Adopt a PET! An Exploration of PETs, Policy, and Practicalities for Industry in Canada

Masoumeh Shafieinejad
Vector Institute
masoumeh@vectorinstitute.ai

Xi He
Vector Inst. & Univesity of Waterloo
xi.he@uwaterloo.ca

Bailey Kacsmar
Amii & University of Alberta
kacsmar@ualberta.ca

***Abstract*—Privacy is an instance of a social norm formed through legal, technical, and cultural dimensions. Institutions such as regulators, industry, and researchers act as societal agents that both influence and respond to evolving norms. Attempts to promote privacy must account for this complexity and the dynamic interactions among these actors. Privacy enhancing technologies (PETs) are technical solutions that allow for the development of solutions that benefit society, while ensuring the privacy of the individuals whose data is being used. However, despite increased privacy challenges and a corresponding increase in new regulations across the globe, a low adoption rate of PETs persists. In this work, we investigate the factors influencing industry's decision-making processes around PETs adoption as well as the extent to which privacy regulations inspire such adoption through a qualitative survey study with 22 industry participants from across Canada Informed by the results of our analysis, we make recommendations for industry, researchers, and policymakers on how to support what each of them seeks from the other when attempting to improve digital privacy protections. By advancing our understanding of what challenges the industry faces, we increase the effectiveness of future privacy research that aims to help overcome these issues.**

I. Introduction

Societal demand for privacy is influencing law-makers, resulting in ongoing introductions of new privacy regulations globally [50], [71], [53], [15]. Most Canadian companies are moderately aware of their responsibilities under Canada's privacy laws and have taken steps to ensure they comply with these laws according to the most recent survey (2023-2024) of Canadian businesses [57]. However, while there has been a lot of effort in privacy enhancing technologies (PETs) research to develop deployable privacy tools that aid organizations, it is unclear whether additional regulations will motivate increased usage of these tools by industry. The divide between research and practice is a prolific one, and it is known that technical developments and the social components of their use in practice can have a great divide [1].

The implications of social contexts for knowledge sharing is an unavoidable first hurdle to bridging the divide before the adoption of novel technologies [3], [2]. In high risk domains, such as emergency rooms, it has been established that better systems emerge when consideration is given to how systems get to those who need them and how to meet those users needs [49]. Thus, researchers need to understand how industry approaches expertise collection if we are going to improve and resolve the gaps and issues originating from different expectations on expertise, communication, and gathering strategies [58], [27]. We investigate the relationship of technical developments of PETs in conjunction with how emergent policies and regulations are influencing adoption or avoidance of such technologies. We observe PETs to be a notable example of the interconnected nature of policy, practice, and design for systems aimed at social-technical problems like digital privacy [32].

A. Research questions

We address the following research questions in the context of Canada's industry and privacy regulations:

- **RQ1:** How does regulation influence industry adoption of PETs?
- **RQ2:** What barriers does industry perceive as preventing them from wanting to or choosing to adopt PETs?
- **RQ3:** What are industry's common practices in regard to sensitive data and PETs?
- **RQ4:** How does industry determine whether they are compliant with relevant laws, regulations, or policies?

We highlight the social challenges expressed by industry as well as propose ways to overcome these issues that contribute to such divides. We focus on the identification of existing or perceived impediments to adopting these technologies and complying with regulations to better understand how the industry-research relationship can be improved. To address our research questions we employ a qualitative survey study with 22 participants. We employ thematic analysis over the collected responses to address our research questions and make the following contributions. (i) We identify insights from industry in regard to how privacy regulations impact their business and their current practices for handling sensitive data. (ii) From our respondents' reported processes, we derive the components of the decision-making process for PETs adoption and its inclusion of both personnel inside and outside of the organizations. (iii) We determine that challenges that impede the adoption of PETs include compatibility with existing systems, feature requirements, lack of clarity for how

Symposium on Usable Security and Privacy (USEC) 2026
27 February 2026, San Diego, CA, USA
ISBN 978-1-970672-07-7
https://dx.doi.org/10.14722/usec.2026.23027
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

they fulfill regulatory requirements, and the broader socio-economic system of industry.

B. Organization

This paper is organized as follows. We present background on PETs and Canada in Section II followed by the relevant related work in Section III, and our methodology is included in Section IV. We organize our results within each research question. Section V is our results for RQ1, Section VI is our results for RQ2, Section VII is our results for RQ3, and Section VIII is our results for RQ4. We provide additional discussion on the key results and impacts of our work in Section IX before ending with our conclusion in Section X.

II. Background

A. What is and is not a PET according to researchers

Privacy-enhancing technologies (PETs) are technical solutions that aim at protecting privacy. These technologies address diverse aspects of privacy, as illustrated by Heurix et al. [29] in their 2015 taxonomy study. There is a wide range of PETs, from 1-n oblivious transfer (OT) [9] in the 1980s to anonymization techniques [69], [43] developed in the 2000s. While many of these PETs have seen practical adoption, their effectiveness can be challenged by emerging attacks and evolving system environments. For instance, k-anonymity [69], initially considered a promising technique for hiding personal identity by masking or generalizing (quasi)-identifiable information, was then shown to be vulnerable to new attacks [43], prompting the development of stronger PETs like differential privacy (DP) [13].

PETs that are widely adopted in the industry, may not represent the state-of-the-art (SOTA) such as k-anonymization for sensitive data release and access control for managing sensitive databases [69], [8]. There are also PETs with widespread deployment and relatively few identified critical vulnerabilities, such as multi-factor authentication [33] for online login, SSL/TLS [42] for data transmission, and AES encryption [28] for data storage. Finally, there are SOTA PETs, which are actively researched but not yet broadly deployed in the industry. These include differential privacy [13], multi-party computation [24], oblivious RAMs [25], [70], homomorphic encryption [7], trusted execution environments (TEEs) [63], federated learning [36], and synthetic data [59], [46]. Our study focuses on understanding what challenges impair industry adoption of these emerging PETs.

While researchers often define PETs as specific algorithms or systems that achieve desired privacy properties, the industry does not necessarily share this definition. Rather, they may include privacy impact/risk assessments, privacy policy development, and privacy control implementation as PETs. Although these practices are essential for establishing privacy within industrial settings and can be significantly supported by PETs, they are not, in themselves, PETs. Rather, they are the frameworks and processes within which PETs can be effectively deployed.

B. Canadian privacy regulations

Personal Information Protection and Electronic Documents Act (PIPEDA) [52] is Canada's federal privacy law for private-sector organizations. It sets out the ground rules for how businesses must handle personal information in the course of their commercial activity. The Canadian government proposed Bill C-27 [53] in 2022 to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act (AIDA). The scope and features of the Acts are summarized in Table II in the appendix. While, the federal privacy law reforms and artificial intelligence regulation contained in the bill are put in an uncertain state following the prorogation of Parliament in January 2025, their potential impact on Canada's industry cannot be ignored [40]. Further, each of Canada's provinces and territories has their own additional privacy regulations and either a commissioner or ombudsperson who is responsible for the privacy legislation in that region [54]. Finally, we note that in Canada, the privacy regulations apply to all sectors and are not separated out by areas such as health having their own regulations. Rather, all sectors must protect that which is deemed to be potentially privacy-harmful regardless of whether the sector that initiated the data collection is a sector considered to be high-risk or privacy critical.

III. Related work

In our work, we center the participants' views and experiences, rather than centering our own preconceived notions or those of the broader research community, to allow us to highlight the differences of interpretations of PETs terminologies (e.g., PETs itself, anonymization, best practices for privacy, etc.) between industry and researchers. Prior research mainly focuses on evaluating comprehension or expectations for a particular PET, such as differential privacy (DP), multiparty computation (MPC), or homomorphic encryption (HE). We provide an overview of related research that seeks to motivate and facilitate the deployment of PETs by examining their interaction with key actors and influencing factors, such as industry needs and regulatory requirements.

A. PETs deployment challenges and facilitators

Numerous studies examine the challenges involved in deploying specific PETs within industry settings. As a promising technique that supports anonymity, Differential privacy (DP) [13] has been the center of attention [12], [14], [21]. Notably, NIST produced a set of guidelines for evaluating DP guarantees [47]. Dwork et al. study deployment challenges by gathering DP experts' opinions in 2019 [14] and distill them into four main categories. Their findings were as well mirrored in the results of a study by Garrido et al. in 2023 [21] on industry participants who were not experts in DP. Several research evaluate or enhance the usability, deployability, and communicative ease of PETs for real-world scenarios. For DP, they cover a wide range, including: user expectations of the DP mechanism [11] and their mental models of DP open-source libraries [67], the usability of DP tools [48], the need

for explanation of the gained privacy [45] in user-suitable metaphors [37] or in risk communication format [20], and considerations for policy makers [44]. The studies of user experience extends to other forms of private computation, such as multi-party computation and private query execution as well [35]. Qin et al. [61] yield insights about the interplay between usability and security in multi-party computation (MPC) applications. For cryptography more broadly, Fischer et al. [19] identify the challenges as: misunderstandings and miscommunication among stakeholders, unclear delineation of responsibilities, misaligned or conflicting incentives, and usability. Agrawal et al. [5] focus on the journey of a number of privacy-preserving computation (PPC) techniques – namely, homomorphic encryption (HE), secure MPC, and DP – from research into production code. They focus on specific application contexts; usability of the libraries and tools from a non-specialist developer's perspective; and the explanation and governance challenges associated with these techniques.

In contrast to the prior research, our work not only includes the technical motivators to PETs adoption, but also the strategic influences – factors that determine whether PETs succeed or fail in real-world cost-benefit evaluations. We explore how industry perceives PETs, what drives their interest, and the obstacles that hinder adoption.

