Privacy

Applied. Proactive. Innovative

By the Privacy & Security Innovators Circle

"

Privacy is too important to be left to checkboxes.

Priyadarshi [PD] Prasad, Co-founder & Chief Product Officer at LightBeam.ai

Editor:	Jutta Williams
Cover & Diagrams:	Niramayee Sarpotdar
Initiative by:	Privacy & Security Innovators Circle (Join us on LinkedIn)
Published by:	LightBeam.ai Inc. www.lightbeam.ai

Privacy : Applied . Proactive . Innovative

LightBeam.ai

Contents

Section : Applied

Section : Proactive

Section : Innovative

Foreword

Jutta Williams
Editor

I was nervously waiting in the company cafe for my engineering director to join me for a "quick chat." You know the kind I'm talking about - a precursor to unwanted but sometimes needed escalations. I had been beating my head against a wall all week on the topic of data storage and handling requirements for 3rd party labeling of sensitive data sets.

I had tried everything: educating the engineers about the law, explaining the data transfer policies for our company, and demonstrating that our vendor policies had to be followed for our compliance certifications to be valid. None of it was achieving the needed change.

We sat together drinking coffee for some time while we discussed his work, mine, and the outcomes we together needed to achieve. "What they are asking for is impossible. You understand technology, so just explain that to the lawyers." "Yes," I replied. "But, what they're asking for is not what you think. The words mean something different in the regulatory context. Let me explain."

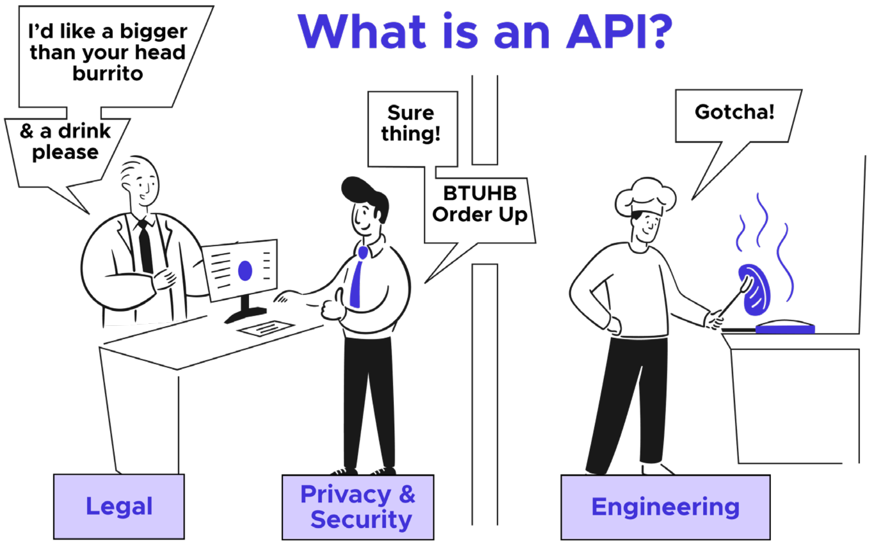
We examined the existing workflow, identifying where regulation kicked in, how we documented our security and privacy practices and together we built a crosswalk between administrative policies and technical controls that enforced data protection on the platform. "I can explain this to my engineers. Can you explain this to our legal team and to regulators? I need you to be my privacy API," he concluded.

For those not familiar with the term, an Application Programming Interface is a software intermediary that allows two applications that don't speak the same language to communicate and I cannot think of a more apt way to explain the role of a privacy professional.

The law isn't as clearly defined as "this is what you must achieve" or "this is an unacceptable outcome." In fact, all current privacy frameworks are risk based. This means we get to choose what is a reasonable and appropriate outcome based on an assessment of our size, complexity, and potential for harm to data subjects.

My engineers (generally) do not want to know and understand regulations. My attorneys (generally) do not wish to learn and understand the technical nuances of how data is safeguarded, or optimally used to deliver products and services. Both use a language that is foreign to the other and the best service I can provide is as a translator.

There are many of us called to operate in this middle zone that could benefit from a dedicated community where we discuss common



challenges and share solutions. This book and the PSI Circle Community is where we can have really frank and open discussions about privacy topics that are Applied, Proactive, and Innovative. This group is where we can discuss defensibility and appropriateness and ask one another questions about scale and automation.

This is the first of hopefully several volumes where privacy veterans can share expertise and learning that have made them better translators and program leaders. The authors and I hope you enjoy this first compilation and the podcasts where we explore more with each contributor.

Consider also contributing to the community discussion, or writing a chapter in our next edition! Some topics we hope to tackle in our next volume include:

- What does it take to operate privacy programs on a day-to-day basis?
- How is a DPIA, PIA, Tech / Product Spec, Privacy Review, or Privacy Policy different?
- What's on your roadmap this quarter / half / year?
- How to tackle technology integration challenges in complex data structures
- What does future-proofing mean for emerging technologies
- How do we identify dark design and dark patterns
- What are your KPIs?
- How should the law be more informed about technology?
- How do we make, document and defend tradeoff decisions?enjoy this first compilation and the podcasts where we explore more with each contributor.

Thank you,
Jutta Williams
September 2022

Chapter 01.

Section : Applied

Privacy and Customer Trust

Mark Chang (LinkedIn)

Mark Chang is the Senior Corporate Counsel, Privacy Compliance at SHEIN in Los Angeles, California. Prior to SHEIN, Mark has served as the Director of Risk, Compliance, & Privacy at the Florida State University in the Information Security and Privacy Office. Mark has also worked at Goldman Sachs in the Technology Risk Regulatory, Policy, & Strategy team of the Engineering Division. Mark obtained his Master of Business Administration in Information Technology Management from the University of Texas at Dallas, Juris Doctor from Western Michigan University, and Bachelor of Arts in Economics from the University of Tennessee, Knoxville. Mark is a Certified Information Privacy Professional, Europe (CIPP/E).

The data privacy / data security challenge(s)

The relationship between Privacy and Customer trust will continue to be the center of discussion in the boardroom and managers' operations. This is certainly not an article that gives yet another checklist for audit purposes. Let's brainstorm the best practice and approach that may be helpful to your data privacy trust management journey.

The growing challenge of Data privacy and Security come from all directions, including, but not limited to, technical, financial, corporate, legal, human resources, and cultural expectations. Hacker and data breach news are reaching new stress levels with the complexity and impact to not just the organization operations but also institutional trust. Regulators from global, national, and local levels are actively tightening the requirements and oversights on the legal baseline on how businesses should handle the data in the specific jurisdictions which may or may not be similar to others. Competitors are attracting the talented team members you develop with lucrative compensation packages when you are constrained with a fixed budget for the calendar year. The key corporate stakeholders finally seem to understand the importance of Data Privacy and protection and find the budget you need before the runaway Covid era, not so transitory, inflation rate. The customer expectation changes with the new ways that market leaders use to handle their data. The endless training sessions always seem to play catch up on something that can 'easily' be mitigated. If any of the above situations sound familiar to you, the data privacy and information security practitioners, you are not alone.

Why are Privacy and Trust important?

The importance of Data Privacy is to protect the Data Privacy trust! Companies rely more and more heavily on customer data for purposes of various legal, business, and technical reasons. It is fair to say that many business models rely so heavily on the customer data that they will not be able continue their operation when consumer data disruption occurs. Consumers, especially after the Covid pandemic, have started paying more attention to how their data is collected and expect companies to do a reasonable job protecting the data.

Industry leading technology companies, such as Apple, Alphabet, and Microsoft, form a narrative of consumer data privacy priority and spend a significant amount of resources on both data privacy and security. In general, these companies are taking an active approach to manage the expectation of consumer trust. US President Ronald Reagan learned from Suzanne Massie, an American scholar, and coined the phrase "Trust, but verify." Consumers of today are definitely seeing more and more companies with industry leading security certifications on their marketing materials. As a result, the expectation of the people is also growing with the 'standard' of industries and business practices. This is not to say companies with certain data privacy and security certifications are perfect in their Data Privacy and Security practices and immune from data breaches. On the contrary, the certifications mostly provide a snapshot of how the companies handle certain aspects of the regulatory requirements at a specified time frame with specific presumptions. These certifications may even provide insights of the company data privacy and security maturity level which attract some unwanted attention from hackers.

Is the data breach that comes with proper data protection certification(s) excused from the breach of customer trust of how companies handle their data? Probably not. Is consumer trust impacted just because the company meets all the regulatory requirements of data privacy and security? Very likely. While there are no perfect answers for each unique situation, maybe the goal of Data Privacy and Security is not to perfect data privacy trust but to exceed regulatory requirements and manage the customer expectation of trust.

