Embedding Privacy by Design in The Lean Startup

An agile approach to privacy

Chris Willsher

June 2020

Foreword

This paper is a well thought out response to those who believe that privacy is a barrier to innovation – the exact opposite is true! It supports what I have been saying for some time now -- privacy breeds innovation and prosperity. Incorporating privacy early on in the design and development process, taking a user-centric approach to risk management and integrating privacy throughout the lifecycle of the personal information can provide a competitive advantage to any startup's agile development process. The paper demonstrates how Privacy by Design and The Lean Startup method can be integrated seamlessly. The value proposition is one that allows a base of trust right out of the gate, which steadily enhances the growth of customers and their loyalty.

Ann Cavoukian, Ph.D., LL.D. (Hon.), M.S.M.
Executive Director,
Global Privacy & Security by Design Centre

Acknowledgements

The author wishes to acknowledge and thank Michelle Chibba, Instructor, Ryerson University, Toronto, Canada for her guidance and feedback on this paper.

Cover photo by Matthew Henry/Unsplash

As new privacy regulations come into place, many organizations need to adapt to these requirements. Complying can be a challenge as they need to understand and adopt these approaches into the development of their products.

These challenges are especially acute for startup companies looking to establish innovative new products. Many of these organizations lack an understanding of privacy regulations or may simply view them as irrelevant (Chen et al. 2018). There are also views by entrepreneurs that privacy is an inhibitor to innovation and requires trading off features to ensure protection of data (Goldfarb & Tucker 2012). In addition, many current best practices for considering privacy as part of product development, such as privacy impact assessments (PIA), are lengthy and time-consuming (Oetzel & Spiekermann 2014).

These challenges run in opposition to many product development methods which are agile and iterative. Development cycles typically last a few weeks so versions of a product can be tested and validated with customers quickly. One such product development methodology is The Lean Startup, which uses a continuous cycle of Build-Measure-Learn to create and test versions of products in rapid succession (Ries 2011, p. 93). This method takes a proactive, customer-centric approach to the implementation of product design and development.

By shifting from a compliance approach to a more proactive one, startups can address data privacy issues more effectively. Privacy by Design, developed by Ann Cavoukian in the 1990s, is a method that actively embeds privacy into the development of technologies and business processes (Cavoukian et al. 2010). Seven principles comprise this approach (Cavoukian 2011):

1) Proactive not Reactive; Preventative not Remedial
2) Privacy as the Default Setting
3) Privacy Embedded into Design
4) Full Functionality – Positive-Sum, not Zero-Sum
5) End-to-End Security – Full Lifecycle Protection
6) Visibility and Transparency – Keep it Open
7) Respect for User Privacy – Keep it User-Centric

There are several common elements between The Lean Startup and Privacy by Design. Both view customers as being core to proper implementation of these methods. Both take a proactive approach to product development. And both are squarely focused on implementation. By exploring the common traits between these two approaches, an adaptation can allow for a more iterative approach to privacy that can better align with The Lean Startup's Build-Measure-Learn cycle.

Overview of The Lean Startup methodology

The Lean Startup is a product development methodology that was created by Eric Ries in response to what he saw as outdated development methods. Traditionally, product development followed a longer-term approach where products were conceptualized, built, developed and launched before ever being put in front of customers. In many instances this led to failure as assumptions were not validated along the way. The developed product did not fit a customer need and therefore

resulted in lost time and money for the organization (Ries 2011, p. 9).

Ries slowly developed the concepts around The Lean Startup to bring scientific methods into the practice of innovation. It was intended to provide entrepreneurs with a more efficient method of creating value and evidence has shown that following this method can achieve this goal (Frederikson & Brem 2017). Companies of all sizes, including GE and Dropbox, have utilized The Lean Startup methodology to help in the development of their products.

The Lean Startup method includes five principles (Ries 2011, p. 8-9):

1) Entrepreneurs are everywhere.
2) Entrepreneurship is management.
3) Validated Learning.
4) Build-Measure-Learn.
5) Innovation Accounting.

The first two principles set the groundwork that entrepreneurship can reside within any size organization and requires a new set of thinking to deal with the extreme uncertainties involved in innovation (Ries 2011, p. 8).