B. PETs and regulations

The introduction of privacy regulations has made evident changes in PETs research papers. Some discuss how their proposed technology aligns with privacy regulations, despite persistent communication gaps between experts in the two fields [31], [26]. For example, synthetic data generation technologies are perceived to provide a practical replacement for the original sensitive data [46], [59]. Others draw inspiration from the tension between data privacy policies and socially beneficial analytics to develop usable, privacy-preserving systems – Synq [17] for instance, exemplifies this in computation over encrypted data. Additionally, some PETs research gives dedicated attention to the technology's relationship with regulations. Walsh et al. [72] examine privacy laws and regulations that limit disclosure of personal data, and explore whether and how these restrictions apply when participants use cryptographically secure multi-party computation (MPC). Another body of work focuses on assessing the privacy promises of PETs [68], [22]. Giomi et al. introduce Anonymeter, a framework for quantifying privacy risk in synthetic data [22], equipped with attack-based evaluations for the singling out, linkability, and inference risks, which are the three key indicators of factual anonymization according to data protection regulations, such as GDPR.

As regulations increasingly mandate the deployment of privacy-preserving mechanisms – and with the emergence of Canada's new privacy regulation (C-27) serving as a key inspiration to this work – we included a focused investigation into how regulations influence PETs adoption.

IV. Methodology

Our study is targeted at the needs, norms, and expectations of industry actors in Canada in regard to privacy regulation and privacy technologies. As these needs and expectations are not well known, we chose to avoid prematurely narrowing the scope of permitted responses to something that would fit within a quantitative survey style. Further, our targeted participant pool corresponded to challenges with time availability and anonymity that prevented a focus group or interview style study. We learned of these challenges during our recruitment effort as participants in industry were concerned with information sharing restrictions as employees. Thus, we chose to do an open-ended survey style to (i) ease access and effort for our intended participant pool while still (ii) affording freedom to our participants concerning how much or how little they shared with us. Our qualitative survey methodology aligns with formal notion of qualitative surveys by Jansen [34] which includes all studies that focus on the diversity of a population. We developed our set of open-ended survey questions to include as few questions as possible while still covering the scope of our research questions. While quantitative surveys typically have more than our six questions, qualitative surveys such as ours have no standard number of questions, rather they focus on coverage in a manner more similar to that of designing interview question guides. In the end, our survey facilitated a non-presumptuous understanding of industry's perspective on privacy, and allowed us to point out areas for future research. The final study consists of an exploratory online survey with six questions where our responses were collected between May 2024 and January 2025.

A. Study domain

We investigate how the industry of Canada approaches the adoption of novel privacy technologies and what impacts this adoption with consideration as to the potential relationship of established policies such as PIPEDA [52] and proposed ones such as Bill C-27 [53]. Our survey questions focus on (i) understanding the existing data handling practices and procedures of companies in Canada, (ii) exploring the impact of regulatory frameworks on privacy practices and technological advancements, and (iii) identifying gaps and challenges in current privacy policies and technologies.

We choose Canada as it has had a version of a national privacy law since the 1980s when the *Privacy Act* [51] was first formulated, and has since seen revisions with PIPEDA in 2000, and a recently proposed update to PIPEDA that was a part of Bill C-27. Based on the privacy law evolution that exists in Canada, we hypothesize that Canada's industries have some basic ways of handling sensitive customer or client data as part of their normal processes. We further hypothesized that the emergence of new regulations may result in companies having concerns that their current, previously compliant, data handling practices may be insufficient and are actively seeking resources and strategies that could address their concerns.

B. Question design and study procedure

Participants entering our study were informed that participation was voluntary and that they could withdraw at any time before they submitted the study by pre-emptively exiting the survey. They were then prompted to indicate via radio button response whether they agreed to participate or did not agree to participate in the study. If they agreed, the study proceeded to our first question and continued until all questions were answered or until the participant exited the study. The full set of questions is included as Appendix A.

In the following, we refer to survey questions as SQs. The questions in our survey build in terms of their specificity. Since more details relating to the goals of our study were included as the questions progressed, the order was not randomized, and each participant received the exact same set of prompts.

For instance, the first question in our survey serves as a general baseline and warm-up question for our participants and asks about the current data handling practices that the respondent's organization may use for customer or client day. The survey then builds up, with SQ2 inviting explanations of what resources or plans the company considers when new privacy regulations emerge, SQ3 asks about compliance, SQ4 queries the decision-making process for the adoption of PETs, SQ5 requests examples of privacy technologies that they perceive as being widely adopted, and finally SQ6 inquires as to what factors ease the use of privacy technologies for their industry. Overall, completing all six questions takes participants approximately 15 minutes.

In developing our questions, we ensured that our design investigates what technologies the industry perceives as privacy-preserving, even if they do not match what research experts in privacy would classify as PETs. We have made an intentional effort in our survey not to predefine these notions, thereby reducing bias. Finally, before releasing our study we ran a small pilot. No issues emerged with the study during this pilot.

C. Participant recruitment

Recruitment: We primarily recruited our participants through a non-university mailing list (a not-for-profit institute in Canada) as well as through the research teams own networks of industry folks. This email list includes 170 contacts of which 143 engaged with the email in some fashion. Of those that engaged with the email approximately 55% have under 200 employees and the remainder have over 200 employees. Of those contacted, the majority are in the information technology sector followed by the health sector and then the financial sector. Two participants were recruited through the sharing of a QR code at an event about new regulations in Canada where the majority of participants were from companies in the technology or financial sector. The rest of the participants, recruited for saturation testing, received an email directly from the research team.

The email, whether from the researchers or sent via the non profit organization, described the research and provided a link to our short survey. Following the link would bring potential participants to our consent information, and then, if they so choose, they could proceed to answer our survey questions or exit the link. Participants were informed clearly that there was no expectation or requirement to participate and that they could quit the study at any time during the survey. To ensure there was no power differential between the researchers and those recruited, the survey was completely anonymous such that we are unable to determine who did or did not participate.

Participants: While we did not collect demographics, we only recruited those who did satisfy our requirements. Participants were between the ages of 18 and 65, working in industry in Canada, and English speaking. We limit participants to adults working in Canada as the focus of our investigation is the Canadian industry's approach to compliance with privacy regulations. We restrict to English speaking as that is the language in which the study is administered.

Our initial recruitment via mailing lists resulted in responses from 16 participants. We then recruited an additional six participants using our personal industry networks. These additional six were selected from different industries and in different roles to test our proximity to reaching thematic saturation [23], at which point after the six participants' responses were included, we found that saturation was reached and we stopped recruitment at our total of $N = 22$ participants. We assigned each participant in our final set a random identifier between one and 60, and referred to them throughout as P#, where # is their identifier.

We note that being a privacy expert is not a requirement for our participants as we are trying to understand industry's perceptions and beliefs about PETs and not to assess their expertise. Rather than evaluating whether or not "industry" has the correct views and whether they are "qualified" to speak on these things we focused on hearing openly what industry members actually think about and respond. Quality of responses was very rich with participants providing several sentences to paragraphs per question as their responses.

D. Research team

Our team includes industry experience as a cryptography consultant as well as expertise and experience in qualitative coding and security and privacy technical expertise. Collectively our team holds expertise relevant to creating and assessing PETS, industry and PETs, and qualitative research.

E. Qualitative analysis

We analyzed participant responses using an inductive approach to allow themes to emerge [64]. Responses were organized first by survey questions. Then, to ensure sound consideration for the breadth of specializd knowledge in the responses relating to industry practices and privacy technologies, all members of the research team collaboratively analyzed all participant's responses to that question. First, the research team employed pre-coding in the form of highlighting or otherwise noting significant participant quotes within each response [41]. Then, for each survey question the responses were transferred to a shared document which contained all participant responses for that question. The research team

then collaboratively moved the responses across the digital file space, which resembles a digital whiteboard, to cluster and group responses based on their similarity following the practice of affinity diagramming (alternatively known as the KJ method) [30], [66], [38]. Once initial consensus was reached that the collaboratively formed clusters were complete, the research team identified a short phrase to capture what was represented in the cluster, which became our sub-themes. The representative short phrase captured either either words or phrases mentioned by respondents (as in In Vivo coding) and values or priorities indicated by the respondents (value coding). After establishing the sub-themes, we analyzed these sub-themes together with the research questions that the survey questions were targeted at. This second phase of analysis produced the final themes that are stated in our results and presented as an overview in Table I of the appendix.

F. Ethics

The full study, including recruitment emails and documents, the survey questions, and our data handling, were reviewed by our institutions' equivalents of IRB. We ensure anonymity by not collecting personal identifiers. All questions were optional and participants could choose to not answer any question. The participants could withdraw by exiting the survey early, without completing it. All of this information was included in the consent form the participants were provided with before they could proceed to complete the survey. As our target participants were industry folks who would be discussing their business practices and norms we wanted to ensure that we could keep their participation private and not have any undue pressure on them. Therefore, we kept our survey short (six questions) and did not provide remuneration that could otherwise connect our participants to our survey. Thus, participants in our study's only benefit is to contribute to science that works towards a better understanding of what fosters or impedes the adoption of privacy technologies by industry.

G. Limitations

Our study focuses on industry within Canada and thus has a Canada-based population, which correspondingly, is a WEIRD[1] population [65]. While this is a limitation of our study, it is a deliberate one, to allow us to focus on an understudied region with established and emerging privacy norms and regulations. In addition, we do not claim that we cover the entire Canadian industry via our study. Instead, we focused on identifying and learning interesting and valuable themes from our participants' responses, which advance our understanding of what the industry in Canada faces and needs. With saturation, we reached a point where no additional themes were emerging, and we deemed it the stopping point for insights that can be gathered from this method. Our responses may have been impacted by the timing of our data collection as most of our responses came in while Bill C-27, which was a privacy law, was under consideration by the Canadian government. We cannot predict how the potential changes that would have resulted had C-27 passed could have impacted our participants or how it may have made regulations more prevalent in participants' minds. Correspondingly, we cannot know how it could have impacted the participants' perceptions on what responses would be more socially desirable, a factor that persists in human-response based empirical studies [62].

