy Act controls the way that agencies collect, use, disclose, store and provide access to individuals' personal information, and is relevant to all government departments, different size companies, schools, religious groups and clubs in New Zealand [38]. The key principle [42] and rights [39] of the Privacy Act are as follows: **Key Principles:** (1) *Purpose of collection* (2) *Source of information*, (3) *What to tell an individual*, (4) *Manner of collection*, (5) *Storage and security*, (6) Access, (7) *Correction*, (8) *Accuracy*, (9) *Retention*, (10) *Use*, (11) *Disclosure*, and (12) *Unique identifiers*; **Individuals' Rights:** the Privacy Act gives the right to: (1) *Access your information* and (2) *Ask for correction when it is wrong.*

3 ANALYSIS OF THE PRIVACY AND DATA PROTECTION LAWS OF VARIOUS COUNTRIES USING A FRAMEWORK ANALYSIS METHODOLOGY

The framework analysis [19] method has been developed by qualitative specialist researchers from the UK who work for an independent social research institute. The method involves five distinct phases, which are interlinked and provide a thorough methodical framework: (1) the familiarisation process, (2) developing a theoretical framework, (3) indexing, (4) charting and (5) synthesising the data. These phases allow the researcher to understand and interpret the data, shifting from mainly descriptive accounts to a conceptual explanation of the situation. Figure 1 presents an overview of the analysis process. The analysis in this research is based on the latest version of each law.

3.1 The Method

3.1.1 ***Familiarisation process:*** In the first stage, all the regulations from the privacy and data protection laws of the selected countries are read in order to attain a good understanding of these privacy and data protection laws.

3.1.2 ***Developing a theoretical framework:*** For the second stage, after becoming familiar with all five regulations, two key themes emerged to identify principles and rights. Each regulation from these issuers was read to identify its principles and rights. Using the Airtable tool, all the principles of a specific issuer were grouped together as sub-themes of the key theme principles in a single table, as well as the rights, where all the rights of a specific issuer were grouped together under the main themes. If there were two matching principles of different laws, the general name of a principle was chosen to identify that sub-theme. This step has been developed in stages by developing a theoretical framework containing all of the privacy and data protection laws from the countries specified above.

3.1.3 ***Indexing:*** This stage included a thorough reading of all the regulations. Since there are some variations in the concept of a specific principle or right between different issuers, a section was created for each sub-theme using the OneNote app in order to compare between the various issuers' laws concerning a specific principle/right. Each section was filled out using the defined principle or right of a specific law. If the issuer does not have a matched principle or right, the whole regulations would be read to find any matched provisions that could be assigned as the issuer's view of this principle/right. If there is no provision that can be assigned as the issuer's

view, N/A (Not Applicable) was assigned to that principle or the right of that regulation. Hence, the final table was developed in stages as part of the indexing process.

3.1.4 ***Charting:*** Once the data was indexed in accordance with the theoretical framework, it was summarised in thematic charts by cutting down the original data to form manageable sections of text which could be easily understood, before placing the appropriate theme into the theoretical framework chart. After filling out all of the principles or rights with the matching text, a general definition was given to each principle or right in order to gain an overview of the meaning of each, regardless of the slight differences between regulations. The charts were devised on a Word document. Each chart contains fields for the following information: (i) *Definition of a principle/right*, (ii) *The issuers' names*, (iii) *The article's number, recital name, principle number, or principle name*, (iv) *The name of the principle in that law*, and (v) *The quoted text that clarifies issuers' views on a specific principle/right.*

3.1.5 ***Synthesising the data:*** This phase involved re viewing the charts to ensure the data set made sense, before checking that the summaries on the charts matched the original data and conducting a comparison between the themes and sub-themes. This phase facilitated further revision of the quoted text from the regulation that was assigned to a specific law.

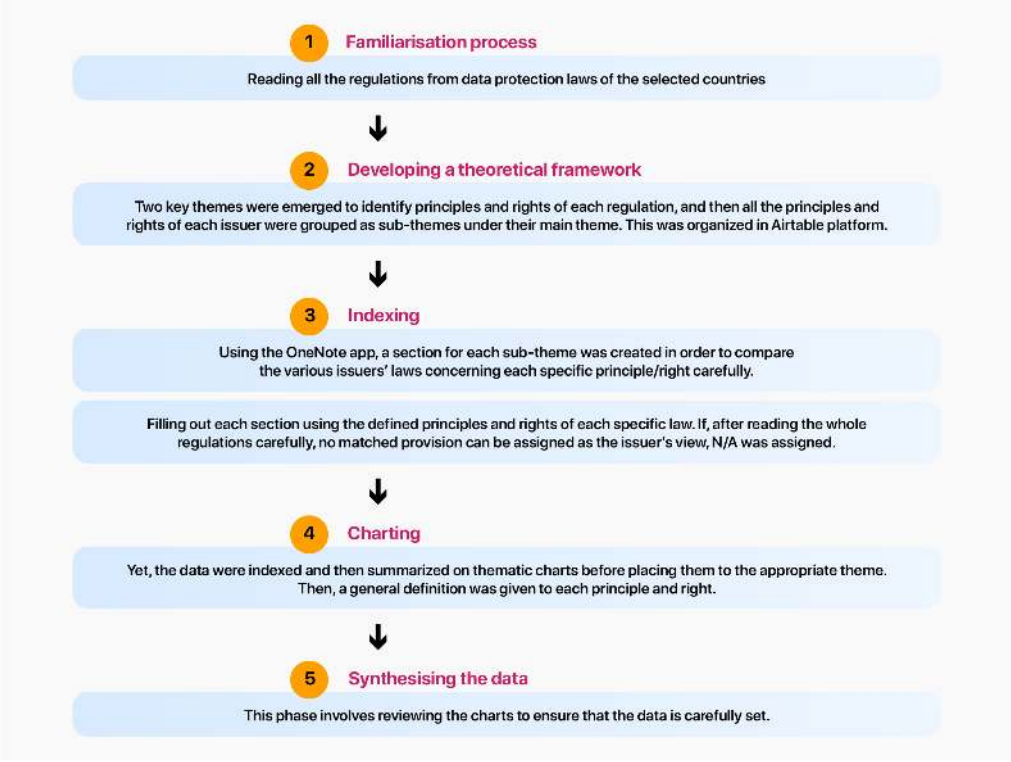

Fig. 1. Overview of the Analysis of the privacy and Data Protection Laws

4 RESULTS

This section presents an overview of each key principle and right that resulted from the analysis process, as explained in the previous section. The detailed results of the Combined Privacy Law Framework (CPLF) [2] are presented in the Technical Report [3].

4.1 Key principles

13 key principles emerged from the analysis process and have been defined as follows:

(1) ***Transparency principle:*** 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.
(2) ***Purpose Limitation Principle:*** 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.
(3) ***Limiting Use and Disclosure Principle:*** An organisation may only use or disclose personal information for the purposes for which it was collected.
(4) ***Data Minimisation Principle:*** Where personal data is required, it must be relevant, adequate and limited only to what is needed for the purpose stated.
(5) ***Consent Principle:*** The individual's consent is required for the collection, use, and/or disclosure of their personal information.
(6) ***Lawfulness of Processing Principle:*** Personal information must be processed by fair and lawful means.
(7) ***Accuracy Principle:*** 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.
(8) ***Storage Limitation Principle:*** Personal information must not be stored for longer than necessary once it has met the purposes for which it was collected.
(9) ***Security Principle:*** Safeguarding procedures must be in place to protect personal information and prevent its loss, misuse or disclosure.
(10) ***Accountability Principle:*** An organisation is responsible for complying with all privacy and 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.
(11) ***Anonymity and Pseudonymity Principle:*** Individuals must be given the option of not identifying themselves, or the choice of using a pseudonym, in relation to certain matters.
(12) ***Source Principle:*** Unless there is an exception, personal information must be collected from the person the information is about.
(13) ***Cross-border Transfer of the Personal Information Principle:*** Individuals' information is expected to be protected and handled appropriately, wherever the processing takes place.
(14) ***Dealing with Unsolicited Personal Data Principle:*** 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.'
(15) ***Adoption, Use or Disclosure of an identifier Principle:*** Adopting, using, or disclosing a unique identifier that was created for an individual for a different purpose should be prohibited.

4.2 Individuals' Rights

11 Individuals' rights emerged from the analysis process and have been defined as follows:

(1) ***Right of Individuals to Exercise their Rights:*** Individuals shall have the right to exercise their privacy and data protection rights.

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

(2) ***Right to be Informed:*** Individuals must be informed about the collection, use and/or disclosure of their personal information.
(3) ***Right of Individuals Access:*** Individuals have the right to access the personal information which an organisation is holding about them.
(4) ***Right to Rectification:*** Individuals shall have the right to ask for correction of their personal data.
(5) ***Right to Erasure:*** Individuals shall have the right to ask for deletion of their personal data.
(6) ***Right to Restriction of Processing:*** Individuals shall have the right to restrict the processing of their personal data.
(7) ***Right to Object:*** Individuals shall have the right to object to the processing of their personal data.
(8) ***Right to Object to Marketing:*** Individuals shall have the right to reject the processing of their personal data for direct marketing purposes.
(9) ***Right to Data Portability:*** 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.
(10) ***Right to Object to Automated Decision-Making:*** Individuals must have the right to object to a decision that is based solely on automated processing.
(11) ***Right to Withdraw Consent:*** Individuals shall have the right to withdraw consent at any time.
(12) ***Right to Complain:*** Every data subject shall have the right to lodge a complaint.
(13) ***Right of Individuals not to be Discriminated:*** A business shall not discriminate against a consumer because the consumer exercised any of their rights.

5 DISCUSSION

This section discusses the results of the comparison between the GDPR, PIPEDA, CCPA, Australia's Privacy Act 1988, and New Zealand's Privacy Act 1993 (the detailed results of the CPLF are presented in the Technical Report [3]). The Table 1 and Table 2 show an overview of the similarities and differences between the principles of the privacy and data protection laws selected for this study.

5.1 Scope of the Laws

The GDPR contains fully comprehensive data protection laws, although federal privacy law in the US, including the CCPA, are viewed as being the most important legislation on privacy developments in the country. Furthermore, while all of these five laws have similar core legal frameworks that aim to protect individuals' data, the CCPA is different from the other laws in a number of ways as it covers a different scope. In particular, this means that the GDPR, PIPEDA, APPs, and New Zealand Privacy Act (1993) articulate rules for organisations to comply with when processing personal data to protect individuals' privacy. The CCPA, however, only concerns individuals' rights, rather than guiding organisations.

As mentioned previously, the GDPR has a far wider scope compared to other laws. While the scope of New Zealand's Privacy Act (1993) is limited to its agencies, and the scope of the CCPA only covers businesses that do business in California and process Californian residents' data, the GDPR is applicable to all businesses, public bodies and institutions, including not-for-profit organisations. That is, an organisation that has been established in the EU and processes personal data, regardless of the location where that data is processed; organisations established outside of the EU that offer goods or services, whether paid for or free, or those monitoring the behaviour of individuals living in the EU. APPs has similarities to these scopes since it applies only to APPs' entities, and it covers acts that have been completed or engaged in, including those outside Australia and the

external territories, where the organisation has a link to Australia [37]. The PIPEDA, however, is restricted only to commercial organisations and for-profit activities, [43] and is applied to personal data that moves across provincial or national borders as part of the commercial transactions that organisations are involved in - subject to the act or similar legislation [41].

5.2 Key Principles

The CPLF is to a large extent similar in relation to their principles, even though they use different terms for naming those principles, and embed one principle under another one, have different conditions, or are broader than others (as highlighted in the Technical Report [3]). However, the CCPA differs from the other laws, as its primary focus is on sharing and selling rather than collection.

5.2.1 ***Transparency principle:*** With regard to the transparency principle, the GDPR, PIPEDA, APPs, and New Zealand's Privacy Act (1993) assert that the privacy policy has to be clear and easily accessible. In contrast, the CCPA does not mention this explicitly - only as a general desire for its data practices.

5.2.2 ***Purpose Limitation, Data Minimisation, and Limiting Use and Disclosure Principles:*** The GDPR, PIPEDA, APPs, and New Zealand's Privacy Act emphasise the need for the purpose of data collection to be stated before or during the time of collection. They require data to be collected for clearly specified legitimate purposes, and not used beyond that (used or disclosed) in a way that is not in line with the purposes set out. They also emphasise that the collection of personal information has to be limited only to what is necessary to fulfill the stated purpose. The APPs and New Zealand's Privacy Act clarify that the collection of personal information should be linked to a function or activity conducted by the organisation. However, the provision of the GDPR is wider, as it allows additional processing to archive data that is in the public interest; for scientific or historical research purposes, or for statistical reasons. Nevertheless, this must be done in accordance with specific conditions that are not incompatible with the purposes originally stated. Even though the CCPA does not have an equivalent provision that requires businesses to specify or identify its purposes, it asserts that it is mandatory to give the consumer notice when collecting or using extra categories of personal information for other purposes.

5.2.3 ***Storage Limitation Principle:*** Regarding storage limitation principle, the GDPR, PIPEDA, APPs, and New Zealand's Privacy Act assert that organisations must not keep personal information for longer than necessary, and it must be used only for the reasons it was collected for. The PIPEDA and APPs suggest destroying, erasing, or anonymising all personal information that an organisation no longer requires. The GDPR, however, allows personal data to remain if it needs to be archived. In contrast, the CCPA does not set out clear provisions for businesses for data retention, whereas service providers and third parties are prohibited from keeping, using, or disclosing personal information for any reason other than those specified for the services set out in the original business contract.