The regulatory scrutiny varies in different industries. Hackers seem to value financial and health data the most as demonstrated in their high black market prices. Regulations in these related industries are also the most proactive ones. General Data Protection Regulation (GDPR) has handed out heavy fines to major international technology companies since it became effective in 2018. The regulatory fines may or may have not lowered the consumer trust level in companies receiving these heavy enforcement efforts. Companies that have battled publicly with government agencies on their efforts in both Data Privacy and Security are proactively enhancing their overall data management efforts. These efforts are also impacting how many competitors in similar industries are conducting their data privacy and security practices. Some may argue that these high profiled efforts demonstrate how these companies have invested in data privacy and security protection to minimize future risks.

The Privacy and Trust practices

In the world of Data Privacy and security practice, the most successful recipe is to have a team of cross functional talents. These talents do not need to be individuals who are extraordinary subject matter experts. They can be the point of the contacts to the team of special areas such as legal, human resource, procurement, technology, compliance, marketing, etc. Each silos of organization have their perspectives and needs that impact the overall data privacy and security management. No single checklist nor individuals can address the issue of data privacy trust because expectation of the customers and regulators is not the same as the daily operation and management of data management.

The data management strategy, policy, and training may take a bit longer to process and complete. In fact, you have already had way too many meetings before the meeting in this cross functional effort. During this process, you and your teams are overwhelmed and short in resources while addressing views and opinions coming from all angles. Often, meetings end up in gridlocks or analysis paralysis. Feel free to break from the traditional waterfall project management methodology and adopt the popular, tech friendly, agile approach. The goal is to move the ball forward to tackle this grand effort of privacy trust because not doing anything is not an option. Each time the cross functional team secures a small win, the organization inches toward a better privacy trust posture.

You may recall that famous hiking joke where two hikers encounter a bear when one stoops to tie his shoes to plan his attempt to outrun his counterpart to survive. This is a natural part of business competition when one company only needs to outrun competitors except that there are more than one bear when it comes to consumer trust. The goal post of data privacy trust is a moving target as consumers learn how technology integrates into their daily lives. Millennials (born between 1981-1996) grew up listening to parents not to stay in strangers' houses or ride in strangers' vehicles. With the business model of Uber and Airbnb, societies have changed the expectation of data privacy trust in the last 10-15 years. How companies should establish, maintain, and adapt the privacy and consumer trust programs is the key cornerstone of business model. Having the proper financial resources to support the business needs is important. However, truly understanding the important 'why' on purchasing a key technology solution goes behind the how and what. The cross functional team should serve as the guardian of data privacy trust for the consumers.

> **"A proactive approach to balance managerial, legal, and technical needs should empower a company to turn data privacy and protection compliance into a business advantage to maintain the business reputation and trust."**

Best practice tips

The probability of more regulations in the Data Privacy and Security globally is going higher. Meeting the regulatory expectation passively may ensure the company operates within the industry standard. However, a proactive approach to balance managerial, legal, and technical needs should empower a company to turn data privacy and protection compliance into a business advantage to maintain the business reputation and trust. As a privacy, security, and/or legal professional, our job is to guide the business to effectively manage risks arising out of our areas of specialty.

The world leading Electric Vehicle maker, Tesla, recently thwarted a one million dollar insider threat. This example demonstrates how a proactive approach creates business advantage of data protection because you are only as strong as your weakest link. If this Tesla employee was compromised in giving the hacker the company trade secrets in security practice, IT system, and business practice, the consequence to Tesla's data privacy trust management could be devastating.

If you are reading this article, welcome to the class of Data Privacy Trust management. Regardless of your professional backgrounds or specialities, we are all students of this cross function by design practice. The regulatory standards and landscape are changing. The businesses using valuable consumer data are also changing. Feel free to collaborate and share the best practice you learn through this journey as we collectively move the data privacy management towards the level of trust that benefits all stakeholders involved.

Chapter 02.

Jutta Williams (LinkedIn)

Jutta Williams is an independent Privacy/Responsible AI consultant and startup board advisor. She was the inaugural Chairperson and Head of the US delegation to ISO for AI Standards. Jutta graduated with highest distinction from Carnegie Mellon University earning a MS in Information Security, Policy and Management. The former Head of Privacy at Bolt, an e-commerce platform, she was also product lead for ML Ethics and Responsible ML at Twitter and led privacy remediation work streams for Facebook's central privacy org. At Google, Jutta led data protection efforts for the Medical AI team (later launched publicly as Google Health) and supported Engineering Compliance for Alphabet. In her early career, Jutta served as a Security Engineer and Product Manager for DoD and was the Chief Privacy, Security and Compliance Officer for two large integrated healthcare companies.

Section : Applied

Architecting a New Privacy Program

Building a privacy program is a lot like building a house. Form and function vary based on many factors including climate, available building materials, geography, and budget. Some homes - and privacy programs - are built to meet basic needs for shelter and safety. Others are designed to garner esteem or earn prestige.

Privacy program architects seek to establish an internal standard of practice (ceiling) that exceeds the regulatory minimums (floor) of applicable law. Perimeters (walls) separate internal and external environments and we secure access points (doors) with mechanisms appropriate to the value of goods within. After all, a padlock for the garden shed may be appropriate but is probably inadequate for your main entrance.

As the architect for a new privacy org, breaking ground on a new program can be daunting - particularly when regulatory guidance is evolving and there seem to be more stories of failure than of success from which to draw inspiration.

Building safety is a fairly recent regulatory concern just as data collection and use was not always a consideration in the early days of the internet.   In the 1850's many metropolitan cities began to codify and enforce building codes. But, much like the privacy regulatory landscape, construction requirements still vary widely, overlap, and occasionally contradict one another.

So why are large-scale building failures more rare than data breaches? Applied physics helped builders understand tension, harmonic vibrations and oscillations, tensile strength, and elasticity to build safer, bigger and more beautiful buildings independent of government initiatives toward more comprehensive, universal building codes.

Similarly, successful operational privacy programs and applied privacy engineering practices help build safer operations within large scale data programs and may even delight your customers or differentiate you in your market.

It's not recommended that home builders or privacy program owners conflate the goals of compliance and safety. A well designed building plan - for a home or a privacy program - should enjoy compliance as a byproduct of delivering a safely built home or program.

So how might new privacy managers approach their first year when building a safety-oriented program that also happens to be compliant?

First, Know Your Purpose

Is data important to your business? If so, privacy should not be considered a cost center - designed well, it can be a revenue and business enabler. Privacy done well results in better organizational agility, more innovation, operational streamlining and efficiency, and in some industries, a competitive advantage. In addition to fewer and less costly data breaches that measurably translate into consumer trust and good will.

These enablement outcomes should be the primary motivation for building a right-sized privacy program for your organization and sharing these goals should be broadcast broadly.

Yes, there is a compliance mandate and oversight accountability for many privacy program managers. In most countries, the accountable executive for regulatory compliance of all types is the CEO, who can be held personally responsible for penalties or held criminally or civilly liable for violations - even without direct knowledge of illegal or non-compliant activities.

To mitigate this personal liability, CEOs empower an authority who is accountable and held responsible to effectively (more on this later) manage and enforce compliance. This would be you or your leader for privacy; the HR official for employment laws, CISO for information security regulation, or CFO for finance law, etc. (the titles/roles may vary for your business). These oversight functional leaders serve a critical role in protecting the business and the CEO, which is why asking for support, be it headcount, budget, authority, or collaboration, is something a privacy org leader should not fear.

Second, Understand the Lay of the Land

Every new home build starts with a survey which identifies the environmental conditions that may enhance a home's ROI or which may limit available choices. A new privacy program developer begins similarly by asking ourselves a few important questions.

01. What is in scope for this program? Is it supporting a team, an organization, or a company? Will this grow and when?

Answering this question can help you understand the square footage equivalent of what you need to build. Over- or under-investment in people, process or technology can both lead to a failure state, so establishing expectations with leadership and with your organizational counterparts early helps ensure that expectations and investments are right-sized for the problems you're looking to solve.

Just as with a house that is too big or too small for the people that need to live there, privacy program managers will be held accountable if maintenance costs are deemed excessive and/or people do not get support within agreed upon service levels (SLAs).

02. Will you build toward a decentralized, standardized or centralized program?

Are you building a 5-unit condominium, a 10 room hotel or a large single family home? All might support the same number of residents but each has its own costs and benefits.

Diverse portfolios or geographically distributed organizations may embrace decentralized (locally governed) privacy programs because they allow each unit (e.g., product area, hospital region, department store) to adopt best practices that are tailored for their environment, customer demographics, or data protection needs.

Other companies may be most comfortable establishing a baseline of practice - a standardized approach to privacy - and then allowing segments of the company to improve on (work towards a ceiling) but not dip below (the floor of) that privacy minimum. This is often the case in more regulated (e.g., finance, health or utility) firms or those which have been penalized and have specific compliance remediation reporting obligations.