[1]Western, Educated, Industrialized, Rich, and Democratic

V. Results on regulation's impact

Our first research question, RQ1, focuses on understanding how regulation influences industry adoption of privacy technologies. In this section we present our results organized by the themes that emerged from the relevant survey questions. These themes emerge from SQ2 which prompted respondents to share what resources or plans their organization considers when faced with new regulations.

A. Evaluate the relationship to their organization

In terms of the relationship regulation has to organizations, participants reported on the importance of compliance in their companies, their views on whether they were beholden to such regulations, and the risk their organizations faced in terms of preserving business processes given changing regulations.

Participants in our study emphasized that any applicable regulations require their compliance, and that fulfilling the requirements of such regulations is something they ensure. P23 emphasized the importance of compliance:

> *"We fully understand the importance of these regulations from both a user and business perspective and are committed to aligning our operations with these standards as we continue to grow." (P23)*

Others even reported learning from regulations, and that they inspired their organization to minimize what they collect such as was the case for P22 in regards to GDPR who stated *"that if we don't collect personally sensitive data, we avoid a lot of risk to our business." (P22).*

While participants emphasized they were cognizant of compliance, they also mentioned that their data may be exempt. For instance, *" We are not directly affected by those regulations, however our clients are affected by those regulation changes"*(P54). Such exemption views include that the data, despite being sensitive, is *"not under the purview of these frameworks"* (P43) and that the regulations *"don't apply to us until the [provincial government] adopts them and formally requests we adhere to them"* (P45).

The final relationship vector discussed by our participants was the potential for it to hinder their business processes. Some expressed concern that they would no longer be able to meet customer demands and that *"...we start to get handcuffed operationally if we have to restrict access"* (P40).

Collectively, participants do report that they make efforts to comply with relevant regulations. However, they also report that they do not collect much sensitive information or that the sensitive information they do collect is not necessarily regulated by such laws.

The conflicting views on what is sensitive data, imply a need for clear guidance on what is and is not regulated and what does and does not satisfy compliance.

B. Monitoring for new guidance

Participants describing their process mentioned a selection of sources as being where they turn to for guidance. When going to official sources such as legislation, participants report it taking extensive reviewing of both the legislation and government summaries. One example provided by a participant about GDPR discussed that reviewing the regulation *"...required a lot of work to click through each of the recommendations, but...I chose to ensure that we were at least current with protocols that were ahead of our legal requirements"* (P22)

Two strategies were reported for finding easier paths to understanding the regulation instead of spending extensive time on government sources. P21 reports that they first, *"review the summaries of the legislation that are put out and if needed review the legislation"* (P21). Other participants have made an effort to acquire additional sources, for instance signing up *"to a few privacy newsletters that allow bite sized consumption of legislative updates across our markets, and we choose to set up notifications for those that appear of interest"*.

Processes do not necessarily rely only on accessing only official government web pages, but also less official, though potentially more intuitive, sources, to learn how the market is impacted by regulations.

C. Identify necessary updates by departmental group

Normal processes, according to our participants, include consideration for the impact structured by the department group. The regulations can cause changes that propagate throughout the entire organization as *"New privacy regulation may result in our internal policy documents and all applications and business lines must follow the policies"*(P51). Determining which departments need what updates may be done through a *"...mapping of the requirements against our frameworks and programs, identification of gaps and plans to make the required updates to support ongoing compliance"* (P4). Ensuring compliance to new regulations includes updates to technical systems, as highlighted by P24 *"...we assess and update our IT systems and processes to meet the new regulatory requirements, including enhanced data protection features or new consent management tools"*. However, the impact on business processes also extends to other internal facing and customer facing departments. Updates are undertaken to "website, marketing, lab services, and software" (P21) as well as to "employee training programs" (P24), and collection practices using "cookies and advertising platforms" (P20).

Updates made in organizations to adapt to new regulations span departments, including less visible ones such as employee training, in addition to more directly impacted ones like IT, legal, and marketing.

D. Consult with appropriate experts

The personnel that are consulted with in regards to how to adapt to new regulations has variations. For some organizations, consultation consists of reviews by their internal *"risk management team"* (P36). Some processes explicitly refer to the vagueness as a factor for why *"The regulations are reviewed by lawyers with a background in privacy"* (P55). Those without such teams may choose to reach outside their organization and *leverage an audit/conformance/assurance partner" (P16)*. Hiring out this task can include having a consulting company that

> *"translates the new regulations and hands them down to us who then explains it to our staff in a more comprehensive manner. The information from the government is FAR to advance for the people who are actually required to do the work"* (P52).

Organizations that are very new, such as startups, may not have internal or external entities they already use. Instead, they may plan to pursue it formally in the future such as to *"...pursue these certifications in the next 6-12 months"* (P23).

The size of the company and how long the company has existed impacts whether it can effectively employ consultation with external experts, outside consultants, or require some future process not yet established.

VI. Results on factors for PETs adoption

Our second research question, RQ2, searches for factors that the industry perceives as important in determining whether they adopt privacy technologies. The following three themes emerged from the analysis of SQ6, which explicitly asked participants what factors influenced the adoption of privacy technologies in their industry.

A. PETs functionalities' compatibility impacts adoption

Our participants highlight both features of PETs that they would view as beneficial in terms of functionality as ones that they view as easing the feasibility of adoption. One aspect that participants report impacting adoption is the effort required to integrate it into their systems. For instance, whether the system is low-impact *"in terms of time and energy"* (P22) or just generally has *"ease of use"* (P55 and P56). Similarly, it should be easy to determine what it can work with as otherwise *"it takes a lot of time to discover whether or not different tools play nice together, especially across platforms"* (P22). The functions need to be compatible with the business goals and support the organizations' *"ability to continue to carry out our mandate"* (P44) which requires there to be "accuracy" (P55)

as well as *"robustness"* (P22), and be both *"scalable"* (P23) and *"affordable"* (P23, P55, P56).

> Ease of integration in terms of time, money, and functionality compatibility with the organization remain factors for technology adoption, including for PETs.

B. The industry's socio-economic system plays an important role in PETs adoption

In terms of PETs adoption, regulatory requirements can encourage the deployment of PETs (P4, P22, P23, P32, P36, P37, P44). However, this encouragement is not unilateral. Participants expressed that for regulations to encourage PETs adoption, the PETs *"technology must comply with relevant privacy regulations"* (P24). While regulation can encourage, participants report several other aspects of the industry's socio-economic system that impact the adoption of PETs. The industry's socio-economic system encompasses its regulatory compliance, market dynamics, interactions with competitors, partners, and emerging innovations that shape its overall position.

Market dynamics, including elements such as client demands, domain expectations, competitors practices, and domain perceived best practices emerged as factors our respondents are influenced by (P21 , P23 , P43, P46). Value was placed on standardization practices, not just by standardization organizations like NIST (P51), but also emergent standards in the form of norms for that field of industry. Emergent standards become not just as safety expectations but also factors that encourage clients to use that business as stated by P23:

> *"if a particular privacy measure is becoming standard in the industry or is being sought after by our clients, it reinforces the need for us to adopt it. Not only do these technologies help safeguard us from potential security breaches, but they also serve as a key selling point for our clients"* (P23).

While the interplay with market dynamics was stated as a motivator for adopting PETs to boost business value and reputation (P36, P44), it was also reported as an impedance for the deployment of less known technologies. For instance, concerns were with how to convey the value in the adoption of PETs deployed by larger competing companies:

> *"It is important that we educate our customers on why we are using different technologies that are not adopted fully in big corporations (especially internationally)"* (P21).

Further relating to organizations needing to account for what large industry leaders are

doing, some report looking to those same large organizations as guides on standards and practices. The views include that since such organizations face bigger consequences for failure they need to pick good practices, or said another way *"large companies are always rightly concerned about data privacy"* (P21). In addition to looking to other organizations to lead, consultants are also employed when considering what best practices are, something that can aid in efficiency for some organizations:

> *"I rely quite heavily on the [consulting] company I hired. I just simply don't have the time it requires or the resources to successfully stay on top of all the new legislation ... and cyber-security [defences]"* (P52).

> The socio-economic system influences companies adoption of PETs. Challenges include what competitors are doing, being able to justify using novel technology that well known large companies are not using, and the time to keep up with new changes and threats.

C. Cost-benefit evaluation forms the process

In the previous theme we discussed how there were several risks that participants expressed concern with, such as the perception of their clients if they used unusual technology. Risks and challenges exist. Correspondingly, it is also the case that a technology's ability to effectively address a data protection need and mitigate the risk of harm and reputation (P16, P23, P24, P36, P43) is necessary for its deployment. While necessary, there are still additional factors that go into the decision process beyond that risk mitigation, as the mitigation is not sufficient on its own. Rather, in addition to successful mitigation, the organization needs to *"... assess whether the technology makes sense from a product and business perspective"* (P23). This assessment can be even more formal when determining whether the overall cost-benefit trade off is worth it, such as using a *" weighted approach to determine which technologies will deliver the greater net benefit for our user base"* (P32).

Among the costs considered by the participants, there are budgetary concerns such as *"the timing, budget, and resources required to implement it effectively"* (P23). In addition to these more conventionally budgetary concerns, there are also concerns for verification needs for organizations that *"conduct regular audits to ensure infrastructure and servers are secure"* (P43). Other costs include efforts to ensure buy-in from both employees and decision makers:

> *"Securing stakeholder buy-in helps ensure the technology receives the necessary resources and backing within the organization...Providing training and raising awareness among employees about the new privacy technologies [also] ensures they are used correctly and helps maintain overall data security"* (P24).