5.2.4 ***Consent Principle:*** While the GDPR, PIPEDA, CCPA, and APPs intrinsically require the consent of the individual for the collection, use and disclosure of personal information, their definitions of the word consent vary. The GDPR states that informed consent must be given freely, and its use must be specific and unambiguous; in addition, APPs bases consent on four elements: the individual is properly informed prior to giving consent; they provide consent voluntarily; consent is current and for a specific objective, and the individual must have the ability and capacity to understand and provide that consent. In a similar way, PIPEDA asserts that the consent should be meaningful. The CCPA, however, allows businesses to sell data from minors based on consent,

although this is only in reference to the sale of information, and is not required for collecting the information. All these laws articulate provisions regarding consent to process children's data. In contrast, New Zealand's Privacy Act does not require consent to be obtained by the agency, and it does not specify if consent to collect the information needs to be provided. In addition, it does not differentiate between information collected from adults or children. However, it does require agencies to take reasonable steps to ensure that the person is aware that they are collecting information from them.

5.2.5 ***Lawfulness of Processing Principle:*** The main operational differences between the GDPR and other laws discussed here concern the various approaches to the legal requirements to process data. The GDPR is much broader compared to the other laws as it allows organisations to gather, use and disclose personal information as long as one of the six grounds contained in Article 6 is met. Unlike the PIPEDA, APPs, and New Zealand's Privacy Act, they only require the collection of personal data to be lawful as a legal obligation. The CCPA, nevertheless, does not provide a clear list of grounds that organisations must adhere to collect information. It only requires businesses to maintain and use the consumer's personal information where necessary, for internal use, in a lawful manner that adheres with the context in which the consumer provided the information if none of the eight specified conditions is satisfied.

5.2.6 ***Accuracy Principle:*** With regard to the quality of the data, the accuracy of personal information is not considered under the CCPA, and neither is the ability of individuals to correct their information; whereas all the other laws in this study require personal data to be accurate, complete and up to date.

5.2.7 ***Security Principle:*** All the privacy and data protection laws in this research assert that organisations must ensure appropriate security when processing personal data. In case of any data breach, it is mandatory for organisations to notify the responsible authorities and individuals; unlike New Zealand's Privacy Act (1993), where data breach notification is voluntary. However, the New Zealand government's new Privacy Act will set out a requirement for data breaches to reported.

5.2.8 ***Accountability Principle:*** Regarding the accountability principle, organisations are responsible for complying with all privacy and data protection laws, including those for personal information under their control. The GDPR, PIPEDA, APPs, and New Zealand's Privacy Act (1993) also set out requirements regarding the appointment of data protection (privacy) officers, to ensure that they are obliged to follow the law. Nonetheless, the CCPA does not focus on obligations related to accountability specifically, although a business or third party can ask the opinion of the Attorney General to obtain guidance on how to properly comply with the provision.

5.2.9 ***Anonymity and Pseudonymity Principle:*** The APPs includes a key principle regarding anonymity and pseudonymity, allowing individuals to have the option of not being identified, or the use of a pseudonym, that is, provided there is no listed exception applicable. The CCPA does not clarify whether its obligations are applicable to personal information that has been given a pseudonym. As with the GDPR and PIPEDA, their provisions contain no direct analog about applying anonymity and pseudonymity where the organisation no longer needs to process personal data. New Zealand's Privacy Act does not, however, have an equivalent principle.

5.2.10 ***Source Principle:*** Both the APPs and New Zealand's Privacy Act require collecting personal information directly from the individual, unless an exception applies. The GDPR does not have a similar principle, however, the data controller must provide the subject whose data they are dealing with, with information if that personal data has not been obtained directly from them. In

the same way, provisions in the PIPEDA and CCPA require organisations to declare the source of this information should the individual request it.

5.2.11 ***Cross-border Transfer of the Personal Information Principle:*** The cross-border transfer of personal information is permitted under the GDPR, PIPEDA, APPs, and New Zealand's Privacy ACT (1993). They require that the rules that protect personal data apply on an ongoing basis, wherever the data ends up, and it is required to take reasonable steps to prevent any overseas recipient from breaching the regulations covering the information. In contrast, the CCPA does not restrict a business collecting or selling personal information if all aspects of that commercial conduct are conducted outside California.

5.2.12 ***Dealing with Unsolicited Personal Data Principle:*** APPs has a key principle regarding the case of dealing with unsolicited personal data, as an entity is required to destroy or de-identify information that may not have otherwise been collected in accordance with the collection of solicited personal data. This situation, however, is not mentioned in all the other laws.

5.2.13 ***Adoption, Use or Disclosure of an identifier Principle.*** When it comes to adopting a unique identifier, whether it is a government related identifier or an identifier that was created for a different purpose, this is prohibited by the PIPEDA, APPs, and New Zealand's Privacy Act. This is unlike the GDPR, which sets out specific conditions for processing national identification numbers and any other identifiers of general application, and restricts using it under relevant safeguarding guidelines. In contrast, the CCPA does not mention any regulations related to this principle, and this could be related to the nature of its legislation.

Table 1 shows an overview of the similarities and differences between the principles of the privacy and data protection laws selected for this study according to the following criteria:

✓	If the issuer's view agrees with the concept of this key principle/right
☑	If the issuer's view is not explicitly stated but agrees with the concept of this key principle/right being inferred from such a provision
N/M	If a regulation contains an explicitly stated provision for a different context from this key principle/right
N/A	If no provision can be assigned as the issuer's view and there is no contradiction with this principle/right

5.3 Individuals' Rights

There are similarities and differences between the rights of the CPLF, which will be discussed below (based on the detailed results shown in the Technical Report [3]).

5.3.1 ***Right of Individuals to Exercise their Rights:*** Individuals have the right to exercise their rights. All the laws in this study require organisations to ensure the exercise of individual rights and to take reasonable steps to put practices, procedures and systems in place that enable them to deal with relevant inquiries and complaints, even though they have differences regarding the way and the condition of responding to individuals' requests.

5.3.2 ***Right of Individuals Access:*** Regarding individuals' right of access, all the privacy and data protection laws grant right of access if a request is made by an individual, unless there is an exception, thereby allowing the individual to view all of the data an organisation is holding about them. Individuals may obtain details about the data that is being processed, and can have access to copies of the data that concerns them. Accessing the information is free of charge, at least for the first time, except for PIPEDA, which allows organisations to grant individuals free access or charge

Table 1. Overview of the Principles

Principle	GDPR	PIPEDA	CCPA	APPS	New Zealand
Transparency	✓	✓	☑	✓	✓
Purpose Limitation	✓	✓	✓	✓	✓
Limiting Use, Disclosure	✓	✓	✓	✓	✓
Data Minimisation	✓	✓	✓	✓	✓
Consent	✓	✓	✓	✓	N/A
Lawfulness of processing	✓	✓	☑	✓	✓
Accuracy	✓	✓	N/A	✓	✓
Storage Limitation	✓	✓	☑	✓	✓
Security	✓	✓	☑	✓	✓
Accountability	✓	✓	✓	✓	✓
Anonymity and Pseudonymity	N/M	N/M	N/M	✓	N/A
Source	✓	✓	✓	✓	✓
Cross-border Disclosure of Personal Information	✓	✓	N/A	✓	✓
Dealing with Unsolicited Personal Information	N/A	N/A	N/A	✓	N/A
Adoption, Use or Disclosure of an identifier	✓	✓	N/A	✓	✓

them a minimal fee. There are, furthermore, some differences, such as regarding the procedure organisations must comply with to respond to an individual's request.

5.3.3 ***Right to Rectification:*** Based on the individuals' right of access, the GDPR, PIPEDA, APPs, and New Zealand's Privacy Act provide individuals the right of correction of personal data that an organisation holds. The GDPR sets out a stronger right, as subjects have the 'right to obtain from the controller without undue delay the rectification to inaccurate personal data concerning him or her'. In contrast to the CCPA, which does not have an equivalent right.

5.3.4 ***Right to be Informed:*** All of the privacy and data protection laws in this study contain prescriptive provisions about the information organisations must provide when collecting and processing individuals' personal information. Moreover, all of the legislation states when information should be provided to individuals and what they should be told about. On the other hand, the GDPR, the CCPA, PIPEDA, APPs, and New Zealand's Privacy Act do not distinguish between the notice given for collecting information directly from individuals, and the notice necessary for information obtained from other sources.

5.3.5 ***Right to Erasure:*** The GDPR and the CCPA both permit individuals to ask for the deletion of their personal information, apart from where exceptions apply. This right is similar in both pieces of legislation, although the applicability and exemptions are slightly different. The GDPR contains the right to the erasure of information (sometimes called the right to be forgotten), and states that the data controller must erase personal data without any unnecessary delay in a range of situations, for example when it is no longer needed for the purpose it was collected, or if the subject withdraws

their consent or objects to the information being processed. Regarding the PIPEDA, APPs, and New Zealand's Privacy Act, individuals do not have clear rights in these laws regarding organisations destroying or de-identifying their information. These laws, however, require organisations to destroy, erase or anonymise personal information that they do not need any more. The PIPEDA, nonetheless, states that it is obligatory for organisations to amend the information if an individual clearly demonstrates the personal information is inaccurate or incomplete. Depending on the nature of the information that is being challenged, the amendment may involve deletion, correction or the adding of information.

5.3.6 ***Right to Restriction of Processing:*** The GDPR grants individuals the right to restriction of processing for their personal data when one of the specified cases applies. In contrast, the PIPEDA, CCPA, APPs, and New Zealand's Privacy Act do not contain the right to restrict data processing.

5.3.7 ***Right to Object, Right to Withdraw Consent, and Right to Object to Automated Decision-Making:*** The GDBR and the CCPA guarantee the right to individuals to request that an organisation stops the processing and selling of their data. The CCPA allows consumers only to opt-out of their personal data being sold, and not collection or other uses that fall outside the definition of selling. In contrast, individuals are allowed to object to any type of processing of their personal data according to the GDPR, including by withdrawing consent or by objecting to its processing, provided the request is based on a legitimate reason, and does not affect the public interest. However, there are no similar provisions regarding the right to object in the PIPEDA, APPs, and New Zealand's Privacy Act. Rather, the provisions in these laws grant individuals the right to withdraw consent at any time. Moreover, for automated processing, while the GDPR grants individuals the right to object to a decision solely based on automated processing, none of the other laws in this study consider this a right.

5.3.8 ***Right to Object to Marketing:*** APPs states that an organisation cannot use or disclose personal information about an individual for direct marketing purposes, and organisations are required to provide a simple method for individuals to ask not to be sent direct marketing communications (known as 'opting out'). Similar to the GDPR, it grants data subjects, among other things, the right to object to their data being processed for direct marketing purposes. Like the CCPA, it is the consumer's right to opt-out of selling their personal information, as well as opting out from the subsequent sale of their personal information by a third party that is given the personal information after its initial sale. In contrast, both the PIPEDA and the New Zealand Privacy Act do not have an equivalent right to object to personal data being used for direct marketing purposes.

5.3.9 ***Right to Data Portability:*** The GDPR and the CCPA recognise the right to data portability, as the CCPA views data portability as being part of the right to access, and the GDPR sets out a separate and distinct right. The PIPEDA, APPs, and New Zealand Privacy Act, nevertheless, do not provide equivalent rights to data portability.

5.3.10 ***Right to Complain:*** All the laws in this study grant individuals the right to lodge a complaint, even though they have differences in their procedures. The PIPEDA, APPs, and New Zealand's Privacy Act encourage individuals, if they have concerns about their personal information being mishandled, to firstly resolve privacy issues directly with the organisation. This is unlike the GDPR and the CCPA, which suggest lodging a complaint to a supervisory authority or to the Attorney General, respectively.

5.3.11 ***Right of Individuals not to be Discriminated:*** In respect of protecting individuals from many consequences, the CCPA contains the right to not be subject to discrimination when exercising their rights, but this right is not supported in the other laws mentioned.

Table 2 presents an overview of the similarities and differences between the rights of the privacy and data protection laws selected for this study according to the following criteria, which is the same as the criteria that were applied to the principles before:

✓	If the issuer's view agrees with the concept of this key principle/right
☑	If the issuer's view is not explicitly stated but agrees with the concept of this key principle/right being inferred from such a provision
N/M	If a regulation contains an explicitly stated provision for a different context from this key principle/right
N/A	If no provision can be assigned as the issuer's view and there is no contradiction with this principle/right

Table 2. Overview of the Rights

Individual Rights	GDPR	PIPEDA	CCPA	APPS	New Zealand
Right of Individuals to Exercise Their Rights	✓	✓	✓	✓	✓
Right to be Informed	✓	✓	✓	✓	✓
Right of Individuals Access	✓	✓	✓	✓	✓
Right to Rectification	✓	✓	N/A	✓	✓
Right to Erasure	✓	☑	✓	N/M	N/M
Right to Restriction of Processing	✓	N/A	N/A	N/A	N/A
Right to Object	✓	☑	☑	☑	☑
Right to Object to Marketing	✓	N/A	☑	✓	N/A
Right to Data Portability	✓	N/A	✓	N/A	N/A
Right to Object to Automated Decision-Making	✓	N/A	N/A	N/A	N/A
Right to Withdraw Consent	✓	✓	✓	✓	✓
Right to Complain	✓	✓	✓	✓	✓
Right of individuals not to be Discriminated	N/A	N/A	✓	N/A	N/A

6 DATA PROTECTION BY DESIGN AND BY DEFAULT AND PRIVACY BY DESIGN SCHEMES

In the previous sections, a Combined Privacy Law Framework (CPLF) was developed by analysing and synthesising five major Privacy and Data Protection laws together. This section presents an overview of Data Protection by Design and Default and an overview of Privacy by Design (PbD) techniques and correlates PbD techniques with the principles and the rights of the CPLF in order to investigate the gap in the previous techniques.