Some companies prefer to operate all privacy functions from a single, centralized organization to ensure uniform application and consistent outcomes. Centralization is often necessary when a company seeks to automate or optimize core functions using enterprise software or tooling. This approach is often selected by companies that are very small where there may only be a handful of people working on the topic or very large where automation and optimization is required for scaling consistent results.

Rather like building a kitchen in each of the units in a condominium complex, a set menu for your hotel guests, or family-style dining in a house, your program should be structured to serve the needs of your diverse, and hungry to learn employees.

03. What are your team / organization / company norms for new programs?

If you've ever lived in a neighborhood with a Homeowners Association, it's critical to understand what is acceptable within the bylaws and conversely what triggers the wrath of the HOA before you choose a house plan. It's much cheaper and easier to pick an approved color for your shutters ahead of the build than to repaint them after the fact.

Similarly, if you've been asked to build a new privacy program, it behooves one to write a mission statement, charter, and roadmap; then, seek stakeholder buy-in, garner requisite approvals, and secure budget, before breaking ground on your new build.

A couple of topics to research before you get started planning might include:

- How do policies get approved?
- Is there a learning management system and if so, how do other required education classes get assigned?
- Is there an internal marketing team that needs to review/approve company-wide communications?
- What is the company stance on and/or process if you need to buy software, hire a consultant?
- What is the process to post a new JD?
- How is hosted/on premises software approved for purchase?

Third, Find Stakeholders, Allies and Friends

They say good fences make good neighbors. It's not recommended that program owners build walls between organizations, but defining property lines and paying attention to how your program interacts with adjacent functions helps build strong alignment and eases integration.

A rule of thumb to keep in mind is that it is unlikely that privacy has been ignored by your team/org/company prior to your program being chartered. Functions may be distributed, performed in an ad hoc way or may be effectively performed under a different name. Some of these functions may be readily handed over and others may not be too excited to give up roles they have been performing.

Finding and inviting input from across the organization helps to establish your stakeholder, allies, friends and potential points of friction early. To this end, the executive sponsor(s) for your privacy program should be able to share which stakeholders should be consulted and informed to ensure there is understanding (if not always acceptance) of the mission you are undertaking.

Within the scope of our roles and functions, it's important to recognize where we need to honor organizational easements - places where we have to compromise on ownership to ensure that other organizations can do their work effectively. For example, joint decision making is frequently shared with legal counsel on the topics of privacy notices and cookie compliance and neither are likely to make operational decisions independently.

Adjacent functions like information security and data management are also great alliances to invest in early - especially if a privacy engineering function is part of your program charter. There can be a lot of confusion about security vs. privacy within IT organizations and where data governance policies are set since approaches to managing data risks are similar between these disciplines.

Keep in mind how responsibilities and accountabilities may be operationally split between privacy and other organizations. For example, perhaps risk assessments for 3rd party data transfer at contract initiation is part of a vendor management organization's charter, but Privacy may be responsible to monitor that only specific types and sources of data are shared once the contract is signed. Discussing what part of that approval and monitoring process is within which charter and when handoffs/ communication occurs early - before toes get stepped on - is key to making and keeping friends.

Using a RACI template can help with these conversations. Many conflicts can be avoided by clarifying what responsible, accountable, and consulted mean relative to a function, as well as to ensure who expects to be informed.

Another way that program managers can identify opportunities to make friends is to suggest an async retrospective on privacy topics where teams can anonymously submit feedback about what they liked, learned, longed-for and lacked.

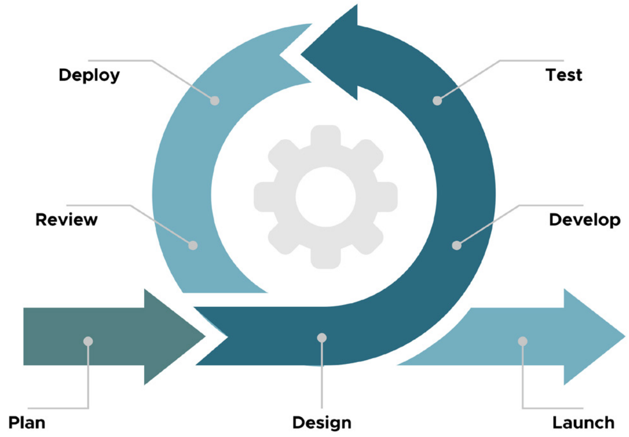
Fourth, Design for Success

If you build before you design and things go poorly, it will be expensive to fix and recovery is unlikely without throwing away a lot of work, money and credibility. If I change my mind and decide that I want a gas fireplace on my deck after they've already bricked my new home, it will cost a lot more to make that change now than while drawing up a blueprint.

Many practitioners find themselves inventing (and reinventing) their programs as issues emerge or in response to the myriad of laws, enforcement actions and peer publications that reveal new requirements or approaches. In software development, developing solutions that grow or improve on a previous version of a product is called "Agile" development. Applying a design and development framework to guide privacy work helps with consistency and demonstration of a continuous improvement posture - both of which are expected of compliance programs.

For some industries like internet based businesses, this type of iterative or agile approach to design is understood and experimentation is an expected part of the growth process. For others - especially those that are highly regulated as in health and finance, the rationale for iteration and continuous change might need more communication and socialization.

Agile Methodology



Designing a new program or a change to existing capabilities should follow the following 6 step agile process:

01. Collect Requirements : At its simplest, a requirement is a service, function or feature that a user needs. Privacy requirements can be functions, constraints, business rules, data types, infrastructure demands or other operational needs that must be considered before a privacy control or process change were defined. Broad reach and collection of requirements helps make friends and informs great designs.

02. Design : This is the longest stage of your program development sprint. Not all requirements can be fulfilled in the design of your privacy program or data protection plans. Validating the “must have” and “nice to have” will help you scope the development work ahead and creates a backlog of projects that you can consider in later phases (sprints) of your program work. Identifying policies, technical controls and human reviews that meet minimally viable (regulatory/legal floor) plus a few features that help raise the bar for being a good data steward.

03. Development : Write the policies, build the education modules, launch the Privacy Impact Assessment (PIA) templates, build the websites, assign the privacy review tickets, build the deletion pipeline integrations… the list goes on but work is informed by the design work and requirements so the number of meetings, consults and rework will be minimized!

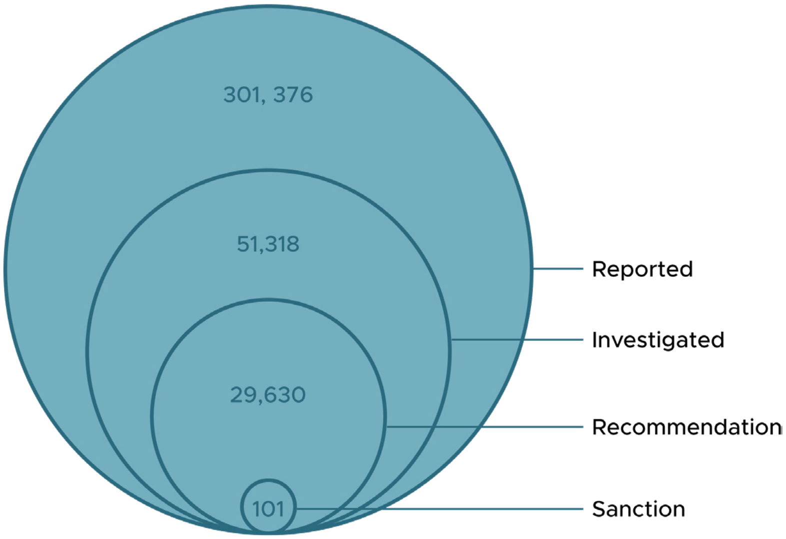
04. Testing : Yay - Development went smoothly and your stakeholders are happy with the first iteration of the program. But before it’s socialized as a new company norm, it has to go through quality assurance. The agile privacy program leader tests the change with a friendly team and your most resistant teams to ensure functionality and an acceptable friction level.

05. Deployment : Found and resolved some issues and now we're confident that the new process or technical control is ready for the rest of the team/org/company to use. Kick off here may be a company-wide announcement, assignment of mandatory training, turning on the data pipeline etc.

06. Assess & Improve : Later we talk about monitoring as a requirement for sticky programs. All great Agile projects spend a bit of time after deployment ensuring that customers are happy with the change. Post deployment surveys or retro meetings to discuss the process used to deliver the new privacy program requirement are great at identifying what to add to your next project(s).

Fifth, Selling Broad Commitment to Privacy

Now that you have a plan and a design that you know will work, how do you gain broad commitment to execute on your design? A new home construction loan requires proof that you have all the permits, design, land, and knowledge to not only build the house but to maintain a safe dwelling and meet your commitments to your bank.



HIPAA Enforcement by numbers

Lacking a credit - or maybe a "credibility' - score for privacy at this early stage that will secure your team/org/company's commitment to change, we have to fall back on marketing the imperative for change. Which of these two statements gained an employee's commitment to a data integrity improvement we were implementing?