> While addressing a data protection need is essential in considering PETs for deployment, there are many other factors that affect their deployment.

VII. Results on common practices regarding PETs

Our third research question, RQ3, studies the common practices for PETs by industry. We synthesize the results for this question which consist of the emergent themes from SQ4 and SQ5. SQ4 and SQ5, respectively, asked participants about their decision-making process for adopting or developing PETs and an example of what participants thought is a (relatively) widely adopted PET in their domain of industry. We formed a collective diagram of the PETs adoption steps by incorporating the descriptions from each of our participants, which we include as Figure 1 in the appendix. We will refer to Figure 1 throughout this section when it relates to the theme under discussion.

A. Decision-making process for PETs adoption varies across industries and organizations

There is a wide range of responses in our study, spanning from *"our decision-making process is a collaborative effort between our CTO, development team, and leadership"* (P23), to *"our decision-making process for adopting or developing privacy technologies involves several key steps"* (P24). Each company undergoes a sub-diagram process based on their size and structure. For example, some responses suggest that PETs adoption decision-making in smaller companies may require fewer steps, and involve the management earlier in the process:

> *"Due to our smaller size as a company, [PETs adoption] decisions are handled among the management team directly with no real formal process. It is left up to the individual teams to think of privacy"* (P40).

In addition to potentially including management earlier, other small organizations attributed their size as a contributor to how quickly they are able to implement changes:

> *"We have an IT Administrator that reviews industry best practices regularly and recommends changes to the CTO. These changes can be reviewed and implemented quickly because we are a small organization"* (P21).

The decision making process, while varied, has five steps we have identified and summarized in Figure 1. To understand the factors that go into each of the five steps, we present the following detailing of them with examples.

1) Need for PETs: Regardless of speed, what the full process is for determining whether to adopt PETs has variation, with the first step having some form of monitoring the status quo and organizational needs (see the first block in Figure 1). The need may be identified during a regular procedure such as *"following consultation with industry and internal [decision makers]"* (P44) or alternatively because changes are *"legally necessary"* (P37). Those involved in the instigation process can be IT professionals (P21, P53, P54), development team, cyber-security (P44, P53), or subject matter experts (P36). Some of the driving factors in this step are internal, such as addressing an identified vulnerability or a data risk (P16, P24, P32, P36), acting to support road-map (P16), and even just to be as secure as possible (P24). Other motivators are more external such as regulations (P24, P37, P38, P44, P53) and standards (P45), client demand/benefit and reputation (P23, P32, P38, P43), consultation and best practices (P38, P44, P46, P53, P54). Finally, even before proceeding further in the process, the technology's ability to assist with regulation compliance (P24, P38, P44), mitigating risks (P4), boosting the industry's market position (P23), or gaining client's approval (P43) is used to validate the need before moving on to explore solutions viability.

2) Exploring Solutions: The exploratory task of searching for available mitigation solutions to the identified need can be influenced by factors inside and outside of the organization. Outside factors include client demand (P23, P43), and recommendations by existing service providers (P46) while internal factors come through various personnel such as *"internal technology and business leaders"* (P16). Some personnel, such as in the case of organizations with dedicated teams, make direct suggestions where *"recommendations come forward from our cyber-security team" (P44).* Other experts may also suggest solutions, even if they are not part of a dedicated team where *"subject matter experts suggest mitigation plans"* (P36).

Other factors that determine which solutions are explored include market dynamic elements such as business domain practices (P46), competitors (P23), industry best practices (P38, P44), and consultation with legal experts (P44). In some cases, vendor evaluation might even precede the solution search part of the process *"if considering third-party solutions, we assess potential vendors based on their technology, reputation, compliance with industry standards, and support offerings"* (P24).

3) Evaluation of the adoption factors: After the initial solution exploration, and possible vendor evaluation, the next step is to evaluate the potential solutions. For this stage, we refer back to the results in Section VI where the same evaluation factors were synthesized by theme as we found in reports on participants' decision-making process. In short, the evaluation process includes cost-benefit analysis, consideration for internal needs, and the compatibility of the technology with the business goals of the organization. We would like to emphasize that PET adoption factors are often interconnected rather than independent. For instance, lowering integration costs can ease the adoption of a PET within an existing service provider. This, in turn, not only improves acceptance within the vendor but can also influence adoption trends across the broader [customer] industry and establish the PET as a good practice – particularly if promoted by a major company. Once a PET becomes a recognized norm, awareness across the clients grows, and the demand for the same level of privacy protection in other products and services increases. This feedback loop further reinforces adoption, as industries are reluctant to risk their reputation by falling behind on privacy practices.

4) Approval and Post Approval: The process reaches a conclusion when a solution gains preliminary agreement from various stakeholders including IT, security, compliance, as well as user representatives (P21, P36, P53). This preliminary

agreement is termed the initial approval stage in our diagram. After the initial approval is achieved, the next requirement is to demonstrate success through testing (P24, P53). If the testing is successful, then the proposed mitigation solution secures final approval from executives and decision-makers (P21, P24, P44). Once the decision is finalized with all stages of approval, an implementation plan is devised (P24, P36, P55), and the solution's performance is closely monitored during full deployment (P24). Afterward, the solution may receive continued monitoring and could loop back to the beginning of the process shown in Figure 1, where you once again determine if there is a need for new PETs.

> The decision-making process for PETs deployment is affected by both the industry domain and the size of the organization. This can serve as a reminder that there will be no one-size-fits-all solution.

B. There are varied practices, not necessarily PETs, for collecting, storing, analyzing, and utilizing sensitive data

When prompted to describe a privacy-preserving technology method that they thought of as widely adopted, some participants described things which researchers and practitioners in the community would not necessarily think of as PETs.

One such non-PET mentioned is testing, where the testing is *"conducted with a limited user group to evaluate effectiveness, usability, and integration"* (P24). While we can agree that testing is an important part of any system change, it is hard to attribute the testing itself with a privacy-preserving function. Approval processes, where material and information *"must be approved"* (P21) before being shared or disclosed are reminiscent of access control processes, and so move us closer to a PET. A not necessarily technological version of access control is also mentioned as a way to protect data, where the organization's solution is *"Have Structural restrictions to limit peoples ability to access sensitive information internally"* (P22). What we found is that while some participants may not have mentioned specific PETs or strictly defined PETs, they do report various types of controls that are used; including, for example, that *"data retention policy is another controller that is commonly used to ensure compliance with privacy mandates and regulations"* (P36).

Responses also mention de-identification and anonymization (P4, P21, P51, P56) including *"anonymization network which works to advance certainty in the industry around how to do this well"* (P4) and *"data that is published in paper in anonymized"* (P21). However, it is well known that simply anonymization does not guarantee privacy, but this is still a common practice in the industry. For instance, while k-anonymity [69], was initially considered a promising technique for protecting personal identity by masking or generalizing (quasi)-identifiable information, subsequent research has exposed many attacks, including downcoding attacks [10], homogeneity attacks and background knowledge attacks [43]. Beyond these vulnerabilities, k-anonymity faces significant practical challenges, especially for high-dimensional datasets [4]. It is difficult to properly determine which attributes should be considered quasi-identifiers or sensitive attributes, which is a crucial first step in applying the technique. Due to these inherent issues, k-anonymity is no longer the primary focus of the recent research on PETs. On the other hand, more robust PETs like differential privacy [13], [12], [14], [21], have not been mentioned by our participants. However, the adoption of these advanced PETs is challenging, as evidenced by the aforementioned related work in Section III-A on communicating differential privacy and related techniques, which can lead to significant misunderstandings and adoption aversion.

In addition to the non-PETs mentioned, participants also mention a solution that is not itself a PET but is a way to procure PETs. That is, one of the solutions put forth by our participants is to outsource to someone else, such as by using *"Secure infrastructure as offered by the common cloud vendors"* (P37), *"antivirus software"* (P22), *"secure file transfer"* (P36, P53), and *"third-party payment processing"* (P40). However, this vendor reliance practice can also fall short of the core PETs definitions. First, vendor reliance solutions that may use some PET component typically operate on a black box model. This lack of transparency means that users cannot independently verify that the technology is operating with the promised level of privacy. Second, the vendor's platform that offers the PET solution can become a single point of failure, vulnerable to issues such as data breaches, insider attacks, or court orders. Furthermore, the outsourcing solutions often promise privacy through a combination of contractual agreements, internal policies, and security measures, rather than the privacy technologies themselves.

> Industry's approach to privacy-enhancement is not necessarily what researchers perceive it should be. However, understanding these processes may guide our understanding of what type of PETs industry needs.

C. There are some PETs that are perceived as widely adopted

While non-PETs were also mentioned in regards to privacy preservation, more conventional privacy-enhancing techniques were also mentioned by participants. Participants report standardized techniques such as encryption as well as techniques such as access control and password management.

Encryption techniques reported support both data storage and transfer. Encryption has some very specific examples provided by participants such as using *"as 256-bit encryption, which protects data both at rest and during transfer"* (P24) and *"SSL/TLS"* (P46). Specific technologies that employ encryption and facilitate the organization's business processes were highlighted as well.

> *"a huge privacy preserving technology our industry uses would be DocuSign, all documents sent through DocuSign are encrypted"* (P53).