6.1 Privacy by Design and Data Protection by Design and by Default

This section presents an overview of the Privacy by Design (PbD) and Data Protection by Design and by Default concepts. Cavoukian [12] developed Privacy by design (PbD) concept before the GDPR, and other national privacy and data protection laws selected for this study, came into force. This concept by Cavoukian suggests that the privacy, as well as friendliness, of IT systems, can be improved by the Privacy by Design (PbD) system [12], based on its design philosophy. This system design has a major impact on privacy and security, which is a key issue affecting the core properties of a system. Privacy protection, therefore, is not something that should be considered to be an add-on; rather, privacy should take priority from the outset. Data protection authorities are addressing issues around Data Protection by Design and by Default (DPbD) [17, 25] and they are supported by the European Commission [16, 18] furthermore, data protection for DPbD is legally required by GDPR [1]. It is important that due consideration of privacy is given during the early stages of the design process for DPbD, and not applied later on as a bolt-on to meet compliance. It is also essential to ensure that all of the personal data that is required for each specific stage of processing is dealt with appropriately. DPbD supports system security, along with a range of data protection measures, for example, data minimisation, pseudonymisation, and transparency. While the legal requirement for DPbD should be enough of an incentive for developers to accept its core principles, its widespread adoption has not yet been proven with regard to engineering processes [30]. This could be because its principles are rather disconnected from the real-life practice of systems engineering. In addition, it can be difficult to translate between the some of the vague terminology contained in the regulations [30]. The meaning of the concepts of Privacy by Design and by Default developed by Cavoukian and GDPR is similar, but they differ in regard to structure. The GDPR, as identified in Article 25 [1], includes "by Default" in its concept and has merged the by Design and by Default concepts in one article; while "Privacy as the Default Setting" has been identified by Cavoukian as one of its principles within the Privacy by Design Scheme [12] as presented in the Technical Report by [3]. Regarding the other laws selected for this study, APPs [58], PIPEDA [26] and New Zealand [32] have agreed on the notion of Privacy by Design, with the latter agreeing on the concepts suggested by Cavoukian [12]. However, the CCPA has not discussed this concept at all.

Perera et al., explain the various terms used in the literature on privacy by design (PbD) techniques, such as principle, strategies, patterns, and tactics [47]. As demonstrated in Figure 2, principles may represent high level, even abstract, ideas and concepts [47]. On the other hand, tactics are specific low level instructions required to implement solutions within a particular context. Furthermore, strategies, guidelines and patterns are situated between these. It should be borne in mind that the difference does not make one type better or worse than the other, as each layer has its own specif strengths and weaknesses. That is, bottom layer tactics facilitate specific solutions to solve specific problems, compared to top layer principles which give insights concerning the general direction that can be taken for further exploration and to solve problems. However, it should be noted that there are some soft boundaries between these layers, as some principles can be interpreted as strategies and vice-versa [47].

Principle: A principle provides a conceptualisation or value used for guiding behaviour or an evaluation. They are usually highly abstract, but provide the overall direction to be followed [47].

Strategies: Unlike principles, strategies focus on reaching a specific outcome, and the design strategy sets out the main approach that should be used to reach a particular design goal. This makes strategies more specific with regard to their aims and goals [23].

Guidelines: Guidelines are used to break down the strategy being followed into lower-level clear instructions that can be followed by the software engineer [47].

Patterns: Design patterns provide a useful way of making decisions about the software system used by an organisation. A design pattern provides a scheme for refining the subsystems or components of a software system, or the relationships between them. It describes a commonly recurring structure of communicating components that solves a general design problem within a particular context [10].

Tactics: Tactics are used to build patterns; to explain, if we imagine a pattern is a molecule, a tactic is an atom made up of the former [9]. That is, patterns are made up of several tactics combined to solve a certain problem. Tactics assist in fine tuning patterns and usually focus on specific attributes and influence trade-off decisions [47].

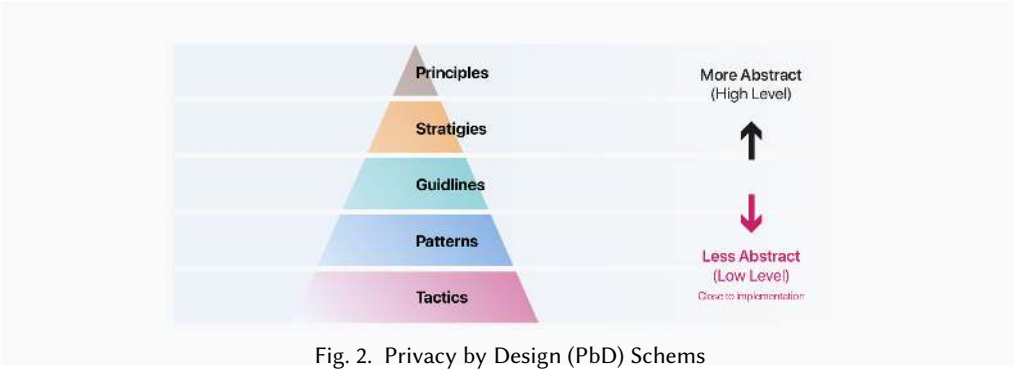

Fig. 2. Privacy by Design (PbD) Schems

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

Privacy by Design (PbD) schemes are produced by various parties (PbD schemes are listed in the Technical Report [3]). Even though all of these schemes aim at guiding software designers and developers to build privacy aware applications, each party has its own frame. Because there are numerous variations in originating contexts, as well as differing aims, each scheme is designed to be able to work in isolation without being fully connected to another. This disconnected view means that understanding different PbD schemes is hard, confusing and frustrating, as is proposing new schemes to fill any existing gaps. Furthermore, these schemes are not only disconnected from each other, but they are also disconnected from the CPLF. Accordingly, this section addresses this issue by synthesising and modelling key PbD schemes into one single knowledge base. The knowledge base not only captures the relationship between various privacy schemes, but it also correlates the principles [11–13, 62, 64], strategies [23, 57], guidelines [15, 47] and patterns [51, 52] of the PbD schemes with the principles and rights of the CPLF. The correlation of principles, guidelines, and strategies are based on large similarities between the description of each principle and right of the CPLF, with the description of each principle, guideline, and strategy of the PbD schemes. Due to space limitations, Figure 4 shows a visualised image of the mapping process (the mapping process are shown in details in the Technical Report [3]). With regards to the privacy patterns, since they are more concrete than the other schemes, a set of criteria is followed when mapping between the privacy and data protection laws and the privacy patterns. Figure 3 demonstrates a visualised image of the mapping between the principles and the rights of the CPLF and the privacy patterns. Details of the mapping are demonstrated in Tables in the Technical Report [3] because of space limitations.

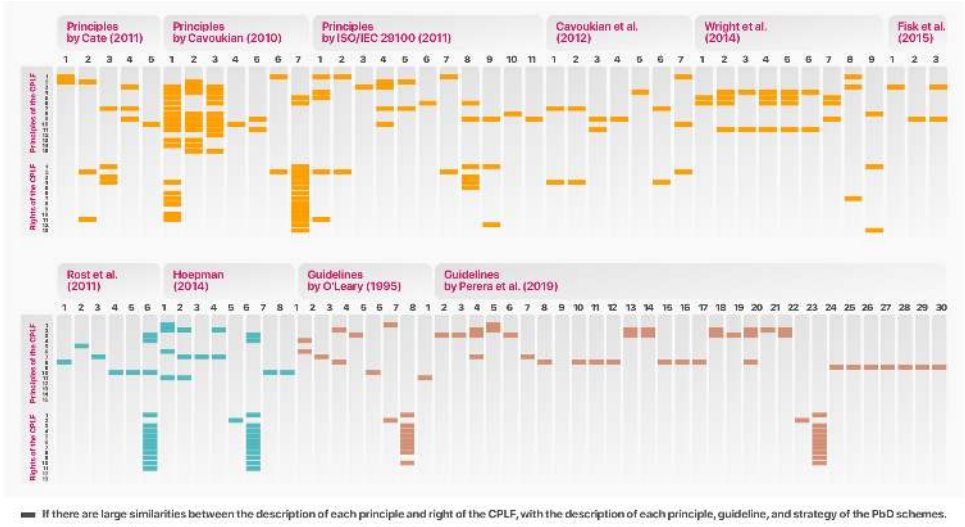

Fig. 3. We took each element (i.e., Principles/Rights) in our CPLF (Combined Privacy Law Framework) and analysed them against all the elements (i.e., PbD principles, strategies, guidelines) within different PbD schemes. This is a visual representation and a placeholder. Please read our Technical Report [3] for details. By doing so, our objective was to understand how different elements within different PbD schemes could help to facilitate common privacy and data protection laws (principles and rights). We argue that, software developers could use our mappings [3] to understand and select PbD schemes and patterns that are helpful to facilitate different privacy and data protection laws within a given IoT application design.

7 INTERNET OF THINGS ARCHITECTURE

This section briefly presents an overview of the IoT in general and its architecture, and demonstrates how to apply and map privacy patterns to IoT architectures at the design stage. The Internet of Things (IoT) may be described as a collection of physical objects or 'things' that are interconnected and have abilities involving computing, and sensing and actuation, along with being able to communicate with each other and different systems in order to exchange information and collect data [49, 54]. Designing and developing processes for IoT applications is more complex than for desktop, mobile or web applications due to several reasons. Firstly, for IoT applications, it is necessary to have both software and hardware, such as sensors and actuators, which can work together across various types of nodes. These include system-on-chips, mobile phones, and cloud platforms, which have a range of capabilities according to the specific condition [48]. Secondly, developing IoT applications requires different software engineering experts, for example, desktop, mobile or web, to work together. This leads to a complex situation as the different software engineering specialists collaborate in order to combine the various types of hardware and software necessary. Moreover, the situation is yet more difficult due to a lack of integrated development stacks for supporting the engineering of end-to-end IoT applications.

7.1 Overview of the Internet of Things (IoT) Software Architecture

Data is typically moved from sensing devices to gateway devices, and to the cloud infrastructure in IoT applications [48], which is the most commonly used architectural pattern for IoT application development; it is known as a centralised architecture pattern [56]. This pattern is usually made up of three components, which are IoT devices; gateway devices, and IoT cloud platforms, and

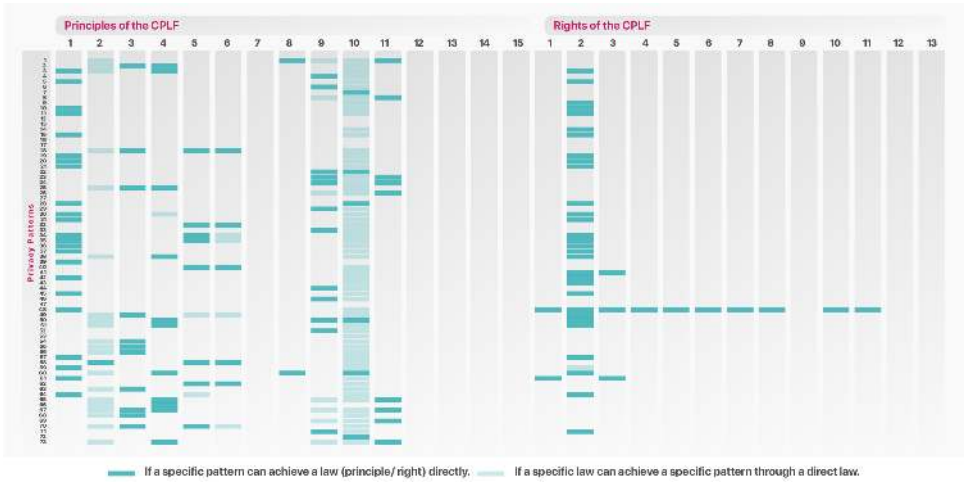

Fig. 4. We took each privacy pattern (73 privacy patterns proposed in the literature) and analysed them against each element (i.e., Principles/Rights) in our CPLF. By doing so, our objective was to understand how different patterns implicitly help to facilitate common privacy and data protection laws (principles and rights). Please read our Technical Report [3] for details. We argue that, software developers could use our mappings [3] to understand and select PbD schemes and patterns that are helpful to facilitate different privacy and data protection laws within a given IoT application design.

these all differ in their computational capabilities. An IoT application usually integrates the various types of devices with their different capabilities [21, 47]. It should also be borne in mind that each requires specific privacy protection measures to be taken into account according to their individual characteristics.