It is the last three that drive the product development engine. Build-Measure-Learn is the core part of the method that helps turn ideas into products (see Figure 1). This is an iterative process that is intended to develop a minimum viable product (MVP) in the shortest amount of time that can be tested with customers (Ries 2011, p. 93). Within The Lean Startup, the idea is to run through this loop as quickly as possible and constantly iterate on product design (Ries 2011, p. 228). The goal is not only to test product or technical questions but also validate fundamental business hypotheses. (Ries 2011, p. 94) This iterative process allows entrepreneurs to put customers at the centre of their decisions and reduce wasted efforts. The result is a more efficient development process that gets to a viable business faster.

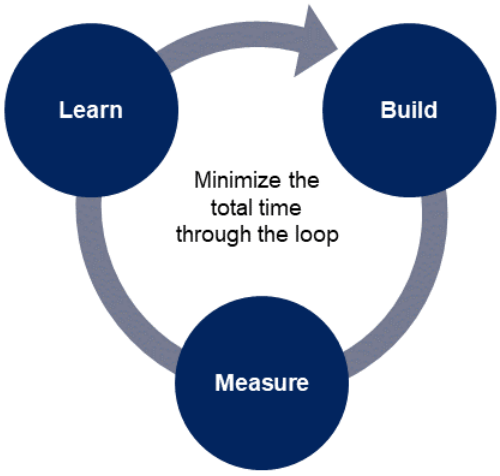

Figure 1: The Build-Measure-Learn process. Source: http://theleanstartup.com/principles

The Build phase focuses on developing the MVP with a minimum amount of time and effort but can be used to measure customer impact (Ries 2011, p. 77). This MVP will likely lack several features that may be essential later. The objective is to have a product that can be tested with a sample of customers to begin validating assumptions. This testing can be done with a subset of existing customers or with new customers that may have expressed interest in a potential solution to their challenges. The approach minimizes the potential risk of wasting time and resources building elements that may not be desired.

In the Measure phase, the goal is to identify the metrics and understand whether the product development is leading to real progress (Ries 2011, p. 77). The concept of Innovation Accounting falls within this phase which seeks to establish actionable

metrics that can help the startup measure progress and establish milestones for their work (Ries 2011, p. 9). This step is intended to bring a more scientific approach to the development of products by treating them as regimented experiments. By looking at how each iteration impacts the results, it allows startups to quickly learn what changes need to be made to create a viable product and business.

In the Learn step, entrepreneurs act on the information gathered through the previous stage. By evaluating results, entrepreneurs can then decide whether to persevere or pivot (Ries 2011, p. 77). In this step, startups need to determine whether they are achieving meaningful results to continue moving forward with their initial concept or adjust their direction based on the learning. This Learn phase is important as many entrepreneurs have difficulty recognizing when there is a need to pivot (Ries 2011, p. 161).

Highlighting Commonalities between The Lean Startup and Privacy by Design

There are several commonalities between the Lean Startup methodology and the principles of Privacy by Design. First, putting the customer at the centre of organizational decisions is critical in both concepts. One of the overarching objectives with Lean Startup is to ensure customer input drives product development (Ries 2011, p. 5). This correlates well to Privacy by Design, as principles six and seven require organizations to be transparent and respect the user within their privacy practices (Cavoukian 2011). In addition, within the European Union's General Data Protection Regulation (GDPR), which has incorporated the concept of Privacy by Design, seeking the views of data subjects is a key component within a Data Protection Impact Assessment (DPIA) (Article 29 Data Protection Working Party 2017). This correlation creates a good foundation on which to ensure agile product development not only provides customers with a valuable solution, but considers privacy in a respectful, transparent manner. Since privacy regulations focus on consumer privacy rights and interests, it will become critical for organizations to learn how to take this into account during product design.

Second, implementation is a central focus in both methodologies. The Lean Startup method focuses on the implementation mechanisms a startup should undertake to improve their chances of success. This is an important aspect in the product development lifecycle as it drives value creation (Talks at Google 2011). The implementation mechanisms are also a crucial factor for Privacy by Design (Cavoukian et al. 2010). This is in part captured within the third principle which requires privacy be embedded into the design of a product, not only from an IT perspective but also within business practices. Identifying how to blend the two concepts together from an implementation perspective can improve the chance of successfully developing a viable product for customers while ensuring privacy is holistically ingrained into the design of the product.