Descriptions in the responses include high-level interpretations about access control such as *"Have Structural restric-*

tions to limit peoples ability to access sensitive information internally" (P22). However, there are no mentions of specific tools that support access control and that granularity of control. There is one detailed example given regarding access control. P32 gives a detailed example,

> *"Intentional regionalization of data. In order to ensure customers maintain the privacy rights afforded to them by where they reside, we offer hosting of our services in multiple geographies, with no data-transfer methods built to move data across these boundaries. We then build our product and privacy practices around the strongest of privacy regulations to allow ourselves a buffer as other jurisdictions adopt parts of these strong privacy regulations."* (P32).

While the description is quite detailed, we do note that it is unclear if the company is using particular in-house database tools or using vendors to support their desired access control policies. We also cannot determine how these practices can meet privacy regulation requirements.

Finally, participants in our study also mention a selection of specific PETs, authentication assistants, password managers, and password assistants. In terms of password management, some mention the practice is company wide, with there being *" enterprise wide password keeper"* (P22) as part of their standard practices. Other access based solutions reported include *"VPN secure sign in."* (P44) and third party access management systems *"for role based account access"* (P46). The mentioned solutions by our participants are still a small subset of the PETs studied by researchers and experts.

> Encryption, access control, and password related solutions are among the PETs that participants mention when asked for ones that are widely deployed.

VIII. Results on compliance verification

The fourth research question, RQ4, is to understand how industry determines whether they are compliant with relevant regulations and policies. The results for this research question are organized by themes that emerged from the analysis of SQ3 along with relevant themes from SQ5 and SQ6.

The responses from SQ3 on the processes industry has for compliance has two overarching types. Some responses include descriptions of very structured approaches and list concrete steps to ensure compliance with existing or emerging privacy regulations. In contrast to the structured approaches, there are those with *"no official processes, and this is a known gap."* (P40). Others are somewhere in between where we do not know the exact steps they undertake, but it is suggested that such steps may exist

> *"We have a very organic process that involves reviewing the legislation and knowing how to navigate issues for our clients"* (P20)

These approaches, whether detailed or ambiguous, can depend on the resources and priority of the organizations. For instance, as we will discuss next, the detailed steps include different personnel in the process, personnel that not all organizations will have.

A. Organizations report various personnel for reviewing privacy compliance

Compliance and its verification is not an isolated task. Participants in our study report a breadth of roles that are responsible for facilitating both compliance efforts and confirmation of compliance. The roles may be filled by internal personnel, external personnel, or a combination of both internal and external personnel.

The internal team can have a designated role, where *"Risk management monitors the change in the landscape and will assess the impact of the regulations"* (P36). They can also be responsible for maintaining privacy and compliance more broadly or as a point of contact for regulatory authorities and individuals.

> *"There is an internal compliance team that maintains the privacy program, reviews emerging regulations, and has internal audit capability to ensure the organization is ready for emerging privacy regulations"* (P32).

Some internal teams collaborate with external partners and clients to review the legislation/government/sector actions (P38, P20, P43, P54, P56).

> *"Our in-house data team monitors the changes and works with our external partner to understand what is applicable to us. We allocate resources based on the priority of implementing these changes in the recommended order"* (P38).

In terms of strictly external personnel, some respondents report that they have trusted legal advisors for consultation and collaboration (P16, P21, P23, P52). They state that the value of such personnel corresponds to the risk of failing to meet these requirements:

> *"if we were to ever miss something from the CRA or PIPEDA we would be fined so fast. So we took the step to hire someone who will never put us in that position"* (P52).

> Ensuring compliance relies on expertise from personnel, who may be on internal teams, internal personnel that consult with external experts, or external contractors that advise on proper compliance practices.

B. Compliance validation includes changes across a range of internal processes

The responses include different classes of internal changes that could be triggered by privacy compliance. Ensuring compliance is something that requires changes to the actual systems, not just as a way to verify compliance, but also as a way to establish new normal processes. To update these practices, some organizations ensure that *"Training is provided*

to employees on data protection principles, privacy policies, and regulatory requirements to ensure they understand their responsibilities" (P24).

Further efforts include transparency through the creation and publication of *" accountability management framework"* (P4) as well as ensuring *"policies are in place to ensure that data of a sensitive nature is not sent out"* (P22). These changes are reflected both in processes and in communications:

> *"Our website and marketing follows best practices that our advisors and internet resources suggest. We have a standard privacy agreement that we use with customers that protects data generated"* (P21)

Compliance efforts include not just changes to actual processes, but also changes to training procedures and updating communications to increase transparency.

C. Process descriptions include a reliance on external organizations rather than specific PETS for privacy compliance

Participants report a reliance on the personnel in organizations they outsource to for software solutions to provide any compliance assurances (P43, P23, P45, P46). Participants rely on organizations such as Microsoft Services and AWS to ensure they are compliant with relevant laws.

> *"Our current approach includes leveraging AWS cloud storage and their security features. We also maintain strict policies against sharing or selling personal data and ensure all survey data is aggregated and anonymized"* (P23).

Responses mention the use of cloud services as the support for security and privacy, which assumes the out-sourced service, such as the cloud service provider or the credit card company, provides sufficient technology to support privacy compliance.

A reliance on outsourced solutions is one strategy for complying with regulations. However, it is unclear whether such solutions can actually ensure compliance.

IX. Discussion

Our survey results create a rich picture that consists of an overview of the PETs adoption process in industry and the roles of the actors who influence it. To fulfill our mission of strengthening connections within the researcher-regulator-industry practitioner triangle, we share some general insights for all three parties and specific findings for each.

A. A unique and dynamic multi-stakeholder ecosystem

For privacy, all elements of the socio-economic system — from regulations to client demand, consultants, competitors, best practices, market position, and reputation — play an active role in various phases of the decision-making journey. Hence, we observe these actions unfolding simultaneously: regulators striving to translate public demand into legislation, industry working to meet market privacy needs *and* ensuring compliance, and researchers developing privacy-preserving technologies that align with real-world concerns by supporting regulation and industry adoption. This interdependence can be frustrating, as each group relies on others whose work is still evolving. However, with effective communication, these efforts can align and reinforce one another.

Compliance verification is an example of a pain point that is notably challenging at this time. To elaborate on the nature of the compliance issue, we focus on the example of anonymity and de-identification as a fundamental pillar of privacy regulations. On one hand, de-identification and anonymity is one of the main privacy topics that were brought up repeatedly in our survey responses. Many mentioned it to be one of the widely deployed privacy enhancing technologies/methods in their industry. However, as we mentioned in Section I, Canadian regulators are highly concerned about industry self regulating [16] on the topic, since the methods industry uses for anonymity are not clear in design or implementation, and are not unified across industry. On the other hand, there are numerous research papers on how various PETs can assist with anonymity and de-identification or evaluate it. This presents an opportunity for collaboration among the three parties. Research institutes, in partnership with industry leaders, can respond to Canadian regulators' call for *issuing codes of practice and certifications by non-regulatory bodies*. This can be achieved by leveraging PETs to provide a unified, systematic, and quantifiable evaluation of anonymization, such as through the use of privacy attacks like membership inference [68], [22].

B. Key findings by stakeholder

Key findings for research institutes: It is advantageous that the usability of PETs is already receiving a lot of attention in the research community. However, it is also crucial to consider PETs compatibility and integration with the existing platforms in industry (recall from Section VI), in addition to their verifiability and compliance (recall from Section VIII). The issuance of certificates by research institutes would be a collaborative effort that could help with the verification process, particularly if is aligned with regulatory requirements, which could then further support PETs adoption. The development of PETs that assist in evaluating privacy requirements will also be greatly valuable to industry actors as it will aid in facilitating regulatory enforcement with additional transparency and testability.

Understanding market dynamics in PETs adoption can help researchers navigate the challenges of bringing their work into industry. Our survey suggests that the choice of which PETs to adopt may be influenced by recommendations from existing service providers. Similarly, smaller companies may implement PETs more quickly due to management involvement earlier in the process, but they may struggle to convince clients to adopt solutions that lack widespread use among larger companies. Additionally, we identify the personnel departments responsible for assessing the need for PETs and exploring mitigation strategies, which are not limited to personnel on privacy focused teams. This suggests that an effective way of propagating PETs in industry is illustrating who among

their peers uses the same or similar systems. Such a peer based grouping seems to be the closest approximation to communities of practice for our participants [73]. Therefore, a viable approach to enhance acceptance is integrating PETs with established solutions. As participants identify blogs and digital newsletters as a source of information, an example of computer-mediated communication that could be harnessed by the technical research community more effectively [60], such platforms may be effective if used to communicate about usages and acceptance rates by peers.

Key findings for regulators: Our study suggests that industry professionals often seek clearer, more accessible communication regarding the regulations that apply to them, along with practical advice on how to achieve compliance. We note that according to a recent Canadian business survey result [57], only one out of four of Canadian businesses have used the information and tools provided by OPC (Office of the Privacy Commissioner of Canada) despite being aware of them. In our survey, respondents (recall Section V) reported government resources to be challenging to use and that they refer to privacy newsletters and other more easily understood sources when trying to decipher new requirements. Informed by our findings, we suggest that it would be beneficial to offer guidance that combines the authority of official sources with the actionable insights typically found in informal channels such as blogs, newsletters, or technical tutorials. Our survey identifies the key resources that Canadian industries rely on for regulatory compliance; from domain experts to consulting firms. Privacy regulators may find it more effective to address communication challenges by engaging with these intermediary parties, to ensure that industry receives clearer and more actionable compliance guidance. This approach could not only improve clarity but also make compliance more attainable for smaller companies that lack dedicated teams for separate tasks or face challenges in securing external counsel, which may lead them to adopt a follower strategy based on larger companies' practices.