The five phases of the data lifecycle is defined as ensuring a systematic approach to thinking about the data flow for the application of our PbD framework within an IoT system. In all of the devices, or nodes, the data passes through five data life cycle phases, which are: Consent and Data Acquisition (CDA), Data Preprocessing (DPP), Data Processing and Analysis (DPA), Data Storage (DS) and Data Dissemination (DD). The CDA phase consists of routing and data collection activities performed by a specific node. DPP refers to any type of processing of raw data in preparation for it being used with a different processing procedure [68]. In general, DPA involves collecting and manipulating data items to attain meaningful information [63]. DD refers to distributing or transmitting data to an external party. These life cycle phases of the data are applicable to all of the nodes contained in an IoT application, and they allow software engineers to implement the mechanisms necessary to protect users' privacy. Even so, due to the decision of the engineers, certain data lifecycle phases in some nodes are not always utilised, for example, a sensor node may simply be used in the DPP phase for averaging out temperature data. This may be followed by either the DPA or DS phases involving analysing or storing the data, and because of hardware and energy constraints, the sensor node can push the data that has been averaged to the gateway node through the DD phase.

7.2 Example of IoT scenarios

In this section, two case scenarios are presented along with their Business Process Model Notation (BPMN) diagrams in order to define their process workflow. Those scenarios will be used later on to highlight the privacy challenges and to demonstrate how to apply various privacy patterns

to the data flow of the IoT architecture. As stated previously, privacy patterns are more concrete compared to principles, strategies, and guidelines. This allows consideration of the perspective of the owner with the problem, with the opportunity for each problem to be solved through the development of an IoT application.

7.2.1 ***Use Case 1: Car Finder.*** This use case is inspired by 'Carfinder' project which has been designed and implemented by IBM® and IBM Business BM Business Partner Zebra Technologies in cooperation with AUDI, as a solution for vehicle tracking in real time [66].

Summary of the Use Case: People often park their cars in different places and can forget where they parked it and may even have no idea where to even begin to finding it. IoT provides a good solution to help people easily find their car. As shown in Figure 5, the car is equipped with a sensor that reports a GPS location. There is also an IoT gateway inside the car, which is operated by the car company and is capable of communicating with the sensor via Bluetooth. The GPS sensor processes the car's location once a person parks his/her car. The GPS sensor then transfers the car's location once it is requested by the IoT gateway. Next, the IoT Gateway transfers the car's location and the gateway ID to the cloud through an Internet connection when requested. The cloud provides data storage service to store the location of the car and the gateway ID in the users' profile. Once the person needs to know his/her car location, he/she can easily access their mobile application on the mobile device and request the car location through a WiFi or mobile connection. In turn, the cloud will process the user ID of the mobile application, and if it is valid, the cloud will respond to the mobile application with the car's location. In addition, the cloud provides computing resources service to analyse the collected car's locations for future suggestions.

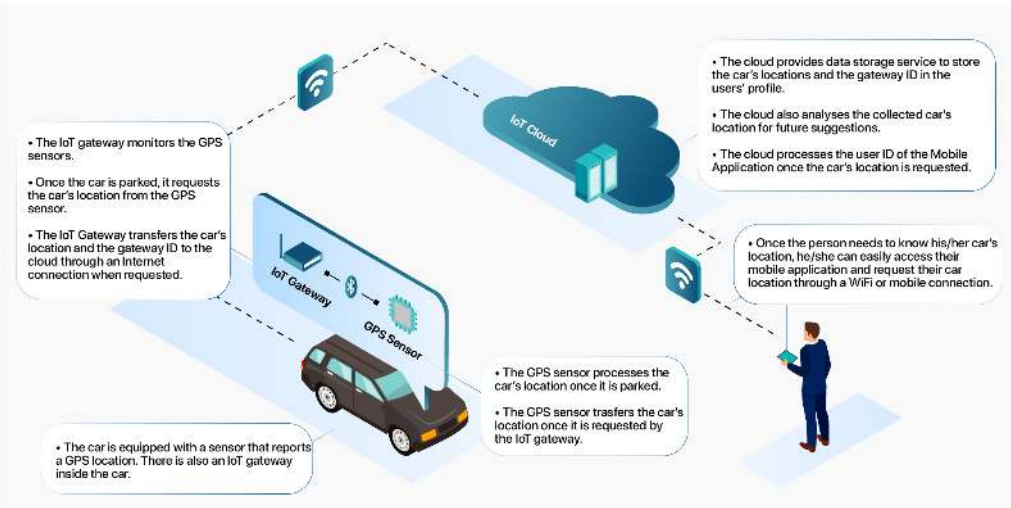

Fig. 5. Use Case 1: Car Finder

The business process model depicted, as demonstrated in Figures 6 and 8 involves four pools, one for each device/service. Each pool has a number of activities in boxes and circles, some handled by external entities such as humans, and some automated. Activities with boxes with dark envelopes show both data transfer and data requests. Those with green circles with envelopes show received messages. The activities marked with service icons in boxes are automatically undertaken or processed by the system; and those marked with a hand icon are undertaken manually by an external entity (e.g., human or agent). The solid arrows between activities denote their sequence in

a design pattern. Each activity may use or produce data recorded on databases, demonstrated by dashed arrows. Finally, the conditions are represented by rhombus notations with cross icon and parallel executions illustrated by rhombus notations with a plus icon.

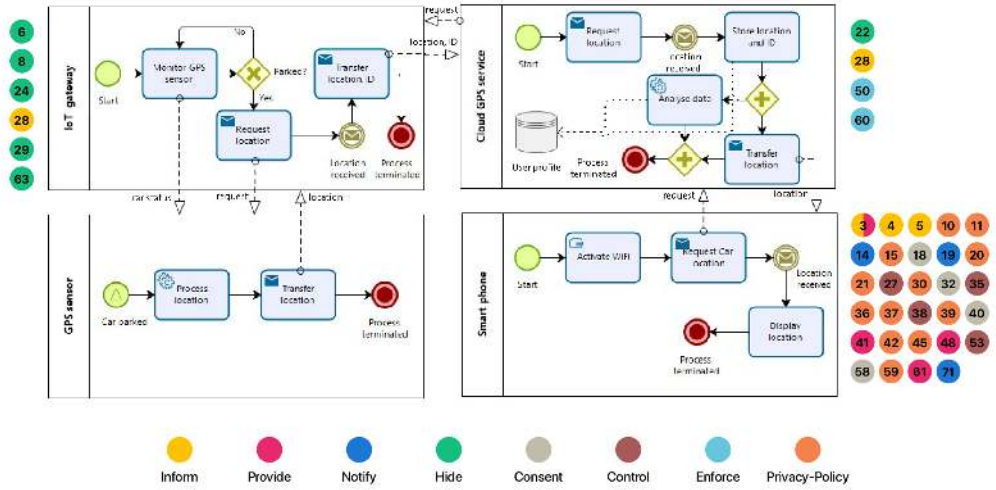

Fig. 6. Business Process Model Notation of the car Finder Use Case with Classified Privacy Patterns based on their purposes

7.2.2 ***Use Case 2: Gym Monitoring System.*** This use case is inspired by smart watches available in the market.

Summary of the Use Case: Sara is a trainer in a gym who faces difficulties in managing the high number of participants in the gym at the same time. Smart Gym is a helpful IoT solution that facilitates trainers managing gym participants and monitoring their progress easily. As shown in Figure 7, within the gym there are two different use cases: **(1)** some participants only use a smart watch, **(2)** and some participants use a smart watch together with a Heart Rate monitor chest strap. As stated previously in Section 7.1, different nodes do different kinds of processing based on their capabilities. Gym Activity is a third-party application that can be used by the participants and a trainer in the gym to monitor their activities. Accordingly, each use case has its own flow as follows:

(1) **Smart Watch Use Case:** Each participant wears a smart watch that includes multiple sensors (e.g., heart rate monitor, GPS, accelerometer) to collect data. These collected data are used to monitor activities, such as how many steps taken, the distance covered, the calories burned, and what the person's heart rate is. Once a participant starts a workout, the Gym Activity application on the participant's smart Watch sends a notification via Bluetooth to the trainer's smart phone which informs her that the participant has started the workout. The trainer, accordingly, can reply with a motivational message to the participant's smart Watch. While the participant starts a workout, the sensor displays a real-time heart rate, the active calories, the distance covered and the total time, on their smart Watch. In case a participant has an emergency situation, an alert is sent to the trainer's smart phone. Once a participant has completed the workout, the Gym Activity application on the smart Watch transfers the average heart rate collected and the average calories burned through Wi-Fi to the local server at the gym, as demonstrated

in Figures 7 and 8. Simultaneously, the Gym Activity application on the smart Watch sends a notification to the trainer's smart phone to inform her that the participant has completed the workout, along with a summary of the workout: the total time, the total calories, and the average heart rate.

(2) **Smart Watch together with the Chest Strap Use Case:** In this case, each participant wears a smart watch together with the Polar H7/H10 heart rate sensor with a chest strap for those who prefer an additional layer of accuracy. Smart watch has the ability to pear with Polar H7/H10 heart rate sensor. Therefore, the participants have to pair the smart Watch with the chest strap device via Bluetooth in order to synchronize the Heart Rate data to the Gym Activity application on the smart Watch and modify the required settings in the application. The complete case would be the same as the previous case.

In both two cases, the Gym Activity application allows the participant to create an account and enter their name, weight, height and age. It also allows participants to display the following information: average heart rate, active calories, and the distances covered. In addition, the participant can present visualised data from previous workout history that displays the statistics of the total calorie losses, and the average heart rate since the participant started. Gym participants can, furthermore, share their workout statistics, their progress of losing weight, and pictures of their body to encourage their friends in the gym. In order for the trainer to improve their participant's progress, the trainer could do advanced analysis on the cloud of their participant's data and suggest different plans for the workout in order to improve their progress, or they could store the workouts in the cloud for archiving purposes.

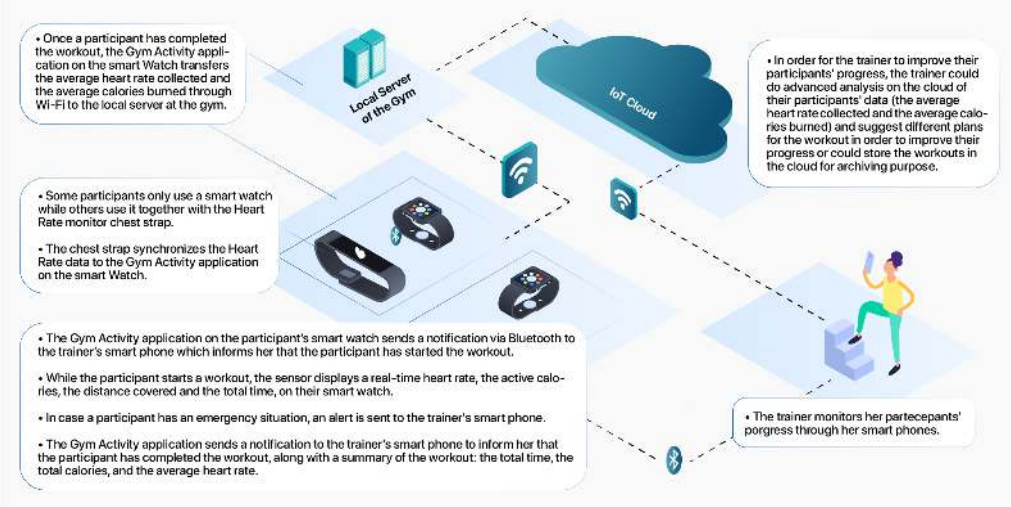

Fig. 7. Use Case 2: Gym Monitoring System

7.3 Mapping Privacy Patterns to IoT architecture

A major problem is that the owner typically focuses on the requirements that would help to address their problem [9] without consideration of privacy issues. Hence, privacy requirements are often overlooked during the design of software architectures for IoT applications. While these devices bring about new services, increase convenience, and improve efficiency, they also bring privacy and security risks. This section aims at guiding developers by demonstrating how to apply the privacy

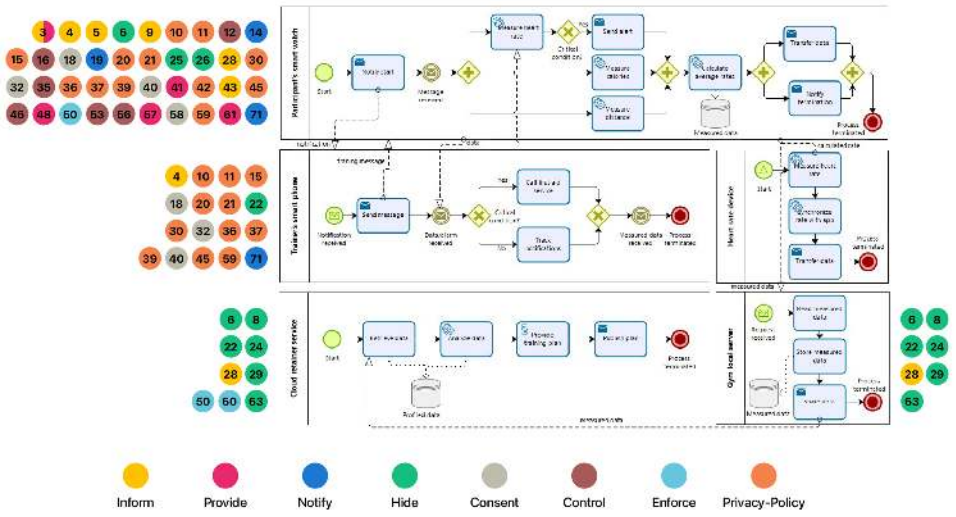

Fig. 8. Business Process Model Notation of the Gym Monitoring system Use Case with Classified Privacy Patterns based on their purposes

patterns to IoT architecture for the two IoT scenarios presented in Section 7.2 and demonstrated in Figures 6 and 8.