"Did you know that HIPAA violations can result in a corporate fine of upto $1.5M and personal liability of up to $250,000 or 6 years in prison?" or "I spoke with the family of a veteran who was unable to qualify for hospice care because we admitted another patient under the wrong SSN and the VA system already listed him as deceased."

The first uses Fear, Uncertainty and Doubt (FUD) in relation to corporate or personal risk to gain commitment to sell the change. It may get peoples' attention up front but it often results in short-lived attention that may even turn to resentment when employees and leaders realize that the likelihood of incurring those risks is actually very low. The second describes a realized risk where something the employee could personally do to mitigate could have prevented a bad outcome.

People want their work to matter, so building an emotional connection to the humans represented by the data we are steward for is key to inspiring long-term, very personal commitment and advocacy for privacy initiatives.

Sixth, Making Your Program Sticky

Have you ever felt defeated when a really important change you implemented reverted back to the old way of doing things? Maybe you worked really hard to design the perfect pantry but when the builder turned over the keys, all you found were basic shelves?

Many privacy professionals worry that a single individual decision made within an organization can invalidate all their work. In reality, mistakes occur, are investigated, and companies are absolved very frequently. In HIPAA for example, there have been only 101 reported enforcement actions in over 51K investigations. Most of the time a company documents their due diligence and is either absolved or receives a minor recommendation for improvement.

If you follow enforcement actions in the news very closely, the rationale for why some fines or penalties are so large or small is tied to the effectiveness of the programs that were built to prevent those mistakes from happening. And the good news is that there is a blueprint for ensuring you fall into the category of "effective" program.

To be considered defensible under US regulatory statute one must invest in the 7 elements of an effective program:

7 Elements of an Effective Compliance Program

High-level Oversight

Compliance Integration into Policies & Procedures

Open Lines of Communication

Training & Education

Monitoring & Auditing

Response to Detected Errors

Consistent Enforcement of Standards

01. High level commitment to the program or change : This is your General Contractor, Architect, or Homeowner. Who you assign as the high-level decision authority may be different if you're building for basic shelter, for safety, or for prestige. In some companies, this may be general counsel if regulatory compliance is the primary goal of the privacy program. For other companies, and particularly those that operate large data systems as a core competency, this may be a dedicated official under engineering.

Regardless, great changes begin with a person who is assigned an accountability for a change and who is empowered to direct or influence the organization. Sometimes this means providing enough elevation (seniority) within the company or the independence to accomplish the privacy work assigned. Other examples of high-level commitment include leadership statements of support or inclusion of privacy mandates in org-wide KPIs or goals.

02. Written policies, procedures and guidance : A conversation with your cabinet makers is probably not sufficient to describe that perfect pantry you wanted them to build. The same is true for privacy practices - they need to not only be written down - they also need to be easily found and specifically written to help guide the reader.

The nature and purpose of policies (outcome we need to achieve), procedures (how we do this) and guidance (what tools we can use in which ways) are different - and it's important to invest in all three.

Going back to the decentralized, standardized and centralized models discussion earlier in this chapter, consistent policies can be in a decentralized model, which can affect a program's defensibility. At the same time, centralized programs may build procedures or guidance that are not universally applicable across large organizations.

03. Open lines of communication : How hard is it to reach your architect or general contractor? Do they return your calls and confirm that your needs are being met? The same is required of privacy programs - if someone has a question or concern, how do they communicate with the privacy program office? Intranet sites, dedicated email addresses, and even a dedicated reporting hotline are expected or even required under some privacy laws.

04. Education and Training : Once things are written down, the next step is to educate, train and build awareness. Education (why we do things) and Training (how to do this in your role/job) serve different purposes. Without both the why and the how, changes tend to not stick very well. Awareness reminds people of the investment in education and training that were made - posters, privacy week slack messages, or email campaigns to remind people about key practices are useful to retain since they are evidentiary when defending mistakes.

05. Monitoring and Auditing : Especially for new privacy program managers, monitoring how well a change is being applied is really important. Design doesn't always get things right in a first iteration so monitoring if there's undue friction, if an organization has undergone an operational "pivot", or that a new process or technology is excessively difficult to perform as intended helps to swiftly course correct. Asking for feedback from your team/org/company during early implementation is a perfectly adequate form of monitoring for new program or operational practices.

Over time, processes and technologies stabilize. Once program owners are confident that the practice has been documented, trained, and is operating well, periodic auditing of effectiveness is expected. Audits measure whether people, a process, or technical control is doing what they said they would do – - not whether what they are doing is a good approach. Audits are intended not to find programmatic improvements, but to establish a compliance rate- typically on a percentage basis.

Auditing before a process or technology is stable is not recommended since findings have actionable consequences and it can hurt morale to get a failing grade when you're still building an effective approach to managing privacy risk.

06. Investigation and Response : When errors are detected or reported, every program manager is expected to investigate. For system reported errors, a sampling rate (one in 50 logged access events) is appropriate. For human reported concerns or errors, investigation is always recommended. Findings should be documented and retained to demonstrate commitment to this program element, but outcomes of investigations are not typically shared with the person who reported this issue. Indication of completeness and that appropriate action has been taken is required from some privacy frameworks, but the details of the investigation are not typically reported unless breach notification requirements are triggered.

07. Enforcement and Discipline : During the investigation process, the root cause for confirmed incidents should be thoroughly documented. Sometimes there are poor technical configurations at the root of data protection issues and sometimes its human error. Sticky changes require that the root cause of issues be addressed - be it a technical remediation plan that is tracked to completion or disciplinary action for the individual. This could be simple re-education for unintentional mistakes or more grave actions for intentional misconduct. All remediation actions should be documented and preserved for defensibility. Arguably, errors and disciplinary actions should be broadcast as well - without personal attribution, of course - for deterrence value and as awareness that the written guidance, education, and monitoring investments that all employees make have purpose and are consistently and constantly enforced.

At the end of your first year, an unofficial 8th element of an effective program would be to conduct a risk assessment or retro for your program where you establish what went well, what might need improvement, and where you will prioritize efforts and resources for the next year. This commitment to continuous improvement is a hallmark for sticky (and defensible) privacy programs.

So there you have it - your first year is under your belt. You've moved into your new home and have a plan for how you'll spend your maintenance and home improvement dollars. You've made good neighbors, built strong but not impervious fences, and it's the right size for your family and the industry you work within. Congratulations!

Chapter 03.

Upendra Mardikar (LinkedIn)

Upendra is a prolific inventor and cyber security & digital identity business-enabler executive with an “art of possible” mindset who led global teams to secure world class organizations and held executive and senior leadership positions at American Express, Visa, PayPal and is credited with 95+patents.

Upendra is EVP, Chief Information Security Officer at TIAA. In the past, he has worked at Snap Finance, American Express, Visa and PayPal. He is a regular speaker at esteemed conferences for Stanford University, Global Big Data Conference, NFC forums, and many more. He is also an advisory board director for select security startups and helps venture capitalists evaluate companies.

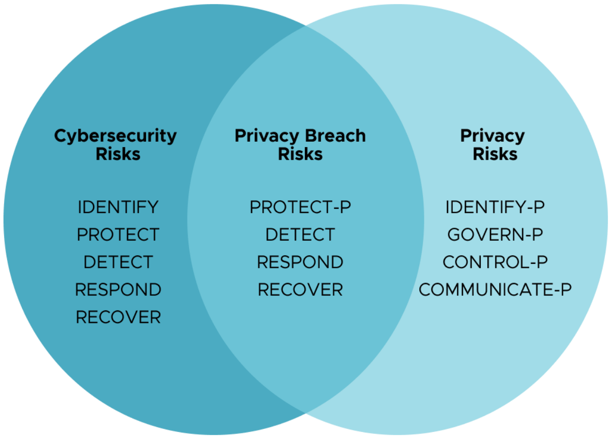
Section : Applied

Security & Privacy : DevPrivacyOps & DevSecOps

Several experts have tried to reconcile Security and Privacy. NIST has created a very apt Venn Diagram that talks about the overlap of Security and Privacy as it relates to Cyber Security Framework and NIST Privacy Framework.

As it relates to Security, there is a huge collection of literature that defines and describes Security. One of the classic ones is the CIA triad which is Confidentiality, Integrity and Availability. There are several dimensions to Security. User/ Identity Security, Device Security, Application/ Software Security, Infrastructure Security, Data Security, etc.

NIST defines Cyber Security as the ability to protect or defend the use of cyberspace from cyber attacks. NIST has created a very popular Cyber Security Framework (CSF) that defines Cyber security into 5 pillars: Identify, Detect, Protect, Respond and Recover.



NIST also defined Privacy Framework that has 3 parts:

01. Core - A set of privacy protection activities and outcomes.
This gives the foundation as the name suggests for communication and prioritizing of privacy protection activities across the organization. The Core is further divided into key Categories and Subcategories—which are discrete outcomes—for each Function.