Key findings for industry practitioners: While no outcome is more rewarding for researchers than seeing their designed PETs deployed in practice, this deployment remains a challenge. Our findings highlight key privacy focus areas in industry that we suggest will benefit from existing research dedicated to PETs design and development in these areas. While industry participants in our study employ well-established products, emerging PETs developed by researchers can offer valuable contributions; both in terms of privacy-preserving and privacy evaluation solutions. For example, in anonymity and de-identification context, current commercial data synthesis applications [56], [6] either follow data sanitizing practices such as removing identifiers, or have not yet reached a level of maturity that allows them to scale effectively with the complexities and volume of industry data. However, there are several research papers advancing against the various practical problems of data synthesis [39], [55], [74].

We propose that one key barrier to the adoption of emerging PETs is a lack of awareness among decision-makers responsible for implementing these technologies. Ensuring that personnel departments stay informed about the latest PETs advancements through education and communication can help bridge this gap. Moreover, by actively communicating their desired features to the research community, industry practitioners can also help with shaping the future of PETs, ensuring that new developments align more closely with real-world needs and constraints.

C. Future Research Directions

We unfold several avenues for deeper investigation and future research. First, there is a need for a thorough picture of PETs used in industry. Our study identifies the privacy focus areas for industry practitioners and their decision making process to adopt PETs with participants mentioning widely adopted privacy enhancing technologies (recall Section VII), but not recent or state-of-the art ones. Second, we emphasize the importance of understanding the impact on privacy due to the ongoing evolution of AI adoption in industry. Future research on the effect of AI on privacy critical areas is crucial as AI technologies continue to evolve and integrate into various sectors. For example, the common strategy reported by participants of "removing identifiers" becomes even less effective in the age of AI, as advanced pattern recognition and memorization capabilities [18] enable re-identification more easily than ever before. Similarly, consent tracking or data disposal is more challenging when the data is used in model training. Finally, we recommend investigation into how best practices emerge. "Best practices" were repeatedly mentioned in our survey as a key resource for addressing various challenges, from regulatory compliance to selecting appropriate PETs solutions. Identifying what drives the initial emergence and integration of these best practices is essential for understanding how privacy technologies gain momentum and eventually become standard in industry practices.

X. Conclusion

Through this study, we identify the breadth of approaches employed by organizations considering PETs and the challenges they face. We further identify a gap between how companies think of privacy technologies and how researchers think of privacy technologies that can contribute to low adoption of the increasingly sophisticated privacy technologies produced by researchers, such as applications of differential privacy, multiparty computation, and trusted execution environments. Thus, clear communication between all parties is needed to ensure all parties share the same understanding of what technical privacy systems can and cannot guarantee. While emergent PETs may not have a clear adoption process as of yet, researchers and policymakers can improve the privacy of the populace through tailoring their efforts to better account for the needs of industry we have brought to the forefront.

Acknowledgment

The work of Xi He was supported by NSERC through a Discovery Grant, an alliance grant, and the Canada CIFAR AI

Chairs program. The work of Bailey Kacsmar was supported by NSERC through a Discovery Grant (RGPIN-2024-04996).

REFERENCES

[1] M. S. Ackerman, "The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility," Human–Computer Interaction, vol. 15, no. 2-3, pp. 179–203, 2000.

[2] M. S. Ackerman, J. Dachtera, V. Pipek, and V. Wulf, "Sharing Knowledge and Expertise: The CSCW View of Knowledge Management," Computer Supported Cooperative Work (CSCW), vol. 22, pp. 531–573, 2013.

[3] M. S. Ackerman, V. Pipek, and V. Wulf, Sharing Expertise: Beyond Knowledge Management. USA: MIT press, 2003.

[4] C. C. Aggarwal, "On k-anonymity and the curse of dimensionality," in Proceedings of the 31st International Conference on Very Large Data Bases, ser. VLDB '05. VLDB Endowment, 2005, p. 901–909.

[5] N. Agrawal, R. Binns, M. Van Kleek, K. Laine, and N. Shadbolt, "Exploring Design and Governance Challenges in the Development of Privacy-Preserving Computation," in Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, ser. CHI '21. New York, NY, USA: Association for Computing Machinery, 2021. [Online]. Available: https://doi.org/10.1145/3411764.3445677

[6] G. AI, "Gretel: Privacy Engineering for Developers," https://gretel.ai/, n.d., accessed: 2025-02-28.

[7] F. Armknecht, C. Boyd, C. Carr, K. Gjøsteen, A. Jäschke, C. A. Reuter, and M. Strand, "A Guide to Fully Homomorphic Encryption," IACR Cryptol. ePrint Arch., vol. 2015, p. 1192, 2015. [Online]. Available: https://api.semanticscholar.org/CorpusID:12737699

[8] J. Borking, P. Verhaar, B. Eck, P. Siepel, G. Blarkom, R. Coolen, M. Uyl, J. Holleman, P. Bison, R. Veer, J. Giezen, A. Patrick, C. Holmes, J. Lubbe, R. Lachman, S. Kenny, R. Song, K. Cartrysse, J. Huizenga, and X. Zhou, Handbook of Privacy and Privacy-Enhancing Technologies The Case of Intelligent Software Agents. Netherlands: CBP (Dutch Data Protection Authority), 2003.

[9] G. Brassard, C. Crépeau, and J.-M. Robert, "All-or-Nothing Disclosure of Secrets," in Proceedings on Advances in Cryptology—CRYPTO '86. Berlin, Heidelberg: Springer-Verlag, 1987, p. 234–238.

[10] A. Cohen, "Attacks on deidentification's defenses," in 31st USENIX Security Symposium (USENIX Security 22). Boston, MA: USENIX Association, Aug. 2022, pp. 1469–1486. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/cohen

[11] R. Cummings, G. Kaptchuk, and E. M. Redmiles, "" I need a better description": An Investigation Into User Expectations For Differential Privacy," in Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. USA: ACM, 2021, pp. 3037–3052.

[12] R. Cummings and J. Sarathy, "Centering Policy and Practice: Research Gaps Around Usable Differential Privacy," in 2023 5th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA). Atlanta, GA, USA: IEEE, 2023, pp. 122–135.

[13] C. Dwork, "Differential Privacy," in Automata, Languages and Programming, M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 1–12.

[14] C. Dwork, N. Kohli, and D. Mulligan, "Differential Privacy in Practice: Expose your Epsilons!" Journal of Privacy and Confidentiality, vol. 9, no. 2, Oct. 2019. [Online]. Available: https://journalprivacyconfidentiality.org/index.php/jpc/article/view/689

[15] L. Edwards, "The EU AI Act: A Summary of its Significance and Scope," Artificial Intelligence (the EU AI Act), vol. 1, p. 25, 2021.

[16] K. El Emam, A. Fineberg, E. Jonker, and L. Pilgram, "Perspectives of Canadian Privacy Regulators on Anonymization Practices and Anonymized Information: A Qualitative Study," International Data Privacy Law, vol. 14, no. 4, pp. 391–403, 12 2024. [Online]. Available: https://doi.org/10.1093/idpl/ipae017

[17] Z. Espiritu, M. George, S. Kamara, and L. Qin, "Synq: Public Policy Analytics Over Encrypted Data," in 2024 IEEE Symposium on Security and Privacy (SP). USA: IEEE, 2024, pp. 146–165.

[18] V. Feldman, "Does Learning Require Memorization? A Short Tale About a Long Tail," in Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, ser. STOC 2020. New York, NY, USA: Association for Computing Machinery, 2020, p. 954–959. [Online]. Available: https://doi.org/10.1145/3357713.3384290

[19] K. Fischer, I. Trummová, P. Gajland, Y. Acar, S. Fahl, and A. Sasse, "The Challenges of Bringing Cryptography from Research Papers to Products: Results from an Interview Study with Experts," in 33rd USENIX Security Symposium (USENIX Security 24). Philadelphia, PA: USENIX Association, Aug. 2024, pp. 7213–7230. [Online]. Available: https://www.usenix.org/conference/usenixsecurity24/presentation/fischer

[20] D. Franzen, S. Nuñez von Voigt, P. Sörries, F. Tschorsch, and C. Müller-Birn, "Am I private and if so, how many? Communicating Privacy Guarantees of Differential Privacy with Risk Communication Formats," in Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. USA: ACM, 2022, pp. 1125–1139.

[21] G. M. Garrido, X. Liu, F. Matthes, and D. Song, "Lessons Learned: Surveying the Practicality of Differential Privacy in the Industry," Proceedings on Privacy Enhancing Technologies, vol. 2023, pp. 151–170, 2023.

[22] M. Giomi, F. Boenisch, C. Wehmeyer, and B. Tasn'adi, "A Unified Framework for Quantifying Privacy Risk in Synthetic Data," Proc. Priv. Enhancing Technol., vol. 2023, pp. 312–328, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:253735298

[23] B. Glaser and A. Strauss, Discovery of Grounded Theory: Strategies for Qualitative Research. London, England: Routledge, 2017.

[24] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," in Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing, ser. STOC '87. New York, NY, USA: Association for Computing Machinery, 1987, p. 218–229. [Online]. Available: https://doi.org/10.1145/28395.28420

[25] O. Goldreich and R. Ostrovsky, "Software protection and simulation on oblivious rams," J. ACM, vol. 43, no. 3, p. 431–473, May 1996. [Online]. Available: https://doi.org/10.1145/233551.233553

[26] R. Grover, "Encoding privacy: Sociotechnical dynamics of data protection compliance work," in CHI '24: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, 2024, pp. 1–13.

[27] C. A. Halverson, T. Erickson, and M. S. Ackerman, "Behind the Help Desk: Evolution of a Knowledge Management System in a Large Organization," in Proceedings of the 2004 ACM conference on Computer supported cooperative work (CSCW). USA: ACM, 2004, pp. 304–313.