7.3.1 ***Mapping Privacy Patterns to the Car Finder Use Case.*** As this IoT solution collects the user's location, which could identify the user and cause a risk to the user's privacy, it is imperative to apply the privacy patterns to the flow of data, not only to protect user's privacy, but also to comply with the privacy and data protection laws. To highlight the way this may work in reality, the next section will examine the previous scenario presented in Section 7.2.2 and apply privacy patterns for developing a privacy-aware IoT application.

It is important to note that different types of privacy protecting measures can be taken for each of these different components based on their characteristics. Applying various privacy patterns would facilitate developers complying with the privacy and data protection laws. When developers apply a specific pattern, it automatically complies with some of the principles or rights of the privacy and data protection laws (as demonstrated in the Technical Report [3]). As shown in Figure 6, when the user receives the car location, the route the data travels is complex as it needs to go through different nodes before reaching its final destination. Taking into consideration the privacy requirements at each element of IoT architecture would help developers to build a privacy-aware IoT application.

(1) **Applying Privacy Patterns to the IoT Gateway:**
When the IoT gateway receives the car location from the GPS sensor, privacy pattern number 6 – **Encryption with a User-managed Key** – ensures personal information that could be transferred or stored by an untrustworthy third party is kept confidential. As data is routed between different nodes, applying pattern 24 – **Onion Routing** – to the data would encapsulate the data within a number of layers of encryption, thereby limiting the amount of knowledge in each node located along the delivery path. This, in turn, would help developers to comply directly with the security principles of the CPLF. In addition, since the exact location of the car should

be stored, it is worth applying pattern 8 – **Use of Dummies** –, which simultaneously adds fake locations in such a way that the third party is unable to distinguish fake from real information. Accordingly, applying these privacy patterns would help developers to directly comply with the Security and Anonymity and Pseudonymity principles of the CPLF. According to pattern 28 – **Trust Evaluation of Services Slides** –, it is important for the user to trust the service does not negatively impact their particular privacy requirements. Hence, a trust evaluation function needs to be used that is in accordance with relevant parameters for measuring how trustworthy communication partners are and to establish their reliability. Accordingly, it helps developers to directly adhere to the Transparency and Accountability principles of the CPLF and granting users the Right to be Informed. As a third party aims to meet the operating requirements, it is important to apply privacy pattern 29 – **Aggregation Gateway** – which uses homomorphic encryption by using a secret question and answer shared only with the third party that is working on enhancing the system. This third-party will not know what the content is due to it being encrypted, yet it can still work on that data in an encrypted format because the encryption system is homomorphic. This encryption prevents any revealing of the user's information, such as the user's habits in this scenario as it collects the car's location. By applying this pattern, the service provider would comply with the security principle of the CPLF directly.
In order to avoid any exploitation of information that could infer sensitive user information, applying privacy pattern 63 – **Added-noise Measurement Obfuscation** – is necessary to avoid this privacy issue. As this pattern seeks to add some noise to the service operation, for example, storing fake parking locations, no extra personal information may be inferred based on the aggregation of the user's information, such as what time they leave or return home. This would result in complying with the principle of Limiting Use and Disclosure of the CPLF directly.

(2) **Applying Privacy Patterns to the IoT Cloud:**
As this IoT scenario requires storing the car's location for the user, which could cause a risk to the user's privacy when any data breach occurs, it is crucial to apply privacy pattern 22 – **Data Breach Notification Pattern** –, to detect and react to a data breach quickly, since it could identify users' locations. This, in turn, would help developers in complying with the Security and Accountability principles of the CPLF. As pattern 28 – **Trust Evaluation of Services Slides** – could be applied to the IoT gateway, it is also applicable to the IoT cloud to ensure that the user trusts the service, and to verify that a service does not undermine their personal privacy requirements. Accordingly, the Transparency and Accountability principles of the CPLF are satisfied, as well as the Right to be Informed being achieved by applying this privacy pattern. Since the data could be access or handled by a third party (the IoT cloud in this scenario), the controller could share the data in ways that may not be approved by the participants. Therefore, applying privacy pattern 50 – **Obligation Management** – facilitates obligations around data sharing, storing and processing to be managed, and responsibilities can be altered if the data is shared among numerous parties. In this scenario, applying this pattern is helpful to ensure that the third party is aware of and complies with the policies required by the user or organisational policies. Accordingly, developers would adhere directly with the principles of the Data Minimisation, Storage Limitation, and Accountability. It also helps developers to grant participants the Right to be Informed. This is similar to the privacy pattern 60 – **Sticky Policy**.

(3) **Applying Privacy Patterns to the Mobile Application:**
The controller of the mobile application has to maintain privacy policies as they are an essential aspect that involves data subjects, users, and aspects of processing; furthermore, it is crucial to follow the laws that stipulate those policies. Privacy patterns **10, 11, 15, 20, 21, 30, 36, 37, 39, 45 and 59** all focus on solving privacy issues in regard to privacy policies. Since privacy policies

usually tend to be complex and long, these privacy patterns are concerned about balancing these policies with regard to accessibility, alongside being comprehensive from a legal perspective. Moreover, these patterns seek to present privacy policies in a clear way to ensure that users are clearly informed about the processing of their personal information. For example, Pattern 11 – **Layered Policy Design** – requires policies to be summarised in a nested way, so users are able to understand what they should expect from dealings with their personal data by a data controller with regard to the terms on which data is managed and to address specific purposes. Accordingly, applying these privacy patterns will help developers to directly adhere to the Transparency principle of the CPLF, as well as the Right to be Informed.

Regarding the personal data of the user, the mobile application should not collect any other information about the user that does not contribute to achieving the specified purpose. This applies to pattern 3 – **Minimal Information Asymmetry**. In this scenario, the objective is to find the car's location, so based on this pattern developers must not acquire any other types of data to include in the application. This will reduce the risk to the user's personal data and will help developers to not only comply with the Data Minimisation principle of the CPLF, but also adhere to the Transparency principle. Furthermore, applying this pattern will grant participants the Right to be Informed, as acquiring minimal information from users would reduce the issue of imbalance within the field of policy knowledge, including the knowledge held by the user regarding the controller and its practices.

As users of the mobile application may not be equipped to maintain strong passwords, remember them and protect them, privacy pattern 4 – **Informed Secure Passwords** – requires controllers to provide users with assistance in understanding and maintaining strong passwords that are easier to remember. This would result in complying with the Security principle of the CPLF directly, and the Accountability principle of the law indirectly. In a similar context, pattern 71 – **Unusual Activity** – asks controllers to alert users of unauthorised access in order to protect users. This would result in complying directly with the Security principle and would grant individuals the Right to be Informed. It also helps developers to comply with the Accountability principle indirectly.

Users are typically unaware of the risks to privacy from their data sharing activities, especially when those risks are either indirect or long term risks. Privacy pattern 5 – **Awareness Feed** – makes users more aware of these risks through requesting that the controller informs the user prior to starting the application processes about car collection locations. Users should be informed before processing personal data and should be given a warning about possible negative consequences at a time that is early enough to be taken note of, while late enough to still be relevant. In a similar fashion, pattern 19 – **Ambient Notice** –, requires the controller to present a succinct yet clear notification as the GPS sensor collects their car's locations, which does not interrupt the user's activity. Similarly, pattern 42 – **Appropriate Privacy Feedback** – requires the controller to provide clear feedback loops that gain the user's attention in order to make sure that the user understands whenever a new car's location is collected, and they can view that data and its possible uses. By applying these patterns, developers would comply directly with a principle and a right of the CPLF, Transparency, and the Right to be Informed respectively, as well as adhering to the Accountability principle indirectly. Like pattern 14 – **Asynchronous Notice** –, it asks the controller to provide a simple reminder that they have consented to the sensor to collect their car's location and users could configure the settings if they do not want to see this reminder again. Applying this pattern would help developers to comply with one right of the CPLF - the Right to be Informed. It also helps developers to adhere to the Accountability principle indirectly.

As demonstrated in Figure 6, the IoT gateway sends the car's location to the IoT cloud, which could be managed by a third party. Therefore, applying privacy pattern 18 – **Outsourcing [with consent]** – is essential before allowing the third party to process their data. Applying this pattern helps developers to comply with three principles of the CPLF directly: the Limiting Use and Disclosure principle, the Consent principle, and the Lawfulness of Processing principle. It also adheres to two principles of the CPLF indirectly: the Accountability principle, and the Purpose Limitation principle, where it should specify the purpose to limit the use and disclosure of the data collected for that purpose. Similarly, pattern 32 – **Sign an Agreement to Solve Lack on a Use of Private Data Context** – involves the controller providing the user with a contractual agreement so that they are more obligated to stick to their word. Like pattern 40 – **Obtaining Explicit Consent** – which requires controllers to obtain unambiguous consent from their users in order to collect and store their cars' locations, either by using contractual consent, or by signifying their consent, such as using a button, where users could click 'I consent.' Applying patterns 32 and 40 will result in complying directly with the Consent principle, and Lawfulness of Processing and the Accountability principle indirectly. Similarly, pattern 58 – **Lawful Consent** – addresses the legal and social obligations involved when the data subject provides consent for their data to be processed, under specific circumstances, in enough detail. This consent of the user should be purpose-separated so that users have to give consent for the collection of the car's location and consent for storing data for further analysis. This would result in complying directly with the Purpose Limitation, consent, and Lawfulness of Processing principles.

Regarding users' preferences, Pattern 53 – **Negotiation of Privacy Policy** – asks the controller to determine their users' privacy preference, and if the user's preference is unknown, they should use the highest level of privacy settings. In this scenario, the controller stores the car's location by default all the time unless he/she chooses 'No' or vice versa. Nevertheless, none of the principles and rights of the CPLF are suited to this privacy pattern. Pattern 35 – **Enable/Disable Function** – requires the controller to allow users to enable and disable any functions, such as disable the sensor which takes the car's location, or disable the function which stores the car's locations to process and analyse them for future suggestions. When developers apply this pattern, they would directly comply with the Consent and the Transparency principles of the CPLF, and this would help developers to grant individuals the Right to be Informed; they will also be adhering to the Accountability and the Lawfulness of processing principles indirectly. This avoids the need to trust service providers to collect personal data by storing the car's location in the mobile application instead of storing data in the IoT cloud. This applies privacy pattern 38 – **User Data Confinement Pattern** – which could be used if collecting personal data for a specific but legitimate purpose that holds a level of risk to the privacy of the user, accordingly, it complies with the Data Minimisation principle of CPLF directly. In a similar fashion, privacy pattern 27 – **Personal Data Store** – improves the amount of control the user has over their personal data by storing their data in a personal storage location (mobile) so the user can decide whether to share their data with a third party who could manage the IoT cloud. This, however, has not achieved any of the principles and rights of the CPLF. With regard to the processing of the collected car's location, pattern 61 – **Personal Data Table** – tracks the processing of the cars' locations to enable the user to view the activities related to their data for the purposes of suggesting parking locations in the future, and they can easily review their preferences. This would result in complying with the Transparency principle of the CPLF and granting users the Right of Individuals Access, and the Right of the Individual to Exercise their Rights.

Pattern 41– **Privacy Mirrors** – addresses the socio-technical domain by suggesting methods, mechanisms, and interfaces which can show the history, flow, state, and nature of the personal data processed which would have otherwise been hidden. In this scenario, the controller should provide the user with access to the data collected about the car's locations, as well as the processing operations concerning their data. This would help developers to comply with the law by granting individuals the Right to be Informed and the Right to Individuals Access. Pattern 48 – **Privacy Dashboard** – is wider as it does not only grant access to the user, but it also allows them to easily control their data themselves and related permissions; that is, by amending, erasing, or modifying the purposes they can be used for, or indeed, those whom the data is allowed to be shared with if this applies. By applying this pattern, developers would be complying with most of the rights of the CPLF: the Right of Individuals to Exercises their Rights, the Right to be Informed, Right to Individuals Access, the Right to Rectification, the Right to Erase, the Right to Restriction of Processing, the Right to Object, the Right to Object to Marketing, the Right to Object to Automated Decision-making, and the Right to Withdraw Consent. This would also help them to adhere indirectly to the Accountability principles.

7.3.2 ***Mapping Privacy Patterns to the Gym Monitoring System Use Case***. As this IoT solution collects personal information that could cause a risk to the user's privacy, the privacy patterns presented in the Technical Report [3] will be applied to the data flow to protect users' privacy and to comply with the privacy and data protection laws. To highlight the potential of this, the scenario presented in 7.2.2 will be revisited and the privacy patterns will be applied to developing a privacy-aware IoT application.