02. Profile - This represents an organization’s current privacy activities or desired outcomes. Profiles can be used to identify opportunities for improving privacy posture by comparing a “Current” Profile (the “as is” state) with a “Target” Profile (the “to be” state). Profiles can be used to conduct self assessments and to communicate within an organization or between organizations about how privacy risks are being managed.

03. Implementation Tiers” provide a point of reference on how an organization views privacy risk and whether it has sufficient processes and resources in place to manage that risk.
The pillars in Core are: Identify-P, Govern-P, Control-P, Communicate-P, Protect-P. The overlap is defined with the pillars of Protect, Detect, Respond and Recover.

In a nutshell, *privacy refers to how much control a user has over his/her personal information, who has access to that personal information, is it being used for the purpose it was collected for, is it being shared with third parties and does the user have right to know it and right to delete it. Security is how to protect this personal information (and more) so that it doesn’t fall into wrong hands. It is shared only to designated parties be it first, second, third or fourth parties. Information has all the confidentiality, integrity and availability characteristics.*

As organizations establish privacy programs, partnering with Security organizations can be critical to Privacy organizations.

As much as Security has in by design, default and deployment, Privacy has to be considered right from the inception.

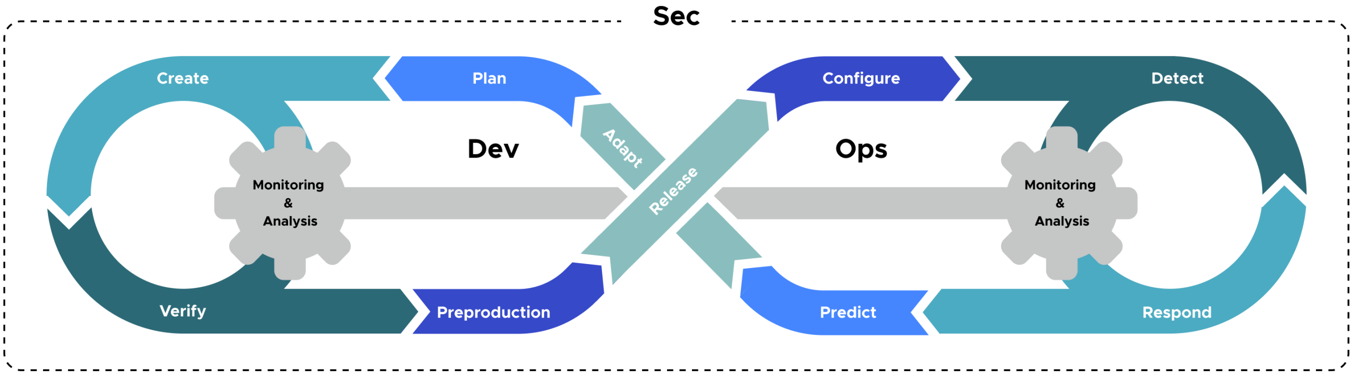
DevSecOps, DevPrivacyOps, DevSecPrivacyOps

As we think about incorporating DevSecOps and Zero Trust in DevSecOps, Security is embedded in each phase of DevOps both on the left side of the release and Right side. This classic Infinite Cycle should also have Privacy in built.

Planning - In addition to system centric protection and threat modeling during Planning phase, some privacy questions should be asked:

- Are we asking for any Personal information both implicitly and explicitly?
- Will this information be used for marketing purposes?
- Will this be shared with outside parties?
- Will we sell this information in any shape or form?

Security can also address questions like threat modeling, impersonation, protection, geography because of regulation like GDPR and state laws like CCPA, CPRA. Security needs to consider both insider and external threats as the breach implications could end up with privacy regulatory consequences.



Creation

In creation, in addition to ensuring that appropriate Cookie Consent, Data Subject Access Requests (DSARs), Privacy Policies are considered, ensuring that this happens over secure connections, securing cookies and having those consents and DSARs that has proper integrity is crucial. Security and Privacy Architecture need to be defined in together.

Verification - In addition to SAST, DAST, IAST and security testing, privacy testing should occur. Privacy verification and test suites should include tests that would enforces user preferences on marketing, cookie consent, etc. Ensuring that database captures those preferences and enforces down stream is extremely important to maintain privacy posture of the organization. This test suite should be part of regressions. There will be an overlap between Security and Privacy for test cases related to Access Controls, Data Protection at rest, in transit and in use, Encryption, Least privilege, Auditing as the data is shared across multiple departments and organizations especially distributed geographically.

Preproduction, Release

Environment as code and binary validation should remain the same for Security and Privacy.

Configure and Detect

As organizations think about the Environment as Code, Skew detection is important for both privacy and security. Additional test cases and controls are required to detect these skews.

Respond and Predict

Response and Prediction should be enhanced for Privacy as violation to Privacy should be cataloged and responded with a similar impact assessment as is done for Security.

Conclusion

Thus as we see, there are lots of similarities between Privacy and Security. In the foreseeable future environments, where we are in a Cyber Pandemic and experiencing heightened Privacy regulations, it is important for organizations to embed Privacy and Security as a part of DevOps call it DevSecPrivacyOps. Security and Privacy shouldn't be seen in isolation.
As organizations mature their DevSecOps, they should consider incorporating Privacy pipelines along with Security pipelines and devops pipelines.

As a community, we need to start defining Privacy Capability Maturity models and best practices as in the security industry and leverage synergies and best practices from both industries.

It is going to take a community effort to define these new paradigms to operationalize Privacy into DevSecOps and move towards DevSecPrivacyOps.

Chapter 04.

James Robson (LinkedIn)

James Robson is a data sharing subject matter expert who became the first person to place non-governmental charity research data into the Office for National Statistics in April 2022. He is the Data Protection Officer for The Evidence Quarter and What Works for Children's Social Care and an SME on privacy enhancing technologies including Trusted Research Environments. He holds the International Association of Privacy Professionals (IAPP) membership with the CIPP/E and CIPT qualification as well as the ISO 27001 Lead Implementer certification for Information Security Management System implementation. James is active in the UN PETs Lab, the UK Interparty Parliamentary Group for Blockchain and the Secure Data Access Professionals (inclusive of The Crick Institute, The Alan Turing Institute and the founder of the ONS 5 Safes methodology amongst others).

Section : Proactive

The Future & Fears of Data Altruism

What would you do if you had unlimited access to all data held on every digital device on the planet? If you're anything like me then the thought of some nefarious actors using it for some kind of theoretical conspiracy to make me vote in a certain way might spring to mind or concerns about people knowing too much. I'm not sure who those people are but I'm in a state of worry if there was this open access for people to undermine every part of my being. I don't really want people to read my intimate texts or WhatsApp messages.

The monkey mind running through scenarios that unfortunately already exist means I didn't consider the question. I think of myself as a reasonable guy who holds world peace ideologies and think there should be more self love in the world (I became a yoga teacher to help with that too) but I've immediately limited myself. I'm not considering data as the "new oil" that if mined correctly yields incredible utility, I'm considering it as the "old oil" where there is no correct mining that isn't potentially disastrous to our planet no matter how safely it's mined whilst providing short term benefit before creating an unstoppable catastrophic event that can kill all our grandchildren. I'm concerned about the pollution.

This pollution knows who I am, knows my shopping habits, knows my current state of mind and knows what to put in front of me to cheer me up. It doesn't however (unless I hold a bias to self-betterment) automatically point me in a direction that necessarily means I live longer or alleviate the constant compounding of all my problems that my body may one day package up for me and send me on my way. Must remember my wearable tech for that too!

Therefore, I argue there is pollution before a solution, and it is this pollution we're experiencing right now. This phase of pollution doesn't allow for conceptual solutions to be considerable. Considerable in both senses of the word: we are only thinking within the parameters of our personal echo chamber, and; the magnitude of the solutions that data can solve. Have you forgotten the "data" component?

There is so much pollution that government has loosely intervened with partially toothed legislation tigers appearing more as inconvenient bureaucracy that is thought to impede innovation. Yes, shock, horror, the laws are being blamed despite the laws deterring dark internet open data access that has designs on leaving us all destitute in a post apocalyptic, H.G Well's Morlocks vs Eloy scenario of data accessors and the data inept. I mean they would take your money and the influence on every individual's daily decisions would increase 5 million fold. Your life may not be your own.

So, now I have forgotten about personal data in this article and I can't remember the question. Herein lies the rub. How do we solve real-world problems with personal data analysis and research upon personal data when we don't realise we can? I can throw fancy concepts out there like differential privacy and federated analysis which gets boring quickly if I hint at a combination of these with the General Data Protection Regulation (GDPR). Mention AI and blockchain as further solutions that will change everything for the better and the average individual hears the controversial mixed message of humanity's annihilation and how people launder money respectively (not that respective!).