[28] S. Heron, "Advanced encryption standard (aes)," Network Security, vol. 2009, no. 12, pp. 8–12, 2009. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1353485810700064

[29] J. Heurix, P. Zimmermann, T. Neubauer, and S. Fenz, "A Taxonomy for Privacy Enhancing Technologies," Computers & Security, vol. 53, pp. 1–17, 2015.

[30] K. Holtzblatt and H. Beyer, Contextual design: defining customer-centered systems. Elsevier, 1997.

[31] S. A. Horstmann, S. Domiks, M. Gutfleisch, M. Tran, Y. Acar, V. Moonsamy, and A. Naiakshina, ""those things are written by lawyers, and programmers are reading that." mapping the communication gap between software developers and privacy experts," Proc. Priv. Enhancing Technol., vol. 2024, pp. 151–170, 2024. [Online]. Available: https://api.semanticscholar.org/CorpusID:264469052

[32] S. J. Jackson, T. Gillespie, and S. Payette, "The Policy Knot: Re-integrating Policy, Practice and Design in CSCW Studies of Social Computing," in Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing (CSCW), ser. CSCW '14. New York, NY, USA: Association for Computing Machinery, 2014, p. 588–602. [Online]. Available: https://doi.org/10.1145/2531602.2531674

[33] C. Jacomme and S. Kremer, "An extensive formal analysis of multi-factor authentication protocols," ACM Trans. Priv. Secur., vol. 24, no. 2, Jan. 2021. [Online]. Available: https://doi.org/10.1145/3440712

[34] H. Jansen et al., "The logic of qualitative survey research and its position in the field of social research methods," in Forum Qualitative Sozialforschung/Forum: Qualitative Social Research, vol. 11, no. 2, 2010.

[35] B. Kacsmar, V. Duddu, K. Tilbury, B. Ur, and F. Kerschbaum, "Comprehension from chaos: Towards informed consent for private computation," in Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security. USA: ACM, 2023, pp. 210–224.

[36] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings, R. G. L. D'Oliveira, H. Eichner, S. E. Rouayheb, D. Evans, J. Gardner, Z. Garrett, A. Gascón, B. Ghazi, P. B. Gibbons, M. Gruteser,

Z. Harchaoui, C. He, L. He, Z. Huo, B. Hutchinson, J. Hsu, M. Jaggi, T. Javidi, G. Joshi, M. Khodak, J. Konecný, A. Korolova, F. Koushanfar, S. Koyejo, T. Lepoint, Y. Liu, P. Mittal, M. Mohri, R. Nock, A. Özgür, R. Pagh, H. Qi, D. Ramage, R. Raskar, M. Raykova, D. Song, W. Song, S. U. Stich, Z. Sun, A. T. Suresh, F. Tramèr, P. Vepakomma, J. Wang, L. Xiong, Z. Xu, Q. Yang, F. X. Yu, H. Yu, and S. Zhao, "Advances and Open Problems in Federated Learning," Foundations and Trends in Machine Learning, vol. 14, no. 1–2, pp. 1–210, 2021. [Online]. Available: http://dx.doi.org/10.1561/2200000083

[37] F. Karegar, A. S. Alaqra, and S. Fischer-Hübner, "Exploring User-Suitable Metaphors for Differentially Private Data Analyses," in Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022). USA: USENIX, 2022, pp. 175–193.

[38] J. Kawakita, "The original kj method," Tokyo: Kawakita Research Institute, Tech. Rep., 1991.

[39] M. Kollovieh, A. F. Ansari, M. Bohlke-Schneider, J. Zschiegner, H. Wang, and Y. B. Wang, "Predict, refine, synthesize: Self-guiding diffusion models for probabilistic time series forecasting," in Advances in Neural Information Processing Systems, A. Oh, T. Naumann, A. Globerson, K. Saenko, M. Hardt, and S. Levine, Eds., vol. 36. USA: Curran Associates, Inc., 2023, pp. 28 341–28 364.

[40] A. LaCasse, "Bill C-27 Awaits Fate After Canada's Prime Minister Resigns," International Association of Privacy Professionals (IAPP) News, January 2025. [Online]. Available: https://iapp.org/news/a/bill-c-27-awaits-fate-after-canadas-prime-minister-resigns

[41] D. Layder, Sociological practice: Linking theory and social research. Sage, 1998.

[42] H. K. Lee, T. Malkin, and E. Nahum, "Cryptographic Strength of SSL/TLS Servers: Current and Recent Practices," in Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement, ser. IMC '07. New York, NY, USA: Association for Computing Machinery, 2007, p. 83–92. [Online]. Available: https://doi.org/10.1145/1298306.1298318

[43] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "L-diversity: Privacy Beyond k-anonymity," ACM Trans. Knowl. Discov. Data, vol. 1, no. 1, p. 3–es, Mar. 2007. [Online]. Available: https://doi.org/10.1145/1217299.1217302

[44] P. Nanayakkara and J. Hullman, "What to Consider When Considering Differential Privacy for Policy," Policy Insights from the Behavioral and Brain Sciences, vol. 11, no. 2, pp. 132–140, 2024.

[45] P. Nanayakkara, M. A. Smart, R. Cummings, G. Kaptchuk, and E. M. Redmiles, "What are the Chances? Explaining the Epsilon Parameter in Differential Privacy," in 32nd USENIX Security Symposium (USENIX Security 23). USA: USENIX, 2023, pp. 1613–1630.

[46] National Institute of Standards and Technology, "2018 Differential Privacy Synthetic Data Challenge," https://www.nist.gov/ctl/pscr/open-innovation-prize-challenges/past-prize-challenges/2018-differential-privacy-synthetic, 2018, accessed 2025-02-26.

[47] J. P. Near, D. Darais, N. Lefkovitz, G. Howarth et al., "Guidelines for Evaluating Differential Privacy Guarantees," National Institute of Standards and Technology, Tech. Rep, pp. 800–226, 2023.

[48] I. C. Ngong, B. Stenger, J. P. Near, and Y. Feng, "Evaluating the Usability of Differential Privacy Tools with Data Practitioners," in Twentieth Symposium on Usable Privacy and Security (SOUPS 2024). USA: USENIX, 2024, pp. 21–40.

[49] M. Normark and D. Randall, "Local Expertise at an Emergency Call Centre," in ECSCW 2005: Proceedings of the Ninth European Conference on Computer-Supported Cooperative Work, 18–22 September 2005, Paris, France, Springer. USA: Springer, 2005, pp. 347–366.

[50] G. of Caliornia, "California Consumer Privacy Act (CCPA)," https://oag.ca.gov/privacy/ccpa, 2018, california Civil Code §§ 1798.100 et seq. [Online]. Available: https://oag.ca.gov/privacy/ccpa

[51] G. of Canada, "The Privacy Act," https://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html/, 1985. [Online]. Available: https://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html/

[52] ——, "Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)," https://laws-lois.justice.gc.ca/eng/acts/P-8.6/, 2000, statutes of Canada 2000, c. 5. [Online]. Available: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/

[53] P. of Canada, "Bill C-27: Canada's Digital Charter Implementation Act," https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/LegislativeSummaries/PDF/44-1/44-1-C27-E.pdf, 2022, 44th Parliament, 1st Session. [Online]. Available: https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/LegislativeSummaries/PDF/44-1/44-1-C27-E.pdf

[54] O. of the Privacy Commisioner of Canada, "Provincial and Territorial Privacy Laws and Oversight," https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/, 2024, accessed: 2025-02-28.

[55] W. Pang, M. Shafieinejad, L. Liu, S. Hazlewood, and X. He, "ClavaDDPM: Multi-relational Data Synthesis with Cluster-guided Diffusion Models," in Advances in Neural Information Processing Systems, A. Globerson, L. Mackey, D. Belgrave, A. Fan, U. Paquet, J. Tomczak, and C. Zhang, Eds., vol. 37. USA: Curran Associates, Inc., 2024, pp. 83 521–83 547.

[56] N. Patki, R. Wedge, and K. Veeramachaneni, "The Synthetic Data Vault," in 2016 IEEE international conference on data science and advanced analytics (DSAA), IEEE. USA: IEEE, 2016, pp. 399–410.

[57] Phoenix Strategic Perspectives Inc., "2023-24 Survey of Canadian Businesses on Privacy-Related Issues," Office of the Privacy Commissioner of Canada, Gatineau, Quebec, Tech. Rep., March 2024, catalogue Number: IP54-96/2024E-PDF; ISBN: 978-0-660-71662-6.

[58] V. Pipek, V. Wulf, and A. Johri, "Bridging Artifacts and Actors: Expertise Sharing in Organizational Ecosystems," Computer Supported Cooperative Work (CSCW), vol. 21, pp. 261–282, 2012.

[59] V. K. Potluru, D. Borrajo, A. Coletta, N. Dalmasso, Y. El-Laham, E. Fons, M. Ghassemi, S. Gopalakrishnan, V. Gosai, E. Kreačić, G. Mani, S. Obitayo, D. Paramanand, N. Raman, M. Solonin, S. Sood, S. Vyetrenko, H. Zhu, M. Veloso, and T. Balch, "Synthetic Data Applications in Finance," arXiv preprint arXiv:2401.00081, 2024.

[60] J. Preece, Online Communities: Designing Usability and Supporting Socialbilty. USA: John Wiley & Sons, Inc., 2000.

[61] L. Qin, A. Lapets, F. Jansen, P. Flockhart, K. D. Albab, I. Globus-Harris, S. Roberts, and M. Varia, "From Usability to Secure Computing and Back Again," in Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019). Santa Clara, CA: USENIX Association, Aug. 2019, pp. 191–210. [Online]. Available: https://www.usenix.org/conference/soups2019/presentation/qin

[62] E. M. Redmiles, Z. Zhu, S. Kross, D. Kuchhal, T. Dumitras, and M. L. Mazurek, "Asking for a Friend: Evaluating Response Biases in Security User Studies," in Proceedings of the 2018 acm sigsac conference on computer and communications security. USA: ACM, 2018, pp. 1238–1255.