(1) **Applying Privacy Patterns to the Gym Activity Application:**
As demonstrated in Figure 8, when a participant starts the workout, the sensor starts collecting different types of data in real-time. The data collected are heart rate, speed, distance and accelerometer, which is used to derive the participant's activity, while the heart rate, distance, and speed could be used to derive the calories burned. Based on this scenario, developers can decide not to acquire any other data that is not used to achieve the objective of this application. This is achieved by privacy pattern 3 – **Minimal Information Asymmetry** – which not only seeks to minimise data, but also contributes to reducing the imbalance of policy knowledge, where users will be more aware of the controller's practices when controllers acquire less information about them. This would help developers to comply directly with the Data Minimisation and Transparency principles and granting participants the Right to be Informed. As the users of the Gym Activity application may not be equipped to maintain strong passwords, remember them and protect them, privacy pattern 4 – **Informed Secure Passwords** – requires controllers to assist users in understanding and maintaining strong passwords that they can easily recall. This would result in complying with the Security principle of the CPLF directly, and the Accountability principle indirectly. However, in the case of unauthorised access, it is crucial to alert the participant and trainer to protect their personal data. This applies pattern 71 – **Unusual Activity** – which would result in complying directly with the Security principle and granting users the Right to be Informed. It also helps developers to comply with the accountability principle indirectly.
Users are typically not aware of the privacy risks presented by data sharing activities, in particular, if they are indirect risks or long-term risks. Accordingly, developers have to inform the users of the Gym Activity application and the possible consequences in a timely manner prior to implementing the application and gathering their personal data, or if there is a risk of personal data being affected if it is not early enough to be appreciated or too late to be relevant. This reaches privacy pattern 5 – **Awareness Feed**. Like pattern 19 – **Ambient Notice** – which

requires the controller to make an unobtrusive but clearly visible notification available at the point when the sensors start collecting their data. Similarly, pattern 42 – **Appropriate Privacy Feedback** – requires the controller to provide feedback loops that are visible and made aware to the user. Accordingly, the user is aware whenever sensors start collecting data, how that data could be used (the trainer), and who is able to see the data (the trainer and the others who the data is shared with). When applying these patterns, the developer would directly adhere to the Transparency principle of the CPLF and grant participants the Right to be Informed. In addition, they would comply with the Accountability principle indirectly. In a similar fashion, pattern 14 – **Asynchronous Notice** – requests that the controller provides a clear basic reminder that they have given consent to the sensors to collect their data, and that users can configure the settings in the event that they do not want the reminder to appear again. This would result in complying directly with part of the CPLF by granting participants the Right to be Informed. It would also help developers in complying with the Accountability principle indirectly.

As participants can share their progress with other participants, it is essential to protect the user's information by informing the participants that their access is not being made private, and to tell them about other users, including possible unauthenticated ones, who can also access the content. This achieves privacy pattern 9 – **Who's Listening** – which helps developers to comply with part of the CPLF as they directly grant participants the Right to be Informed. In a similar fashion, pattern 57 – **Privacy Awareness Panel** – provides the user with reminders on who can see the content they have or will disclose, what is done with it, why, and how it might become identifiable. This would help developers to comply with the Transparency principle of the CPLF and granting participants the Right to be Informed. Similarly, pattern 61 – **Personal Data Table** – maintains the tracking of the processing of personal data to enable users to view the activities and preferences concerning their data and review the preferences they have made in a tabular format. Accordingly, developers would be complying with the Transparency principle of the CPLF and granting participants the Right of Individuals Access, and the Right of the Individual to Exercise their Rights. According to pattern 28 – **Trust Evaluation of Services Slides** –, it is important for the participants to trust the service that is provided by the gym and make sure that the service does not negatively affect their personal privacy requirements. This would result in complying directly with the Transparency and Accountability principles of the CPLF and granting users the Right to be Informed.

As demonstrated in Figure 8, the Gym Activity application sends the personal data to be stored in the local server, and the local server pushes the data to the IoT cloud for further analysis, which could be managed by a third party. Thus, applying privacy pattern 18 – **Outsourcing [with consent]** – is crucial before allowing the third party to process their data. This would result in complying directly with the Limiting Use and Disclosure, Consent, and Lawfulness of Processing principles. It also helps developers to adhere indirectly with the Accountability principle, and the Purpose Limitation principle, where the purpose should be specified to limit the use and disclosure of the data collected for that purpose. Like pattern 32 – **Sign an Agreement to Solve Lack on a Use of Private Data Context** – which means that the controller must provide the user with a contractual agreement, as that will cause the controller to be more dedicated to keeping their word. In a similar fashion, pattern 40 – **Obtaining Explicit Consent** – requires the controller to obtain unambiguous consent from the user in order to collect, store, and analyse their personal data, either by using Contractual Consent or by signifying their consent. For example, a check box that allows participants to provide their consent through checking the box. Applying patterns 32 and 40 would result in complying directly with the Consent, and Lawfulness of Processing principle, and indirectly with the Accountability principle. This is similar to pattern 58 – **Lawful Consent** – which covers in detail the legal and social obligations

surrounding a data subject's consent to processing of their data in specific circumstances. This consent of the participants should be purposed-separated, so the controller should obtain consent for the collection of data when a participant starts a workout and should obtain consent for storing data in the IoT cloud, and so on. Therefore, developers will be adhering directly to the Purpose Limitation, Consent, and Lawfulness of Processing principles.

The controller of the Gym Activity application has to maintain privacy policies as they are an essential part of the processing required for its activities. Furthermore, they do not just rely on the users, which is an important part of the processing, but also implement the laws that mandate these policies. Privacy patterns **10, 11, 15, 20, 21, 30, 36, 37, 39, 45 and 59** all concentrate on solving the privacy issues addressed in privacy policies. This is because privacy policies typically tend to be complicated and very long. In addition, the privacy patterns involved address balancing the accessibility set out in these policies alongside adhering to the legal comprehensiveness required. Moreover, these patterns attempt to clearly set out privacy policies so that users remain properly informed of the way their personal data is being processed. For example, pattern 20 – **Dynamic Privacy Policy** – requires a controller to present the user with extra policy information that is relevant to them as and when needed, according to the context. This would result in complying with the Transparency principle of the law and granting users the Right to be Informed.

In a case where participants share their photograph with other participants, it is safer to remove all of the metadata (ex., location of the photo) not directly visible during upload time or while the service is being used. This will protect personal information from leaks, and prevent the controllers from surprising users, which could alienate them, if the information does not have legal protection. This applies pattern 25 – **Strip Invisible Metadata** – which helps developers to directly comply with the Data minimisation and the Limiting Use and Disclosure principles of the CPLF. It also adheres to the Purpose Limitation and the Accountability principles indirectly. As the participants can share their workout and pictures with other participants, the controller has to use privacy warnings that are contextual to present relevant information and provide suggestions about pending disclosures. This applies privacy patterns 43 – **Impactful Information and Feedback** – which would help developers to comply with part of the CPLF by granting the participants the Right to be Informed.

As the Gym Activity application requires the participants to register their names, the application should allow the participants to identify themselves by using a pseudonym. Pattern 26 – **Pseudonymous Identity** – ensures a pseudonymous identity not to be linked with a real identity. This would result in complying directly with the Anonymity and Pseudonymity principle of the CPLF and complying indirectly with the Security and the Accountability principles. With regard to users' preferences, pattern 53 – **Negotiation of Privacy Policy** – requires the controller to specify their participants' privacy preferences; also, if the user's preference is unclear or unknown, it must assume the highest privacy-preserving setting levels. The controller in this scenario, could enable data collection once a participant starts a workout by default, unless the participant disables the data collection. However, none of the principles and rights of the CPLF are suited to this privacy pattern. Applying pattern 35 – **Enable/Disable Function** – allows participants to enable and disable any service provided by the application, such as disabling the heart rate monitor sensor or disabling the service that enables them to share their workouts with other participants. When developers apply this pattern, they would be directly complying with the Consent and the Transparency principles, and the Right to be Informed. They would also be adhering to the Accountability and the Lawfulness of Processing principles indirectly.

Privacy pattern 46 – **Selective Access control** – allows a participant to specify the participants who can access their content based on a specified rule, such as a rule that is based on participants, or a rule based on context-aiding attributes like age. This would result in complying directly with the Security principle of the CPLF. Allowing participants the option to clarify the privacy level for the content shared with the controller or other users means that they can decide on the level of access given to other participants. This applies pattern 12 – **Discouraging Blanket Strategies**; however, none of the principles and rights of the CPLF is achieved by this pattern. Applying pattern 54 – **Reasonable Level of Control** – enables participants to access information, a service, or other participants, in a selective manner, and make information available to predetermined groups or groups denied by the user. Like pattern 56 – **Buddy List** – which facilitates users finding and assigning others to a directory that is user maintained and contains social circles and contexts for interacting with. Therefore, applying pattern 50 – **Preventing Mistakes or Reducing their Impact** – prevents unintended disclosure of personal information to other participants. It requires the controller to put contextual measures in place in order to predict whether content needs to be processed, or if consent should be re-established, to stop unintentional disclosure and mistakes. This would result in directly adhering to the Limiting Use and Disclosure principle of the CPLF and would grant participants the Right to be Informed. Pattern 41– **Privacy Mirrors** – requires the controller to provide the user with access to the personal data processed, including the history, flow, state and nature of that data. This, in turn, would help developers to grant participants the Right to be Informed and the Right to Individuals Access. Pattern 48 – **Privacy Dashboard** – is wider as it does not only grant access to the user, but it also allows them to easily control their data and the various permissions, such as amending, erasing or modifying the purposes that they can be used for, or the parties it is allowed to share them with, if applicable. Accordingly, developers would be complying with most of the rights of the CPLF: the Right of Individuals to Exercises their Rights, the Right to be Informed, the Right to Individuals Access, the Right to Rectification, the Right to Erase, the Right to Restriction of Processing, the Right to Object, the Right to Object to Marketing, the Right to Object to Automated Decision-making, and the Right to Withdraw consent. It would also help them to adhere indirectly to the Accountability principles.

(2) **Applying Privacy Patterns to the Local Server and the IoT Cloud:**
As each workout information is stored in the local server once a participant completes the workout, it is essential to ensure that personal information is kept confidential by applying privacy pattern 6 – **Encryption with a User-managed Key** to the local server and to the IoT cloud. Developers could also apply pattern 24 – **Onion Routing** – to protect personal data while it is routed between different nodes. Furthermore, while the completed workout for each month is sent to the IoT cloud for analysis purposes, it is good practice to increase the security of the personal information before sending it to the cloud, as this could be prevent any exploitation of personal data. Accordingly, applying these privacy patterns would help developers to directly comply with the security principle of the CPLF and the Accountability principle indirectly. Furthermore, applying privacy pattern 8 – **Use of Dummies** – would help developers to secure personal information by adding fake workouts to the real workout in an approach that prevents the adversary from distinguishing real from fake information. This, in turn, would help developers to adhere to the Security and Anonymity and Pseudonymity principles of the CPLF.
According to pattern 28 – **Trust Evaluation of Services Slides** –, it is important for participants to trust the service that is provided by the gym and make sure that a service will not undermine personal privacy requirements. This pattern is not only limited to the local

server and IoT cloud, but is also applicable to the smart watch. This would result in complying directly with the Transparency and the Accountability principles of the CPLF, as well as granting participants the Right to be Informed. Regarding the services that could be managed by a third party such as the IoT cloud in this scenario, it is important to apply privacy pattern 29 – **Aggregation Gateway** – which implements homomorphic encryption by using a secret answer that is shared with the third party aiming to improve the system. The third-party will not know what the content is because it is encrypted, and so it operates on the data in an encrypted format. This encryption prevents any revealing of the user's health and fitness information. Accordingly, the service provider would comply with the security principle of the law directly. Introducing privacy pattern 63 – **Added-noise Measurement Obfuscation** – ensures that any information that may reveal sensitive user information cannot be accessed. By storing fake workouts, for example, its difficult to infer any other personal information from the aggregation of the user's information. This would help developers to comply with the principle of Limiting Use and Disclosure of the CPLF directly. To prevent any consequences resulting from a data breach, it is crucial to apply privacy pattern 22 – **Data Breach Notification Pattern** – to the local server and to the IoT cloud in order to detect and react to a data breach quickly and to prevent any malicious activity using personal information. Accordingly, developers would be complying with the Security and the Accountability principles of the CPLF.
Since the data could be accessed or handled by a third party (the IoT cloud in this scenario) where the controller shares the data in ways that may not be approved by the participant, applying privacy pattern 50 – **Obligation Management** – ensures that the third party knows about and complies with the necessary user or organisational policies. Accordingly, developers would be adhering directly with the principle of the Data Minimisation, Storage Limitation, and Accountability. It also helps developers to grant participants the Right to be informed. It is similar to the privacy pattern 60 – **Sticky Policy**.