Third, both methods take a proactive approach to their specific discipline. For The Lean Startup, this proactivity comes through the iterative approach and active engagement of customers in the design process. As opposed to long development cycles, The Lean Startup allows entrepreneurs to quickly understand their customers and modify their design as needed. Within Privacy by Design, the first

principle indicates organizations need to proactively consider privacy (Cavoukian 2011). Taking privacy into account at the outset of product development allows organizations to minimize the risks in their data collection and processing practices. Being responsive to customer needs from both a product use and data processing perspective can help an organization thrive and create more meaningful customer engagement.

Challenges in considering privacy

For many entrepreneurs starting a new venture, the goal is to quickly create a viable product and begin generating revenue. This revenue can help fuel their growth through reinvestment back into the organization or can attract funding from external sources that can expedite their growth. To this end, many approaches to entrepreneurship, including The Lean Startup, promote that efforts should be focused on those things that are absolutely necessary to understand and deliver what a customer wants. Anything else is considered waste (Ries 2011, p. 49).

Unfortunately, as growth and demand for the collection of data has risen, privacy is an element that, in many cases, has been ignored. There are a few reasons for this. First, there is a lack of understanding of privacy regulations among entrepreneurs (Chen et al. 2018). Expertise in interpreting privacy regulations is often limited within startups due to their small size and limited resources. They often don't have the capacity to hire or seek out this expertise. So, they may choose to deprioritize privacy for the time being until they've developed their business to a stage where they deem this expertise is required.

There are also some entrepreneurs that question the relevance of privacy regulations and view them as outdated (Chen et al. 2018). And many look to companies such as Facebook and Google to help guide their own privacy practices (Chen et al. 2018). Again, this points to reasons why entrepreneurs may be deprioritizing privacy as they see the regulations, from their potentially limited viewpoint, running contrary to how these larger organizations are approaching the collection and use of personal data. If these organizations do not seem to be bound by the need for transparent, ethical data practices, then an entrepreneur may take the view that following privacy regulations is a competitive disadvantage. Startups may decide to take an approach of 'strategic non-compliance' as a means to circumvent regulatory commitments (Martin et al. 2019). However, given Facebook's long history of poor privacy practices (Ho 2018) organizations need to be cautious with this approach as increasingly large fines within privacy regulations could lead to a swift end to their business.

Adding to this, there is a notion that privacy is detrimental to innovation and can inhibit an organization's ability to grow. Privacy and innovation are still viewed by some as a zero-sum game where "privacy regulation should represent a trade-off between the benefits of data-based innovation and the harms caused by violations of consumer privacy" (Goldfarb & Tucker 2012). There are certain negative impacts that privacy can have on startups; in particular, entrepreneurial discouragement, product abandonment, and data minimization (Martin et al. 2019). Some entrepreneurs may feel that regulations prohibit them from executing their product vision in the manner they deem will be successful. This leads to either pivoting their idea into a new business model or abandoning the idea altogether. And the

minimization of data can lead to them being 'data-starved'. This can put them at a competitive disadvantage when looking to compete against much larger organizations with established customer bases that generate significant volumes of data.

Privacy impact assessments (PIA) are often viewed as a best practice tool to help assess and mitigate risk around personally identifiable data. It is often viewed that PIAs should be conducted at the outset and throughout the course of a project. However, the method for conducting a PIA can be lengthy and thorough (Oetzel & Spiekermann 2014) and for this reason they are typically done at a given moment instead of throughout the project lifecycle (Kroener et al. 2019). In an agile development process, the rapidly changing design requirements often make following a PIA process difficult and time consuming. In addition, entrepreneurs are often wary of traditional management practices out of fear it will add bureaucracy or stifle innovation (Ries 2011, p. 15). These factors make it challenging for startups to utilize existing privacy methodologies and practices to consider data protection in the development of their products.

That being said, the negative effects of privacy regulation are often viewed over the short-term as companies need to adapt to the new way of conducting business (Martin et al. 2019). Positive impacts may take time to appear in-market as organizations get through research and development of these new solutions. Organizations may also undertake compliance innovation to adjust their product design to make it more privacy-friendly by enhancing default privacy settings, using anonymized versus personally identifiable data, or embedding greater security into their systems (Martin et al. 2019). Compliance innovation could provide a market advantage for organizations by offering customers a more privacy-focused solution (Chen et al. 2018).