[63] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted Execution Environment: What It is, and What It is Not," in 2015 IEEE Trustcom/BigDataSE/ISPA, vol. 1. Helsinki, Finland: IEEE, 2015, pp. 57–64.

[64] J. Saldaña, The Coding Manual for Qualitative Researchers. London, England: SAGE publications Ltd, 2021.

[65] J. Schulz, D. Bahrami-Rad, J. Beauchamp, and J. Henrich, "The Origins of WEIRD Psychology," Available at SSRN 3201031, vol. 2018, 2018.

[66] R. Scupin, "The kj method: A technique for analyzing data derived from japanese ethnology," Human Organization, vol. 56, no. 2, pp. 233–237, 1997.

[67] P. Song, J. Sarathy, M. Shoemate, and S. Vadhan, "" I Inherently Just Trust That it Works": Investigating Mental Models of Open-Source Libraries for Differential Privacy," Proceedings of the ACM on Human-Computer Interaction, vol. 8, no. CSCW2, pp. 1–39, 2024.

[68] T. Stadler, B. Oprisanu, and C. Troncoso, "Synthetic Data–Anonymisation Groundhog Day," in 31st USENIX Security Symposium (USENIX Security 22). USA: USENIX, 2022, pp. 1451–1468.

[69] L. Sweeney, "K-anonymity: A Model for Protecting Privacy," Int. J. Uncertain. Fuzziness Knowl.-Based Syst., vol. 10, no. 5, p. 557–570, Oct. 2002. [Online]. Available: https://doi.org/10.1142/S0218488502001648

[70] S. Tople, Y. Jia, and P. Saxena, "PRO-ORAM: Practical Read-Only Oblivious RAM," in 22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019). Chaoyang District, Beijing: USENIX Association, Sep. 2019, pp. 197–211. [Online]. Available: https://www.usenix.org/conference/raid2019/presentation/tople

[71] E. Union, "General data protection regulation (gdpr)," https://eur-lex.europa.eu/eli/reg/2016/679/oj, 2016, regulation (EU) 2016/679 of the European Parliament and of the Council. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj

[72] J. M. Walsh, M. Varia, A. Cohen, A. Sellars, and A. Bestavros, "Multi-Regulation Computing: Examining the Legal and Policy Questions

That Arise From Secure Multiparty Computation," in Proceedings of the 2022 Symposium on Computer Science and Law, ser. CSLAW '22. New York, NY, USA: Association for Computing Machinery, 2022, p. 53–65. [Online]. Available: https://doi.org/10.1145/3511265.3550445

[73] E. Wenger, Communities of Practice: Learning, Meaning, and Identity. United Kingdon: Cambridge university press, 1999.

[74] H. Zhang, J. Zhang, Z. Shen, B. Srinivasan, X. Qin, C. Faloutsos, H. Rangwala, and G. Karypis, "Mixed-Type Tabular Data Synthesis with Score-Based Diffusion in Latent Space," in The Twelfth International Conference on Learning Representations. USA: ICLR, 2024. [Online]. Available: https://openreview.net/forum?id=4Ay23yeuz0

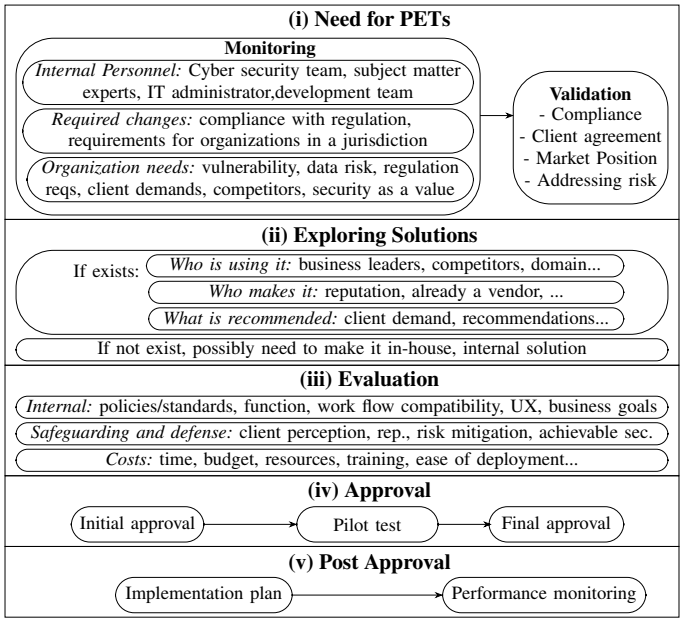

Fig. 1. Decision-making process for PETs adoption as captured from the respondents. The process flows from top to bottom for the large rectangular steps and proceeds through the different components within each larger overall step.

APPENDIX

A. Survey Questions

The following are our six open-ended free-form text response questions we used as our survey. These were made available to our participants after the consent page. The order was not randomized and each participant received the exact same set of prompts.

The informed consent page that was shown requested participants consent or decline to participate in the study. This consent page was also when they were informed about being able to skip questions, quit at any time, and any other relevant information for their decision to proceed through our study.

SQ1 What are the current data handling best practices regarding potentially sensitive customer or client data within your company? This includes methods for collection, storage, analysis, and utilization of such data.

SQ2 When new privacy regulations (such as GDPR, CCPA, PIPEDA, or Bill C-27) emerge, what resources or plans does your company consider in determining the best course of action?

SQ3 What processes does your organization employ to ensure compliance with existing or emerging privacy regulations?

SQ4 Please outline the decision-making process within your company regarding the adoption or development of privacy technologies. For example, when considering the adoption of methods like two-factor authentication.

SQ5 Please describe an example of a privacy-preserving technology method for the collection, storage, analysis, and utilization of sensitive data that you think is (relatively) widely adopted in your domain of industry.

SQ6 What factors facilitate the integration or creation of privacy technology methods for the collection, storage, analysis, and utilization of sensitive data within your domain of industry?

B. Decision-making process for PETs adoption

Figure 1 illustrates the decision-making process for PETs adoption as captured from the respondents.

C. Themes and Sub-Themes

Table I provides an overview of our themes and sub-themes that emerged during our analysis.

D. Canadian Policies

Table II provides a summary of Canadian privacy and AI regulations.

RQ1 Themes and Sub-Themes				
Theme: Evaluate the relationship to their organization				
Compliance	Relevance	Cost evaluation	Market loss	Risk evaluation
Theme: Monitoring for new guidance and reports				
	(Official) Summaries	Review legislation	News letters	
Theme: Identify necessary updates by departmental group				
	IT systems	Employee training	Control systems/processes	
Theme: Consult with appropriate experts				
Legal team	Outsource/external counsel	Privacy team	Risk management team	Certification
RQ2 Themes and Sub-Themes				
Theme: PETs functionalities' compatibility impacts adoption				
Adoptability	PETs design features	Amount of data	Learnability	Usability
Theme: The industry's socio-economic system plays an important role in PETs adoption				
	Business logic	Regulations	Validation	Audits
Theme: Cost-benefit evaluation forms the process				
Roadmap	Risk management	Resources	Education	Verification
RQ3 Themes and Sub-Themes				
Theme: Decision-making process for PETs adoption varies across industries and organizations				
Company size	Dedicated teams	New Initiatives Review	Regular Monitoring	Consultation
Data risks	Roadmap	Regulations	Reputation	Best practices
Clients	Existing services & vendors	Business leaders	Competitors	Legal consultants
IT	Development team	Cyber-security	Compliance	Decision makers
Theme: There are varied practices, not necessarily PETs, for collecting, storing, analyzing, and utilizing sensitive data				
Outsourcing	Approval processes	Data retention policies	Performance monitoring	Anonymization
Theme: There are some PETs that are perceived as widely adopted				
	Encryption	Access control	Password management	
RQ4 Themes and Sub-Themes				
Theme: Organizations report various personnel for reviewing privacy compliance				
Legal advisors	Internal officers	Designated team	Government advisors	Point of Contact for Service
Theme: Compliance validation includes changes across a range of internal processes				
	Training	Policy Updates	Transparency	
Theme: Process desc.s include a reliance on external organizations rather than specific PETS for privacy compliance				
	AWS	Microsoft (365)	Norton	Credit card company

TABLE I

THIS TABLE PROVIDES AN OVERVIEW OF OUR THEMES AND SUB-THEMES THAT EMERGED DURING OUR ANALYSIS.

	PIPEDA	CPPA (C-27)	Tribunal Act (C-27)	AIDA (C-27)
Scope & Purpose	Federal privacy law for private-sector organizations in commercial activities	Proposed replacement for PIPEDA, modernizes privacy protections	Establishes tribunal for appeals and penalties under CPPA	First federal AI law; regulates "high-impact" AI systems
Key Features	Rules for collection, use, disclosure of personal information, requires meaningful consent, rights of access/correction	Clarifies "deidentified" and "anonymized" information, protection for minors, mandates privacy management programs	Provides specialized dispute resolution, Tribunal can impose fines up to $25M CAD or 5% of global revenue	Requires risk assessments, transparency, record-keeping; prohibits harmful AI practices
Status (2025)	In force since 2001, amended over time (2009)	Introduced 2022; not yet in force	Part of Bill C-27; not yet in force	Part of Bill C-27; not yet in force

TABLE II

SUMMARY OF CANADIAN PRIVACY AND AI REGULATIONS: PIPEDA (CURRENT LAW) AND PROPOSED REFORMS UNDER BILL C-27 (CPPA, TRIBUNAL ACT, AIDA)