7.3.3 ***Applicability of Applying Rights of the Privacy and Data Protection Laws.*** As shown above, in sections 7.3.1 and 7.3.2, privacy patterns have been mapped to two different IoT scenarios. When developers apply a specific pattern, it automatically complies with what is applicable from the principles or rights of the privacy and data protection laws, as demonstrated in the Technical Report [3]. The mapping process, as demonstrated in Figures 6 and 8, differs based on the scenarios of the use cases, where we have different components (e.g., IoT gateway, IoT Cloud, Smartphone etc.) and characteristics. Accordingly, we acknowledge that the rights of privacy and data protection laws are not absolute and can only be applied in certain circumstances. Take the Right to Data Portability as an example, where individuals have the right to receive their personal data in a readily useable format that allows the individual to transmit the information to another organisation. Applying this right is not possible in both scenarios as the specifications of the above use cases do not include the transition of the data to that organisation. However, the Right of Individuals Access is applicable in both scenarios where we have an application (Smartphone in scenario 1 and Smartwatch in Scenario 2) for each user to access their personal data. This could be applied through the following privacy patterns: Privacy Mirror, Privacy Dashboard, and Personal Data Table as demonstrated in the Technical Report [3]. Therefore, we cannot enforce all the rights to be supported in any IoT scenarios, as it depends on the specifications of the use cases given and on the IoT components.

8 RESEARCH CHALLENGES AND OPPORTUNITIES

In this section, the objective is to identify some of the major challenges that should be addressed, and potential research directions in order to support software developers building privacy-aware IoT applications. These challenges have not been addressed yet in academia and they are as follows:

prioritising the privacy patterns, creating new privacy patterns, enriching developers' tools to support privacy, and building privacy by design tools.

8.1 Prioritizing the Privacy Patterns

Various privacy patterns have been mapped to different principles and rights of the CPLF in order to facilitate developers complying with privacy and data protection laws (outcome of the detailed mapping is presented in the Technical Report [3]). Privacy patterns provide an important reference point for developers [51, 52]. However, they are often introduced during a fairly late stage of the design after key choices and decisions have been made; even so, they assist with documenting common practices and standardising terminology. From a practical perspective, however, there are still problems around developers having the competence needed to choose patterns and implement the ones most relevant to the artifacts being designed. Accordingly, making the right decision and trade-offs regarding the choice of a privacy pattern, from among all the available patterns without compromising the core functionality of a system, would stand as a barrier to software developers.

Figure 9 demonstrates the prioritisation of the privacy patterns based on the number of key principles and/or individual's rights of the CPLF achieved. We cannot claim that a particular pattern is more important than another just because it achieves many numbers of principles and/or rights. To illustrate, privacy pattern 17 – **Privacy Dashboard** – achieves eleven of the principles and rights (1 principle, 10 rights) of the CPLF. However, it mainly focuses on the individual's access and it does not consider other important principles, such as Data Minimisation, despite all the privacy and data protection laws in this study asserting the importance of achieving this principle. Therefore, prioritising the privacy patterns based on the number of achieved principles and/or rights of the CPLF is not useful.

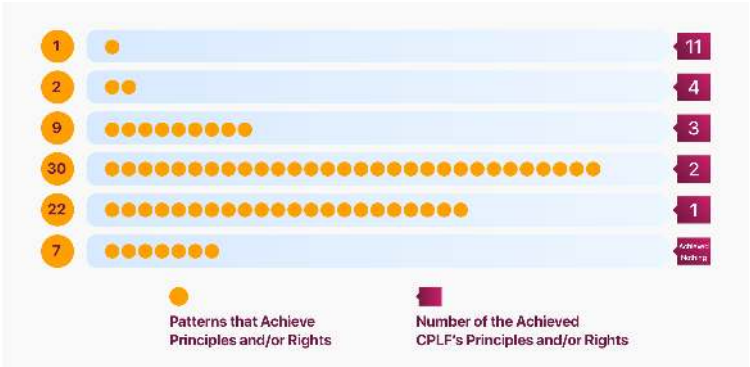

Fig. 9. Prioritisation of the privacy patterns

Figures 10 and 11 show another way of prioritisation of privacy patterns. It ranks the CPLF's principles and rights based on the agreement of the issuers of the privacy and data protection laws of the five selected countries on a specific principle/right according to the criteria mentioned below. That means that if a privacy or data protection law agrees with the concept of a specific principle/right, this principle/right will attain a score of two for that issuer. And, when the issuer's view is not explicitly stated but agrees with the concept of this principle/right, this principle/right will get a score of one for that issuer, or otherwise nothing. Nonetheless, there is a need for scientific evidence for the prioritisation process.

Even though Jason Hong's team of PrivacyGrade.org has graded one million Android Apps based on their usage of sensitive information [24], no previous study has investigated the prioritisation

✓	If the issuer's view agrees with the concept of this key principle/right
☑	If the issuer's view is not explicitly stated but agrees with the concept of this key principle/right being inferred from such a provision
N/M	If a regulation contains an explicitly stated provision for a different context from this key principle/right
N/A	If no provision can be assigned as the issuer's view and there is no contradiction with this principle/ right

Fig. 10. Prioritisation of the privacy patterns based on the ranking of the CPLF's principles

of privacy patterns to help developers make the right decision and trade-off regarding the choice of privacy-preserving ideas. Therefore, developers can balance between the privacy-preserving techniques and the core functionality of the system.

8.2 Creating New Privacy Patterns

According to the Technical Report [3], synthesising various Privacy by Design (PbD) schemes into a single knowledge base, captures the relationship between the principles, strategies, and guidelines of the PbD schemes after they have been largely disconnected from each other. This knowledge base supports software developers in discovering the privacy protection mechanisms required to solve the problem at hand swiftly and efficiently. It also shows how some of the schemes were extended based on other schemes, and how some of the schemes' phrases are connecting with each other. However, correlating the principles, strategies, and guidelines of the PbD schemes with the principles and rights of the CPLF reveals that there is a need to improve the existing principles, strategies, and guidelines or to propose new PbD schemes in order to mitigate the gap with regard to the rules of the various privacy and data protection laws (outcome of the detailed mapping is presented in the Technical Report [3]).

Nevertheless, as stated previously, privacy patterns are more solid and more appropriate for explaining data usage in a specific context, and are more effective than the principles, guidelines or strategies of the PbD scheme. According to the technical Report [3], mapping between the privacy

Fig. 11. Prioritisation of the privacy patterns based on the ranking of the CPLF's rights

patterns and the principles and rights of the CPLF indicates that various principles and rights of the CPLF have not been achieved by any of the existing privacy patterns. These are the principles: **Source**, **Cross-border Disclosure of Personal Information**, **Dealing with Unsolicited Data**, and **Adoption, Use, and Disclosure of an Identifier**; and these are the rights: **Right to Data Portability**, **Right to Complain**, and the **Right of Individuals not to be Discriminated**. Furthermore, the problem is not only limited to the applicability of a particular privacy pattern to achieve a certain law, but the applicability of implementing the same pattern in different ecosystems as there are few operating-system-specific details. Let us take – **Location Granularity** – as an example of a pattern. Implementing this pattern in Arduino is different from implementing the same pattern in Raspberry Pi, which has a different operating system. Privacy patterns, however, can still be identified as low-level designs that help software developers to build a privacy-aware system. Therefore, harnessing the effort not only to create new general privacy patterns that cover all the rules of the privacy and data protection laws, but also to create IoT specific privacy patterns while taking into consideration various ecosystems, would help IoT developers to comply with privacy and data protection laws and to build privacy-aware IoT applications.

8.3 Enriching Developers' Tools to Support Privacy

In order to build a privacy-aware IoT application that complies with the rules of privacy and data protection laws, software developers need to deal effectively with the legal aspects of it, understand its provisions, and translate these legal requirements into technical requirements that are applicable to the technical domain. However, as stated previously, studies have shown that developers from a range of backgrounds often lack the skills necessary to ensure effective privacy management [8, 63], and the difficulties that exist in regard to compliance with regulations are predicted to increase in the future [7]. While some guidelines are available, most concentrate on the legal aspects, rather than technical requirements, which results in them being unsuitable for the tools used to build applications, and this disconnects them from the practical environment that developers are working in. Thus, developers face the problem of relating the guidance provided to actual technical considerations, such as ensuring a specific design, or making sure its implementation properly meets privacy requirements.

As shown earlier in this paper, in order to help developers across different regions exceed these obstacles, different privacy and data protection laws of various countries have been analysed. This analytical method shows how dealing with legal aspects is a very complicated process, as there are vague provisions that need to be understood and various key principles and individual rights that should be taken into consideration. Investigating the previous efforts on guiding software designers and developers to protect personal information, several researchers have proposed various principles, guidelines, strategies and patterns of the PbD schemes as demonstrated in the Technical Report [3]. Nevertheless, after correlating these privacy schemes with the key principles and rights, it has been demonstrated that not only are many of these principles, strategies, and guidelines disconnected from the technical domain, but they are not adhering to the rules of the CPLF. A further issue is demonstrated when applying privacy patterns to different use cases, as patterns are more appropriate than principles, strategies, and guidelines. This reveals how it is difficult for software developers to choose the right position of a pattern where the IoT scenario is complicated, and where the data moves between many nodes that have different computational capabilities. It is, moreover, difficult for developers to make the right decision and trade-off regarding the choice of a privacy pattern from among all the available patterns without compromising the core functionality of the system. The problem is not only limited to these challenges but, moreover, there is a lack of practical guidance that considers the technical domain for developers to build a privacy-aware IoT application [29].

Enriching existing developers' tools to support privacy-preserving techniques will ensure that developers are more aware of the use of personal data and how it can potentially be exploited, throughout the process of application building. In addition, this shift in emphasis will lead developers to consider the implications of their applications, and the possibility of using alternatives that pose less risk when personal data is involved. Precisely, through introducing notions of privacy into the development environment, the environment itself could provide guidance that specifically addresses the artifacts being built, and this may enable software developers to better adhere to the provisions required by law. This will not only place the burden on software developers, but will also save developers time and effort.

8.4 Building Privacy By Design Tools

According to Roeser (2012), "Engineers can influence the possible risks and benefits more directly than anybody else" [55]. Even so, software engineers typically face a number of issues concerning privacy management. For example, they may pass the responsibility over to experts; however, this is based on the assumption that software engineers have access to such experts, even though this is unlikely for small businesses or individual designers. In addition, privacy experts need to have the technical competence to understand the impact of development decisions on privacy [30]. While guidelines exist, they are usually geared towards a legal rather than technical domain, and are generally disconnected from the tools and environments used by developers to design their applications. Moreover, privacy guidelines are usually drawn on during the latter stages of the design phase, even though their application would be easier and more effective if they were applied earlier. In addition, software engineers face the challenge of relating guidance to technical aspects, but this guidance may not align with some design choices or implementation details.

In contrast, as shown previously in Section 3, analysing the privacy and data protection laws of various countries is a very complicated process, as there may be vague provisions that are difficult to understand, and key principles and individual rights that must be considered. Research has shown that previous efforts to guide software designers to ensure the protection of personal information, has led to a number of principles, guidelines, strategies and patterns of Privacy by Design (PbD) schemes being proposed. The mapping between these privacy schemes and the key principles and

rights as shown in the Technical Report [3] is time consuming where software designers have to do so manually. Even so, once these privacy schemes have been correlated with the key principles and rights, it has been shown that many principles, strategies, and guidelines are disconnected from the technical domain; furthermore, they often do not adhere to the rules of the CPLF. Another issue involves applying privacy patterns to different use cases, where patterns are more concrete than principles, strategies or guidelines. Therefore, it is difficult for software developers to choose the position of a pattern if the IoT scenario is complicated, and if the data moves between several nodes with different computational capabilities and constraints on resources. It is, moreover, difficult for developers to make the right decision and trade-off regarding the choice of a privacy pattern from among all the available patterns without compromising the core functionality of a system. The problem is wider than these challenges, yet there is a lack of practical guidance for designers in the technical domain to support the design phase of building IoT applications.

Placing a greater focus on the development of privacy tools as a central aspect of the design process, and not simply as an additional factor, will ensure that software engineers pay more consideration to personal data, and its potential to be exploited throughout the process of application design. In addition, this shift in focus should encourage software engineers to consider the implications of specific IoT application designs, including whether to use alternatives that pose less risk to personal data. Furthermore, privacy by design tools will not only remove the burden from software designers, but will also save time and effort, which will make this process of designing a privacy-aware IoT application faster, more reliable and consistent.

8.5 Using Gamification Techniques

In order to engage and motivate software designers and developers building a privacy-aware IoT application, the technique of play gamification has recently emerged. This is the use of game mechanics and related elements within various contexts [53]. Using gamification [4, 61] in the design and development stage is a useful and innovative way of increasing productivity and motivation, and companies that have used this approach have seen increased productivity and greater involvement [20, 61] of software designers and developers in applying privacy patterns. This is because gamification enables people to learn new material, as well as gaining practical knowledge through engaging in certain activities. Moreover, a large number of studies have shown the positive impact of gamification on training outcomes [46].

The components typically used in gamification are points, as these are convenient for realisation and players can understand them. In this system, for each action performed, the user gains a point [5]. Therefore, in order to guide software designers and developers, it is essential to have a marking scheme to base the points on when using gamification techniques. Prioritisation of the privacy patterns is one of the approaches that we could base the points on. As shown in the previous section, the privacy patterns were prioritised based on the ranking of each achieved principle/right of all the CPLF. So, once a software designer or a developer chooses a specific pattern, he/she will gain a score based on the prioritisation's ranking of that pattern, as seen in Figure 10 and 11. Nevertheless, as stated previously, there is a need for an in-depth understanding and scientific evidence of how prioritisation should be carried out to ensure privacy.