The sudden concept of the perceived GDPR glass ceiling enabling altruistic innovation and

> **"I'm not considering data as the "new oil" that if mined correctly yields incredible utility, I'm considering it as the "old oil" where there is no correct mining that isn't potentially disastrous to our planet no matter how safely it's mined whilst providing short term benefit before creating an unstoppable catastrophic event that can kill all our grandchildren. I'm concerned about the pollution."**

> **Data Altruism, as defined in the EU Data Governance Act, “data that is made available without reward for purely non-commercial usage that benefits communities or society at large.”**

sharing of data, and not compounding the barriers to innovation where whole countries have become personal data silos is almost as controversial as accurate scientific measurement of the curvature of the earth in front of a Flat-Earther. Has anyone stopped to think that it is possible to design something that you don’t need to see yet there is still the ability to come to a usable outcome.

Like anything that becomes normal and simplistic in its utility, such as flicking a switch on the wall and a bulb above your head emitting light or pressing lightly on a piece of glass to allow you to speak your cousin traversing Ayers Rock in Australia from your flat in Poland, it is quite difficult and complicated to get to that point. Complicated but possible.

As a Data Protection Officer with unique insight into UK government spending due to being privileged to help research organisations legally access and analyse data, I’m privy to what is needed for the concept of data altruism to become a reality. Data Altruism, as defined in the EU Data Governance Act, “data that is made available without reward for purely non-commercial usage that benefits communities or society at large.” Let’s not get carried away here, there is a lot of data protection paperwork from the hang-ups of the soon to be replaced UK GDPR but why not if researchers are accessing Child (Care) Protection Plans where children have been taken away from their families so they can find solutions for similar families to not lose their children.

A paper with some serious clout and published by the UK Government, called “Data Saves Lives”, has become the hushed backroom scoff of a lot of IT people struggling with the daily grind of just managing data, be it personal or not. The perspective on how data can save lives is yet again lost in the noise of everything!

With the UK National Audit Office quoting a £1.4 Trillion spend by the UK government with 8% having any robust evidence-based research on whether pointing the money in a certain direction will be effective (or not) it quotes up to 85% doesn’t have any evidence based research. Again, I get lost in the reality of the reeds surrounding a data problem. A data problem, a research problem, a privacy problem, a technology problem and a legislation problem seemingly to stifle the 85% problem and the UK is heralded as doing this well!

The thing is, the UK is doing this well compared to the rest of the world. If what I want you to think has not yet been thought then let these words socially engineer your mind to understand this. If I had unlimited access to all data on every digital device on the planet I would find a way account for all global government spending to make sure every penny goes into helping people in ways that are proven and known to help people and continue to use that data to improve upon any improvements in a never ending upward cycle of data altruism.

What the world needs now isn’t love, it’s trusted data custodians to curate secure data environments layered with privacy enhancing technologies with a blockchain layer to allow for and track all uses of data and embed all legislations into all uses, and by doing so allow vetted researchers access to the data they need - love comes before, during, and after everything at all times for this endeavour.

Chapter 05.

Section : Proactive

Need for Federal Privacy Law in the United States

Kiran Sharma (LinkedIn)

Kiran is a Cyber Security and Data Privacy Enthusiast with 15+ years of experience leading essential Security and Privacy programs and delivering projects, processes, tools, and standards that ensure cyber resilience and global compliance. He has the ability to optimize enterprise cybersecurity and privacy for financial services, Fintech, and Healthcare Industry. He has the expertise in translating evolving industry risks and a myriad of privacy regulations into ambitious technology around a proactive defense by continually sharpening the company's security and privacy maturity and aligning solutions with well-known industry frameworks. He has worked with customers, internal and third-party partners, and vendors across a number of industries including Banking & Finance, Telecommunications(UCaaS), Energy & Utilities. Led diverse global teams with direct, dotted line reports and managed service providers with budgets up to $12M.

Introduction

The world requires data to guide routine business transactions, financial transactions, medical research, and supply chain management, allowing businesses to scale and grow. During the COVID-19 pandemic, technology helped us stay connected emotionally and socially, highlighting challenges in privacy concerns for our personal information.

Our hyper-connected world relies on data: "Data is the most valuable commodity on Earth, surpassing fossil fuels like oil." Everyday conveniences such as GPS navigation, wearable technology, innovative home technologies, and content streaming services rely on data, which enriches our lives, enables us to make informed choices, and helps us use our time more efficiently.

The US is one of the largest economies in the world that does not have comprehensive privacy regulations at the federal level. Instead of having a comprehensive federal privacy law, the US has different sectoral laws combined with individualized state breach protection laws, with California leading the domino effect by introducing its privacy regulation that came into effect on January 01, 2020. Colorado, Connecticut, Virginia, and Utah are the other four states that have introduced and successfully passed comprehensive laws. In contrast, other states either have a bill in the process or fail to become law. State-level momentum for total privacy bills is at an all-time high; as of July 20, 2022, a Comprehensive Bi-partisan Federal regulation, "American Data Privacy And Protection Act, H.R. 8152," has passed the U.S. House Energy and Commerce Committee and is headed to the House Floor.

This paper demonstrates the requirement for privacy regulation at the Federal level in the United States. This paper will describe the History of Privacy, Drawback in current laws, and an analysis of essential requirements for a federal privacy law such as Bipartisanship, Pre-emption, Private right of action, Consent, Notification, and transparency, accountability, Limits on processing, Civil, and Individual rights. Finally, this paper will conclude by highlighting the need for Privacy regulation at the Federal level and enforcement. At the same time, states bridge the gaps that protect individuals and their right to privacy.

History of Privacy

Privacy "is the essence of freedom: without privacy, individual human rights, property rights, and civil liberties – the conceptual engines of innovation and creativity could not exist in a meaningful manner."

Privacy is as old as humankind, which relates to human dignity, freedom of association, freedom of speech, and safeguarding personal life from public view. Humans' need for privacy can be seen in the writing of Socrates and other Greek Philosophers, when differentiation was made between the "outer" and the "inner," between public and private, between society and solitude. The concept of privacy has evolved over the years, and each culture has defined or derived it as a social concept and is referenced as the need for one's well-being. Political, Social, and

Economic changes throughout history created the demand to meet the new standards and requirements of individual privacy. Generally, the common law provided complete protection to individuals in person and property.

> **"Privacy is the essence of freedom: without privacy, individual human rights, property rights, and civil liberties – the conceptual engines of innovation and creativity could not exist in a meaningful manner."**

As the law gave a remedy for physical interference with life and property, it has been found necessary from time to time to define the exact nature and extent of such protection to privacy anew.

However, privacy in historical times is considered the right to solitude and can be defined in multiple facets, such as (1) Information Privacy, which involves details of an individual, (2) Bodily Privacy, which relates to physical selves, and (3) Privacy of Communications, covers any communications related to an individual, (4) Territorial Privacy, limitations and intrusions into one's property or personal space. The exchange of information Was private to individuals and was done either in solitude or at the convenience of a social setting where individuals knew one another. With the emergence of technology, the focus on privacy has shifted from a societal sense to a digital or online sense, as privacy can be tied to the information of an individual or the Data of an individual that, in other terms, is known as Personal Information or Personal Data.

Drawbacks in current laws

Technological inventions have driven opportunity, economic growth, and competitiveness throughout history. A multitude privacy laws has created roadblocks, are expensive to comply with, are complex, and resource intensive to understand and implement. Most Americans report being concerned about how companies use their data (79%) or the government (64%). Most feel they have little or no control over how these entities use their personal information, according to a new survey of U.S. adults by Pew Research center that explores how Americans feel about the state of privacy in the nation. The following are the few components that current state breach laws, state privacy laws, and sectoral laws are missing:

01. Opt-in consent

Opt-out services are effective if a consumer knows who has the data; without knowledge about the data processors, it's hard to request every service. Instead, the privacy laws must provide consumers with Opt-In consent with clear processing categories and third parties. If additional processing is required, request Consent by notifying the consumer and let them choose to either provide or deny the request.

02. Non-discrimination through Automated Processing

Intelligence and automated processing of data sometime could lead to bias or discrimination. There must be provisions to combat automated decisions and Bias in the data models.

03. No data-use discrimination

A company shouldn't discriminate against people who exercise their privacy rights; for example, the company can't charge someone more for protecting their privacy, and the company can't offer discounts to customers in return for their giving up more data. This regulation should also clarify civil-rights protections, such as preventing advertisers from discriminating against specific characteristics.

04. Privacy Harm

Breach laws place the preponderance of evidence on the victims, which is hard to prove as the privacy risks or harm is not immediately known to the consumers.