There is also a need to embed privacy into the company culture. Privacy norms need to be institutionalized in the companies that are developing innovative new solutions while collecting and using personally identifiable data (Waldman 2018). When looking at this organizations, it becomes difficult to embed these privacy norms across the company. Even in organizations that have a senior level executive dedicated to privacy there are challenges spreading directives to the practitioner level. Technologists and product managers often have a narrow view of privacy that covers notice on how data is used and security of data assets. And legal teams often take a compliance view to privacy. For startups, embedding privacy as a cultural norm early on can minimize the need to bolt it on as the company grows. And it can provide an advantage versus larger competitors that may not be able to quickly adjust to the continuously changing privacy environment (Waldman 2018).

Embedding Privacy by Design into The Lean Startup

Considering privacy within The Lean Startup methodology needs to allow for a more iterative and adaptable approach while still taking into account key privacy principles. This will enable product development teams to more easily integrate data protection into existing processes and ensure it minimizes any disruption in the product development flow.

Risk management frameworks can inform how privacy risks could be considered within The Lean Startup methodology. A privacy

risk management framework was developed in 2010 that takes Privacy by Design into account. This framework has five key steps organizations need to consider (Information and Privacy Commissioner of Ontario. 2010):

1) *Establish context*. This step requires an organization to consider the internal and external contexts which may impact privacy.
2) *Identify privacy risks*. Organizations need to identify where potential privacy risks may reside to be able to mitigate or eliminate them.
3) *Analyze and evaluate risks*. At this stage, it is important to evaluate the identified risks to ensure an organization directs resources appropriately based on the level of risk.
4) *Treat risks*. Organizations need to identify and implement the most appropriate methods for addressing these risks to eliminate or at least reduce the potential impact.
5) *Continuously monitor*. Continuous evaluation and monitoring of risks ensures the organization has and continues to effectively mitigate the identified privacy risks.

Throughout this process it is also important to maintain regular communication with stakeholders. This ensures there is constant awareness of potential issues and maintains a level of transparency around privacy practices both internally and externally.

The steps identified in the privacy risk management framework outlined above are consistent with other risk frameworks. A process designed for information system security, outlines five stages: identification, analysis, assessment, resolution and monitoring (Eloff et al. 1993). Again, it follows a similar flow of establishing an understanding of the context of the risks, then analyzing, assessing and resolving these risks accordingly. This framework also considers continuous monitoring to ensure risks remain under control.

The continuous monitoring and frequent communication outlined in the privacy risk management framework align well to The Lean Startup. The cyclical nature considered with continuous monitoring is in line with the iterative nature of the development process. And obtaining regular feedback from customers in The Lean Startup helps to ensure an organization is constantly understanding their customers' needs.

These steps can inform a framework to embed within The Lean Startup methodology that will allow for iterative consideration of privacy throughout this process (Figure 2). It will provide companies with a proactive method to build privacy into the design of products and improve transparency with customers.

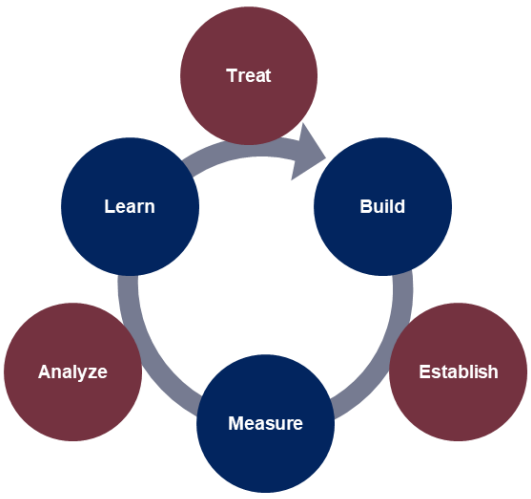

Figure 2: The Establish-Analyze-Treat process within Build-Measure-Learn

Three steps can be built into The Lean Startup methodology to address privacy risks

as part of the ongoing development cycle. These steps, Establish, Analyze, and Treat serve as complements to the Build, Measure, Learn cycle. The risk management framework can be broken down within these three areas to help company address their privacy challenges.

The Establish step considers the contexts in which personal data may be collected as part of the product development and begins identifying specific privacy concerns. This step would happen as part of the Build phase of The Lean Startup methodology. As an organization considers the product they wish to develop, they would begin to establish the context under which personal data may be collected and processed. This would include identifying the data needs and processes that are crucial to developing a successful product that will help entrepreneurs understand the flow of data. This can lead to a holistic view of the end-to-end data lifecycle and identify potential risk points.