9 CONCLUSION

Developers of IoT applications, like any other developers, face difficulties when adhering to privacy and data protection laws and the associated Privacy by Design (PbD) techniques. However, developers from a range of backgrounds have a tendency not to be fully skilled in privacy management, and problems around adhering to regulations are predicted to increase even more in the future. It is, therefore, essential for developers to make an effort to meet privacy and data protection

requirements and to comply with the law. In this investigation, the aim was to assist developers in understanding legal requirements, to map these legal requirements to various PbD schemes in order to build better privacy-aware IoT applications, and to comply with privacy and data protection laws. Various privacy and data protection laws have been analysed, which are the General Data Protection Regulations (GDPR), the Personal Information Protection and Electronic Documents Act (PIPEDA), California Consumer Privacy Act (CCPA), Australian Privacy Principles (APPs), and New Zealand's Privacy Act 1993. Then, existing PbD techniques were reviewed and correlated to the principles, strategies, and guidelines, along with the key principles and individuals' rights in the CPLF. In addition, the privacy patterns were mapped – as they are more concrete - with the privacy and data protection laws and it was demonstrated how to apply the privacy patterns to the right position of a given IoT architecture. Applying the privacy patterns to IoT architectures helps developers to highlight the privacy challenges, which, in turn, would help them comply with the law as they have been correlated. This study concludes that the major challenges that have to be resolved to achieve effective privacy protection in IoT applications are: prioritising the privacy patterns, creating new privacy patterns for IoT and operating system specific domains, enriching developers' tools to support privacy, and building privacy by design tools.

REFERENCES

[1] 2016. EUR-Lex - 32016R0679 - EN - EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC

[2] Yasemin Acar, Sascha Fahl, and Michelle L. Mazurek. 2016. You are Not Your Developer, Either: A Research Agenda for Usable Security and Privacy Research Beyond End Users. *Proceedings - 2016 IEEE Cybersecurity Development, SecDev 2016* (2016), 3–8.

[3] Atheer Aljeraisy, Masoud Barati, Omer Reana, and Charith Perera. 2020. *Exploring the Relationships Between Privacy by Design Schemes And Privacy Laws: A Comparative Analysis.* Technical Report June. Cardiff University. 40 pages. http://orca.cf.ac.uk/132613/

[4] Satoshi Arai, Kazunori Sakamoto, Hironori Washizaki, and Yoshiaki Fukazawa. 2014. A gamified tool for motivating developers to remove warnings of bug pattern tools. *Proceedings - 2014 6th International Workshop on Empirical Software Engineering in Practice, IWESEP 2014* (2014), 37–42.

[5] Darius Ašeriškis and Robertas Damaševičius. 2014. Gamification patterns for gamification applications. *Procedia Computer Science* 39, C (2014), 83–90.

[6] Vanessa Ayala-Rivera and Liliana Pasquale. 2018. The grace period has ended: An approach to operationalize GDPR requirements. *Proceedings - 2018 IEEE 26th International Requirements Engineering Conference, RE 2018* (2018), 136–146.

[7] Rebecca Balebako and Lorrie Cranor. 2014. Improving app privacy: Nudging app developers to protect user privacy. *IEEE Security and Privacy* 12, 4 (2014), 55–58.

[8] Rebecca Balebako, Abigail Marsh, Jialiu Lin, Jason Hong, and Lorrie Faith Cranor. 2014. The Privacy and Security Behaviors of Smartphone App Developers. *In Proceedings 2014 Workshop on Usable Security* (2014).

[9] Len Bass, Paul Clements, and Rick Kazman. 2003. *Software Architecture in Practice Addison-Wesley.* Vol. 3. Addison Wesley. 662 pages.

[10] Frank Buschmann, Regine Meunier, Hans Rohnert, Peter Sommerlad, and Michael Stal. 1996. *Pattern-Oriented Software Architecture, A System of Patterns.* Vol. 1.

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

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

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

[14] B. Costa, P. F. Pires, F. C. Delicato, W. Li, and A. Y. Zomaya. 2016. Design and Analysis of IoT Applications: A Model-Driven Approach. In *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech).* 392–399.

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

[16] European Commission. 2013. *Cybersecurity Strategy of the European Union.* Technical Report. arXiv:arXiv:1011.1669v3 http://www.eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

[17] FL. 2009. *ARTICLE 29 Data Protection Working Party Working Party on Police and Justice The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data.* Technical Report.
[18] Communication From, The Commission, TO The, The Council, The European Economic, The Committee, and O F The. 2014. Towards a thriving data-driven economy. *European Commission* COM(2014), 442 (2014).
[19] Christine Furber. 2010. Framework analysis: a method for analysing qualitative data. *African Journal of Midwifery and Women's Health* 4, 2 (2010), 97–100.
[20] Gloria Piedad Gasca-Hurtado, María Clara Gómez-Alvarez, Mirna Muñoz, and Jezreel Mejía. 2016. Gamification proposal for defect tracking in software development process. In *Gamification proposal for defect tracking in software development process (Communications in Computer and Information Science)*. 212–224.
[21] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems* 29, 7 (2013), 1645–1660. arXiv:1207.0203
[22] Irit Hadar, Tomer Hasson, Oshrat Ayalon, Eran Toch, Michael Birnhack, Sofia Sherman, and Arod Balissa. 2018. Privacy by designers: software developers' privacy mindset. *Empirical Software Engineering* 23, 1 (2018), 259–289.
[23] Jaap-henk Hoepman. 2014. IFIP AICT 428 - Privacy Design Strategies. (2014), 446–459.
[24] Jason Hong. 2017. The Privacy Landscape of Pervasive Computing. *IEEE Pervasive Computing* 16, 3 (2017), 40–48.
[25] Israel Jerusalem. 2010. Resolution on Privacy by Design. In *In Proceedings of the 32nd International Conference of Data Protection and Privacy Commissioners.*
[26] Jean-Denis Kusion. 2018. Minutes - ETHI (42-1) - No. 91 - House of Commons of Canada. https://www.ourcommons.ca/DocumentViewer/en/42-1/ETHI/meeting-91/minutes
[27] Marc Langheinrich. 2001. Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems. In *Ubicomp 2001: Ubiquitous Computing*, Gregory D. Abowd, Barry Brumitt, and Steven Shafer (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 273–291.
[28] California State Legislature. 2018. Bill Text - AB-375 Privacy: personal information: businesses. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
[29] Tianshi Li and Jason I Hong. 2018. Coconut: An IDE Plugin for Developing Privacy-Friendly Apps. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 4 (2018).
[30] Tom Lodge and Andy Crabtree. 2019. Privacy Engineering for Domestic IoT : Enabling Due Diligence. (2019).
[31] Kai Uwe Loser and Martin Degeling. 2014. Security and Privacy as Hygiene Factors of Developer Behavior in Small and Agile Teams. *IFIP Advances in Information and Communication Technology* 431 (2014), 255–265.
[32] NewZealandGovernment. 2020. Privacy by Design (PbD) | NZ Digital government. https://www.digital.govt.nz/standards-and-guidance/privacy-security-and-risk/privacy/manage-a-privacy-programme/privacy-by-design-pbd/
[33] NPC. 2018. The National People's Congress of the People's Republic of China. http://www.npc.gov.cn/englishnpc/index.shtml
[34] Office of the Australian Information Commissioner. 2013. Australian Privacy Principles — OAIC. https://www.oaic.gov.au/privacy/australian-privacy-principles/
[35] Office of the Australian Information Commissioner. 2014. Australian Privacy Principles quick reference — OAIC. https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-quick-reference/
[36] Office of the Australian Information Commissioner. 2014. Rights and responsibilities — OAIC. https://www.oaic.gov.au/privacy/the-privacy-act/rights-and-responsibilities/
[37] Office of the Australian Information Commissioner. 2019. Chapter B: Key concepts — OAIC. https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/
[38] Office of the Privacy Commissioner of Canada. 2013. Introduction. https://www.privacy.org.nz/the-privacy-act-and-codes/privacy-act-and-codes-introduction/
[39] Office of the Privacy Commissioner of Canada. 2013. Office of the Privacy Commissioner | Your Right To Know - an OPC advice sheet. https://www.privacy.org.nz/news-and-publications/guidance-resources/your-right-to-know-an-opc-advice-sheet/
[40] Office of the Privacy Commissioner of Canada. 2016. Businesses and your personal information. https://www.priv.gc.ca/en/privacy-topics/information-and-advice-for-individuals/your-privacy-rights/businesses-and-your-personal-information/
[41] Office of the Privacy Commissioner of Canada. 2016. How the OPC protects and promotes privacy. https://www.priv.gc.ca/en/about-the-opc/what-we-do/mm/
[42] Office of the Privacy Commissioner of Canada. 2016. Office of the Privacy Commissioner |Commissioner of the privacy principles. https://www.privacy.org.nz/news-and-publications/guidance-resources/a-quick-tour-of-the-privacy-principles/

[43] Office of the Privacy Commissioner of Canada. 2018. Summary of privacy laws in Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/

[44] Office of the Privacy Commissioner of Canada. 2019. PIPEDA fair information principles. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

[45] Office of the Privacy Commissioner of Canada. 2019. PIPEDA legislation and related regulations. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/

[46] Erick B. Passos, Danilo B. Medeiros, Pedro A.S. Neto, and Esteban W.G. Clua. 2011. Turning real-world software development into a game. *Brazilian Symposium on Games and Digital Entertainment, SBGAMES* (2011), 260–269.

[47] Charith Perera, Mahmoud Barhamgi, Arosha K. Bandara, Muhammad Ajmal, Blaine Price, and Bashar Nuseibeh. 2019. Designing Privacy-aware Internet of Things Applications. (2019). arXiv:1703.03892 http://arxiv.org/abs/1703.03892

[48] Charith Perera, Chi Harold Liu, and Srimal Jayawardena. 2015. The Emerging Internet of Things Marketplace from an Industrial Perspective: A Survey. *IEEE Transactions on Emerging Topics in Computing* 3, 4 (2015), 585–598. arXiv:1502.00134

[49] Charith Perera, Arkady Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. 2014. Context aware computing for the internet of things: A survey. *IEEE Communications Surveys and Tutorials* 16, 1 (2014), 414–454. arXiv:1305.0982

[50] POPI. 2013. Protection of Personal Information Act 2013. , 75 pages. https://popia.co.za

[51] privacypatterns.org. [n.d.]. Collecting patterns for better privacy. http://privacypatterns.wu.ac.at:8080/catalog/

[52] privacypatterns.org. [n.d.]. Privacy Patterns. https://privacypatterns.org/patterns/

[53] Claudia Ribeiro, Carla Farinha, João Pereira, and Miguel Mira da Silva. 2014. Gamifying requirement elicitation: Practical implications and outcomes in improving stakeholders collaboration. *Entertainment Computing* 5, 4 (2014), 335–345.

[54] Rob van der Meulen and Gartner. 2017. Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015. https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

[55] Sabine Roeser. 2012. Emotional Engineers: Toward Morally Responsible Design. *Science and Engineering Ethics* 18, 1 (2012), 103–115.

[56] Rodrigo Roman, Jianying Zhou, and Javier Lopez. 2013. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks* 57, 10 (2013), 2266–2279.

[57] Martin Rost and Kirsten Bock. 2011. Privacy by Design and the New Protection Goals. *DuD, January* November 2009 (2011), 1–9. https://www.european-privacy-seal.eu/AppFile/GetFile/ca6cdc46-d4dd-477d-9172-48ed5f54a99c

[58] Sebastian Schulz. 2014. Privacy by Design. *Computer und Recht* 28, 3 (2014). https://www.oaic.gov.au/privacy/privacy-for-organisations/privacy-by-design/

[59] Laurens Sion, Kim Wuyts, Koen Yskout, Dimitri Van Landuyt, and Wouter Joosen. 2018. Interaction-Based Privacy Threat Elicitation. *Proceedings - 3rd IEEE European Symposium on Security and Privacy Workshops, EURO S and PW 2018* (2018), 79–86.

[60] Aashish Srivastava and S Bruce Thomson. 2009. Framework analysis: a qualitative methodology for applied policy research. (2009).

[61] Jakub Swacha. 2016. Gamification in Enterprise Information Systems: What, why and how. *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems, FedCSIS 2016* 8 (2016), 1229–1233.

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

[63] Yung Shin Van Der Sype and Walid Maalej. 2014. On lawful disclosure of personal user data: What should app developers do? *IEEE 7th International Workshop on Requirements Engineering and Law, RELAW 2014 - Proceedings* (2014), 25–34.

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

[65] Wei Xiong, Hanping Hu, Naixue Xiong, Laurence T. Yang, Wen Chih Peng, Xiaofei Wang, and Yanzhen Qu. 2014. Anomaly secure detection methods by analyzing dynamic characteristics of the network traffic in cloud communications. *Information Sciences* 258, 60773192 (2014), 403–415.

[66] zebra.com. 2012. *Implementation of the "Carfinder" project.* Technical Report. www.zebra.com

[67] Qingchen Zhang, Laurence T. Yang, Zhikui Chen, Peng Li, and M. Jamal Deen. 2018. Privacy-preserving double-projection deep computation model with crowdsourcing on cloud for big data feature learning. *IEEE Internet of Things Journal* 5, 4 (2018), 2896–2903.

[68] Shichao Zhang, Chengqi Zhang, and Qiang Yang. 2003. *Data preparation for data mining.* Vol. 17. 375–381 pages.