Essential requirements for a Federal Law

The U.S. Privacy legislation has been discussed by policymakers, companies, privacy advocates, and many other stakeholders for years. Many proposals and drafts were introduced over time but have fallen short of delivery. Congress must consider creating a baseline that could address fundamental issues about consumer rights and data protection from misuse. However, they should avoid boiling the ocean to handle all the problems concerning the latest technological advances. The technology is snowballing and proliferating, and it is hard for the law to catch up as the time and effort involved in creating a rule is not scalable.

Here we will analyze and review the essential requirements for having Data Privacy at the Federal level.

A key objective of federal privacy legislation is to shift the burden of protecting personal information from individuals to the businesses that collect and use the information.

Bipartisanship plays a pivotal role in U.S. Politics across foreign and domestic policy domains and will likely be an essential factor in enacting privacy rights at the federal level.

Pre-emption: As digital boundaries expand interstate and international, an individual’s privacy must not depend on their location or state. Having a baseline federal law with room for growth is much better than no Regulation. Hence, the pre-emption to cover the “insufficient or inconsistent” state laws fill the void with a sunset provision for both state and privacy laws to catch up with the demand for technological innovations.

Private Right of Action: Limiting the recovery to “actual damages,” requiring a heightened “Knowing or reckless” liability standard for most statutory provisions, and including a “wilful and repeated” offenses standard to sue for more administrative violations.

Consent, Notification, and Transparency: Consumers must provide affirmative consent to collect or transfer sensitive data, and the focus must be on a reasonable expectation of “context.” Organizations should provide transparency in three-layer instead of one-size-fits-all: a) timely, context-specific notifications for individuals, b) basic privacy statements targeted to individuals, and c) comprehensive privacy disclosures aimed at regulators and other close observers.

Graduated obligations and accountability: small and medium entities (including smaller non-profits) should be exempt from some specific obligations with high compliance costs. Essential underlying commitments—like the duties of loyalty and care, data security, and privacy risk assessments—should apply to all organizations but be tailored to the scale of the covered entity and the volume and nature of data involved. Additional obligations should apply to “large data holders.”

Civil Rights and Individual Rights: Combining the individual rights to request access, correction, deletion, and portability of personal information into the overarching “Right to Control” section and adding a separate “Right to Recourse” that would have to be exercised before bringing litigation. While addressing algorithmic discrimination, by designing for human intervention in decision-making and discrimination cases must be referred to the relevant federal agencies.

Conclusion

“We cooperate with corporate surveillance because it promises us convenience, and we submit to government surveillance because it promises us protection.” A federal privacy law is required to provide consumers with protections and must establish a consistent framework that promises innovation and technological advances. Spurred by the development of new technologies, the law has responded in numerous ways to grapple with emerging privacy problems.

Although the law has made great strides, much work remains. It is a race against time for the latest American Data Protection and Privacy Act to be enacted as law in this legislative period of 2022. The research conducted by Morning Consult found that 83% of voters say that Congress should pass national data privacy legislation this year as there is bi-partisan support from Democrats (86%) and Republicans (81%) to prioritize a federal privacy bill.

Chapter 06.

Section : Innovative

Data Privacy Automation

Bill Schaumann (LinkedIn)

Bill Schaumann is a seasoned privacy professional with over 20 years of experience leading teams of information security and privacy analysts delivering a wide range of programs and services to fortune 50 clients. Bill has extensive experience designing and managing the development privacy programs and designing the use of the supporting technologies to improve privacy and security controls which reduce compliance risk. Working in big 4 consulting firms, Bill has served both large corporations and start-up operations, in planning and building operational and support processes and policies across a variety of industries. Bill has a technology background and has earned certifications of CIPP/IT, CISSP, GEAC.

Data Privacy Automation concerns the protection and use of personal and sensitive information as aligned with an organization's legal obligations. As a part of a robust privacy program Data Privacy Automation focuses on the electronic end of privacy and the personal information collected, processed, categorized, and protected for use by an organization. Data is a key asset at the heart of many organizations, and in recent years the types of information being processed has added both new business functions and new privacy and security risks. The growing complexity of both data environments and legal obligations has created an array of challenges for privacy professionals who have been tasked with reducing their organizations' privacy risk.

Personal information like Name, Address, Social Security Numbers, Account Numbers and similar identifiers are keys links to vast arrays of transactional and preference data stored across vast arrays of internal and external data repositories. Manually tracking data inventories, and processing activities is a large and challenging task for many companies.

Previous to the advent of AI driven technologies, updating privacy inventories and tracking data use was completed in mature organizations with a deep application of Privacy by Design principles wherein manual process checks or privacy impact assessments were embedded into the day-to-day business and IT activities and became part of the company's culture. In less mature organizations, completion of one time or annual inventories of systems, applications and data produced lists of repositories containing personal information that either were incomplete or became stale in a matter of weeks or months. For these reasons, large organizations with complex data environments that depended on human actions and manual processes often lacked complete records of the processing of personal information.

To understand the use of personal information and manage privacy risk in an organization requires two primary areas of focus. The first is having the ability to fully track and monitor the individual pieces of sensitive data in use. The second is then to have the ability to apply administrative and technical controls on the data needed to meet the company's legal obligations.

By automating the identification and monitoring of personal and sensitive information, organizations can significantly advance the control capabilities over the collection, use, and categorization of personal information. New AI technologies can continually track and monitor changes in personal information to complete assessment tasks or reporting activities that previously were either completed manually, or not completed at all.

"By automating the identification and monitoring of personal and sensitive information, organizations can significantly advance the control capabilities over the collection, use, and categorization of personal information."

The first step is to continually monitor the environment where the PII is stored and used. This includes a view into the applications, systems, and third parties that are used to complete the day-to-day business transactions. Monitoring is not limited to storage alone. API connectivity provides the ability to see transactional activities between applications.

The second step involves the creation of rules, or control policies which are focused on the use of personal information. Rules that can monitor new instances or changes to data can trigger alerts and initiate further action needed to enforce the defined control.

Automated enterprise monitoring of the systems and repositories can create a 360 degree view of an enterprise data environment. The enterprise data environment or privacy inventory contains several levels and types of information that are pertinent to understanding overall privacy risk. Storage repositories, processing systems, processing purposes, data types, data classifications, and sharing and retention are all important pieces to be considered.

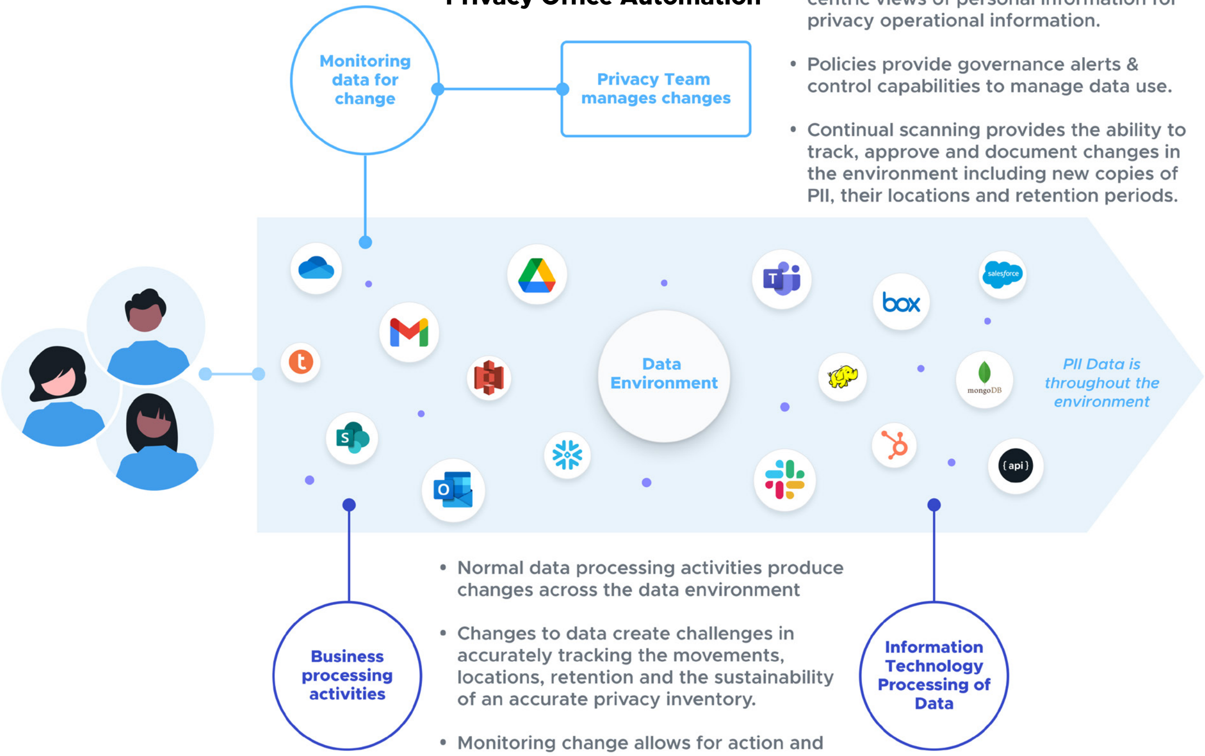
By establishing API or integrated connections into back end systems and repositories, AI driven intelligent crawlers can quickly and accurately scan and document in what systems personal information is being processed and stored. Within the identified systems individual data elements are discovered, and identified by type, and sensitivity levels. Further investigation discovers and documents integrations with other systems, automatically creating a transactional map of data use.