Organizations should be gathering a number of pieces of information at this stage. This can be done by asking these questions:

- What external factors from a social, technical, regulatory, or competitive standpoint may impact our product and our consideration of privacy?
- What changes need to be made to our internal culture to ensure we are prepared to properly address privacy needs?
- What sources of data are being collected? What is personally identifiable?
- What is the intended use of data?
- What data processing, both manual and automated, is taking place?
- What business processes need personal information?
- What data may be an output from the solution?
- Where is the data being stored?
- Who will have access to the data?
- How long do we need to keep the data?
- What security risks are inherent in the process?

The goal at this stage is to build an understanding of how personal data plays a role within the context of the product. Doing so will allow the development team to proactively identify a flow of data within the product and serve as a starting point for the rest of the process. Thinking through and documenting this information at this stage will make it easier to consider and address potential impacts as the development moves through the iterative steps.

By considering the context upfront, it introduces an opportunity to quickly address or think thoroughly about how data is being processed. This proactive consideration could minimize any revisions needed later in the production cycle and free resources to work on other key elements of the product. Serious issues may be immediately identified at this stage and proactively addressed to reduce the risk of critical gaps before being released for customer review.

Using an example of a company developing a smart doorbell product, the organization would need to consider the data being collected from their customers. They may require personally identifiable information from customers to set up their account. This would likely include name, address, email address, and possibly credit card information if there is an ongoing monthly service fee. Much of this information would

be captured in their customer databases, in their financial systems and from an IT perspective to allow their customers to access their account information. Many considerations around how and where this data is used would need to be considered and ensure customers are aware of and consent to these potential uses.

When cycling through the process, the overall context may not change. However, it is important to at least consider if any of the context has changed based on outcomes from the previous iterative cycle. This helps ensure you consider any aspects that may need to be revised to minimize the risk of missing items that may impact privacy.

The second step in the iterative risk management process, Analyze, requires the organization to consider the extent of the potential risks. This would be integrated within the Measure phase, as organizations begin to assess, at a more granular level, where the privacy risks are in the product. As products are released, the organization will begin to get a sense of how customers are using it and will be able to see real-time flow of data. By reviewing this process, they can get a better sense of other potential risks or parts of the user experience that may not be effective. The product developers can consider how these could be altered and improved to enhance privacy features.

During the Analyze phase, the organization can assess potential risk points and gain an understanding of how customers may feel about processing of data as part of the overall product. Questions can be posed to identify if the customer is comfortable with collection and use of their personal data. The customer can also identify whether they understand data use which can improve the organization's transparency. An opportunity resides in this process to test different consent mechanisms to find viable solutions that will enhance the transparency of the organization's data practices. This valuable insight will lead to improved privacy practices and further embed strong data protection efforts into the organization's product design.

The organization should consider the following questions as part this phase of the development cycle:

- Where are the potential risks?
- What is the extent of the risk (high, medium, low)?
- What would be the extent of the consequences?
- How do customers feel about use of data?
- Do customers understand how we intend to use personal data?
- How is data actually flowing through the system?
- Is there other data being collected we didn't anticipate?

Within this stage, organizations should consider developing actionable metrics around aspects of their privacy initiatives where possible. An example may be the percentage of users that provide consent to have their data used within the product. This could provide the organization with a sense of how well they are conveying use and their ability to quickly attain a customer's trust. Measurements such as this could have long-term impacts on the viability of the business and again provide them with a competitive advantage.

Looking at the development of a smart doorbell, the entrepreneur may want to understand the level to which information is being collected and processed. They may test

different mechanisms for obtaining consent to understand the impact on customers' understanding of the potential use of data. In addition, they can compare this to the impacts this has on customer engagement. By viewing these tests from both sides, the organization can understand how to ensure they are enhancing privacy while also optimizing customer acquisition and creating a positive-sum solution.

The final step, Treat, would happen in conjunction with the Learn phase of The Lean Startup. Here the organization would turn to treating any risks identified during this cycle. Having seen actual customer use, it will help the organization better understand the extent to which the risks may play out. And it will allow them to begin to fix these issues early on.

Organizations can consider the following questions during this phase of the development cycle:

- What changes need to be made to improve privacy?
- Can we minimize the data being collected?
- Can we anonymize data?
- Are there other solutions that could be implemented to reduce risks?
- What privacy enhancing technologies could help mitigate the risks?
- Do we need to consider compliance innovation to address privacy risks?

During this stage, organizations consider whether to persevere with their innovative product or pivot based on the learning. These considerations would also hold true for their privacy efforts. They need to consider whether the privacy efforts they have in place are sufficient or whether there are improvements that could be made. This may require them to pivot on certain elements where privacy risks may have appeared that were not previously identified.

Using the smart doorbell example, in testing the product, the organization may quickly realize the product is inadvertently capturing images of people walking along the sidewalk and storing these in a database. Given these individuals may be unaware their image is being collected and stored, it will require the organization to identify potential solutions to address this challenge. It may require alterations to the camera to shorten the field of focus. Or they may need to provide customers with mechanisms to notify those passing by to be aware surveillance technology is in place. And the company would need to consider encryption technology that prevents their customers from accessing and using these images in any manner unless warranted for legal purposes. By adding a privacy perspective to the iterative product development lifecycle, it can help an organization address these risks early on before their product reaches wide-spread adoption.

The Establish-Analyze-Treat steps would be repeated as iterative cycles alongside Build-Measure-Learn. By taking this approach, it will allow an entrepreneur to consider privacy impacts to any changes they make to their design. This is especially critical for any pivots as this can result in some significant changes to the direction. These could have privacy impacts, that if not considered, could result in the company releasing a product that has inherent risks. If in developing the smart doorbell, the company identified there was a better market for the product as an industrial security tool this may change their privacy requirements. Identifying and addressing these changes during a pivot

allows the company to continuously embed privacy in a proactive manner.

By considering the Establish-Analyze-Treat process within the Build-Measure-Learn product development cycle, organizations can optimize product design while also considering privacy. It provides a proactive, customer-centric approach that embeds privacy into the design of the product. It improves transparency by actively obtaining customer feedback on privacy practices throughout the development lifecycle. And the process allows an organization to holistically consider end-to-end security and a positive-sum approach to their innovation efforts.

For this process to be successful, the organization needs to embrace a culture of privacy protection. The entrepreneur or senior management need to instill this as a practice that encompasses every facet of the organization. Thinking through how personal data is used across the company and ensuring employees recognize the importance is critical. Considering privacy early on can reduce the potential for privacy pitfalls and negative outcomes for an organization (Cavoukian et al. 2010). Embedding privacy into the organization's culture and empowering employees to identify risks can be a way to reduce the potential for disastrous consequences in the future.

This is key for those at the practitioner level as they are often making decisions that impact the collection and use of data. Ensuring they understand the importance of privacy to the organization and arming them with the information they need to make proper choices will help improve the efficiency at which an organization can embed privacy in an iterative design process. Establishing this cultural mindset will help to ensure privacy remains front-of-mind for all employees. This will allow them to consider aspects of privacy in their work and reduce the risk of making decisions detrimental to the organization.

There will be a need for a base level understanding on privacy concepts. While this process can help address the potential risks and identify areas where personal data is being processed, there is still a need to understand what is deemed personally identifiable information or areas of potential consideration for privacy risks. Continued education through various means will be required for privacy to be proactively considered by entrepreneurs and senior leaders. This can come through embedding privacy within post-secondary education, resources through local privacy offices (such as the Office of the Privacy Commissioner of Canada), and through startup accelerators.

Information about privacy also needs to be communicated within an organization. As part of embedding a culture of data privacy, organizations should consider an aspect of their onboarding process to communicate key elements of privacy. This will help to ensure employees are familiar with what is considered personal data and how the organization manages it. Improved literacy around data protection can ensure they are better equipped to identify areas of risk. Again, this can reduce the potential for negative consequences from areas where poor decisions were made.

The process is not without its limitations. Depending on the extent to which an organization tests its product with customers, opportunities for negative consequences from a privacy perspective may still be inherent during these tests. It

does not eliminate all these risks at the outset of product development. It does however ensure that privacy is considered throughout the lifecycle especially as changes are contemplated for the product. This is important as it can still minimize the impact by addressing these risks proactively before a product is in the hands of a large number of customers.

The Establish-Analyze-Treat process does not replace a proper PIA. There may still be a need to conduct a more thorough review of a product prior to a full-scale market launch to further minimize the potential for privacy risks. Conducting this review can also help the company by having full documentation of their privacy review which allows them to show their due diligence in considering privacy. This is helpful in the event an issue does arise as it allows them to prove the efforts they've undertaken to minimize risks which could reduce potential consequences from government privacy officers. However, the Establish-Analyze-Treat process can help reduce the efforts required to conduct a full PIA.

Conclusion

The use of the Establish-Analyze-Treat method for assessing risk can complement The Lean Startup's Build-Measure-Learn product development lifecycle. It offers a way for entrepreneurs to proactively consider privacy within innovation in a transparent, user-centric manner. And it can aid in developing a stronger product. The enhanced process can bring a more iterative approach to privacy that aligns with the rapid development cycles often used in today's technology departments. Rather than privacy being viewed as an inhibitor to innovation and slowing the process down, it can work in conjunction with rapid design to create a positive-sum approach.

Entrepreneurs adopting this method can enhance their ability to create a competitive advantage for their organization. The ability for startups to be nimbler in their approach, as compared to larger competitors, can allow them to integrate and adapt privacy-centric approaches more efficiently. Compliance innovation will likely become increasingly important as customers become more wary of data use.

And innovation needs to come into the methodologies for implementing privacy practices within organizations. Continuing to explore how we can effectively adapt the principles of Privacy by Design within product development will be essential. Without this consideration, zero-sum views of having to choose between privacy and innovation will continue to flourish. Entrepreneurs often need to quickly adapt their product design to meet customer needs. Creating methods that allow for more conscious consideration of privacy that complements instead of impedes progress will be critical to wider adoption of privacy practices.

References

Article 29 Data Protection Working Party. (2017). Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. Retrieved from https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

Cavoukian, A. (2011). The 7 foundational principles: implementation and mapping of Fair Information Practices. Toronto, ON:

Information and Privacy Commissioner of Ontario.

Cavoukian, A., Taylor, S. & Abrams, M.E. (2010). Privacy by Design: essential for organizational accountability and strong business practices. *IDIS*. **3**: 405–413.

Chen, W., Huang, G., Miller, J., Lee, K., Mauro, D., Stephens, B. & Li, X. (2018). "As we grow, it will become a priority": American mobile start-ups' privacy practices. *American Behavioral Scientist*. **62**(10): 1338-1355.

Eloff, J.H.P, Labuschagne, L. & Badenhorst, K.P. (1993). A comparative framework for risk analysis methods. *Computers & Security*. **12**(6): 597-603.

Frederiksen, D. & Brem, A. (2017). How do entrepreneurs think they create value? A scientific reflection of Eric Ries' Lean Startup approach. *International Entrepreneurship and Management Journal*. **13**: 169–189.

Goldfarb, A. & Tucker, C. (2012). Privacy and Innovation. *Innovation Policy and the Economy*.**12**: 65-89.

Ho, V. (2018, December 15). Facebook's privacy problems: a roundup. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/dec/14/facebook-privacy-problems-roundup

Information and Privacy Commissioner of Ontario. (2010). Privacy risk management: building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default. Retrieved from: https://www.ipc.on.ca/wp-content/uploads/2010/04/Privacy-Risk-Management-Building-privacy-protection-into-a-Risk-Management-Framework-to-ensure-that-privacy-risks-are-managed.pdf

Kroener, I., Barnard-Wills, D. & Muraszkiewicz, J. (2019). Agile ethics: an iterative and flexible approach to assessing ethical, legal and social issues in the agile development of crisis management information systems. *Ethics and Information Technology*. Retrieved from https://doi.org/10.1007/s10676-019-09501-6

Martin, N., Matt, C., Niebel, C. & Blind, K. (2019). How data protection regulation affects startup innovation. *Information Systems Frontiers*. **21**: 1307-1324.

Oetzel, M. & Spiekermann, S. (2014). A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems*. **23**(2): 126-150.

Ries, E. (2011). The lean startup: How today's entrepreneurs use continuous innovation to create radically successful businesses. New York, NY: Crown Business.

Talks at Google. (2011). *Eric Ries: The lean startup*. Available from https://www.youtube.com/watch?v=fEvKo90qBns

Waldman, A. (2018). Designing without privacy. *Houston Law Review*. **55**(3): 659-728.