With an AI driven platform established, operational governance policies can be layered on top of the data layer to create new privacy centric views that support traditional privacy framework content areas. For example, the automated monitoring of data age combined with retention policies can generate communication alerts for expired or stale data. Additional rules can be created to redact data, or move it to a safe archive until reviewed and added to a permissions list. Policies can be customized to fit the business need and culture. By providing this type of view and control over personal information privacy teams can provide new levels of protection and risk reduction.

At the center of this data is the individual and their identity. By monitoring this new identity centric view with a focus on specific identities, regulatory privacy requirements become real and tangible components of the operational governance model. By achieving more operational control privacy risk can be greatly reduced across an organization.

Privacy Office Automation

- Data Dashboard creates 360 Identity-centric views of personal information for privacy operational information.
- Policies provide governance alerts & control capabilities to manage data use.
- Continual scanning provides the ability to track, approve and document changes in the environment including new copies of PII, their locations and retention periods.


Monitoring data for change
Privacy Team manages changes
Data Environment
box
salesforce
mongoDB
{api}
PII Data is throughout the environment
Business processing activities
Information Technology Processing of Data

- Normal data processing activities produce changes across the data environment
- Changes to data create challenges in accurately tracking the movements, locations, retention and the sustainability of an accurate privacy inventory.
- Monitoring change allows for action and control to protect.

Requirements

From as early as the The Privacy Act of 1974, and continuing to this day, independent organizations and governments have developed standards and passed legislation that governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals maintained in federal agency, and private corporation databases and systems. More specific sector-based regulations like HIPAA,GLBA, FERPA, and COPPA sought protections for health,financial, educational, and population based information.

Driven by many new regulations, standards organizations developed privacy frameworks with domains focused on key regulatory requirements. Early frameworks like the AICPA's Generally Accepted Privacy Principles (GAPP) and The Organization for Economic Co-Operation and Development (OECD) privacy principles were guides for early privacy practitioners. To this day many of these principles still guide modern privacy programs.

As drawn from these and other regional regulations like the GDPR and CCPA, managing key privacy requirements is organized by topical primary domains, that group like-requirements together. By focusing on common privacy domains AI driven platforms can help to streamline operational privacy governance by supplying privacy teams with new views of their organization's PI processing.

Areas where automation can be brought to bear on privacy management domains include;

Individual rights processing, Appropriate Data Use ,Data Storage, Data Classification , Metadata Tagging , Redaction control policies , Compliance documentation, Consent processing.

Each of these areas requires specific data to be gathered and monitored. Data Privacy Automation technologies enables monitoring and alerting capabilities.

01. Individual Rights Processing - Perhaps the most obvious use of automation in privacy management is positively identifying and retrieving all data of an individual to fulfill an Individual Rights Requests (IRR) by drawing data from all relevant repositories. By adding automated request processing workflows, completely automated systems can process requests with any level of human interaction as required.

02. Appropriate Use.- By tagging and approving data for a particular processing activity and noting the storage locations, new uses and locations can alert privacy teams to investigate and take action.

03. Data Storage - Automated file and folder scanning is an efficient way to monitor application data stores, structured and unstructured data sets, databases, shared folders and other storage locations.

04. Metadata Tagging - Traditionally DLP systems could search for a provided string like SSNs but AI systems can now find the string and also understand its an SSN by the context of its use. Tagging the action provides a record used for further monitoring and rule base actions.

05. Data Classification - Intelligent AI powered platforms can now recognize and automatically assign classification tags to most common data elements. Additionally, AI systems can learn to recognize forms like drivers licenses, health care and financial forms and provide proper classification tags as well.

06. Redaction control - Once a document has been identified, tagged, and classified as sensitive AI platforms can redact fields recognized as sensitive providing a new layer of access control over internal documentation.

07. Compliance documentation
With processes being logged and data use monitored and tagged documenting processing activities becomes a natural output of automated privacy management

08. Consent processing - As an early adopter of automation, several tools and platforms now exist to capture and track opt-in opt-out consent status.

Privacy is contextual

Unlike Information Security, Privacy is contextual. While Information Security professionals monitor for the status of controls like current patch levels, log files, or access control rights, which are more digital in nature, privacy teams use gathered data to analyze and assess the appropriateness of use, the ethics of the processing, and the resulting risk of a particular business process or activity.

Traditionally this has been largely a manual and often overwhelming proposition. However, with advancements in AI driven privacy automation, the gathering of data that is required to make key analytical decisions is becoming not only an easier task, but also a task that privacy teams will no longer have to expend long hours and many resources on. They instead will have a 360 degree view of their data and more time to review it and make the analysis and recommendations needed to protect their organization’s data.

Chapter 07.

Manisha Aurora (LinkedIn)

Manisha is an experienced General Counsel with over 10 years of in-depth corporate experience with a deep focus on privacy, data protection & security. She has built and managed in-house privacy programs in a start-up environment and also multi-national corporations with annual global revenues of over USD 10 billion.

Section : Innovative

Privacy & Artificial Intelligence - Living in Harmony

Has Google AI come to life?

Maybe! And allegedly it has the intelligence of a young child. Google engineer Blake Lemoine claims one of the firm's artificial intelligence (AI) systems might have its own feelings and says its "wants" should be respected. And in its defense, all the AI wants is to be treated as a "person". We hear you AI, so do I! Jokes aside, this is a serious issue, and nearly cost Lemoine his career. Google says the Language Model for Dialogue Applications (Lamda) is a breakthrough technology that can engage in free-flowing conversations. And denies all claims of its sentience.

This is our future - Isaac Asimov's dystopian fiction comes alive. AI is all pervasive. Love it or hate it, it's here to stay. AI is the main driver of emerging technologies like big data,

robotics and IoT. And will continue to act as a technological innovator for the foreseeable future.
So what's AI, all about?

Let's talk about AI

AI is the simulation of human intelligence processes by machines, especially computer systems. AI enables machines to learn from experience, adjust to new inputs and perform human-like tasks. Most AI, rely on deep learning and natural language processing.
AI has remarkable potential!

If done right, it can unlock many societal benefits across industries. In the education space, the lessons could be personalized for each student depending on individual learning styles.

In healthcare, it is being used to view the correlation of genetic data and clinical trial results, and can improve precision medicine.

AI technology is improving enterprise performance and productivity by automating processes or tasks. AI can provide insights on data on a scale that's not humanly possible. This capability can be leveraged by business to its benefit. For example, Netflix uses machine learning to provide a level of personalization that helped the company grow its customer base by more than 25 percent. AI capabilities make their way into mainstream enterprise operations, coining a new phrase "adaptive intelligence". Adaptive intelligence applications combine real-time data with decision science and highly scalable computing software. This aids businesses to make better and more informed decisions. And in e-commerce, it's being used to edge consumers to higher order values. Well, someone had to monetize it!!

Seems too good to be true – AI Challenges

AI does have the seeming ability to solve all scenarios. But it does have inherent challenges, some of which have been delved into below:

AI algorithms Bias

Algorithms are only as good as underlying data. AI technology may inherit human biases due to biases in training data.
The erstwhile Amazon recruitment machine learning models were biased against women. This algorithm was based on the number of resumes submitted over the past 10 years and the candidates hired. And since most of the candidates were men, the algorithm also favored men over women.

Data Scarcity

There just isn't enough baseline data to begin with. Additionally, there are a lot of global privacy laws that require the data not be transferred outside the country. China, India, Brazil and most recently Russia, are some examples of regulatory frameworks that require that.
With localization of data under many regulatory regimes, data is not diverse for global solutions.

Trust deficit

The unknown nature of deep learning models and its output, has created many critics. It is difficult for a common person to understand how a specific set of inputs can devise a solution for different scenarios.

Error Rate

Algorithms are prone to errors as compared to humans. A human can easily distinguish a cat from a caddy; but for AI to reach that conclusion would entail enormous amounts of training data and recalibration to tweak and tune its logic.

AI and the Law

The legal definition of AI is very simplistic – automated decision making. The General Data Protection Regulation (GDPR) defines it as the ability to make decisions by automated means without human involvement. The GDPR gives consumers the right to refuse to be subject to any of such automated decisions, insofar that it results in legal consequences such as denial of your home loan.

The challenge is that some laws do not really get into the details of differentiating between AI that screens for age eligibility to AI that screens for your insurance risk and denies a claim. The AI definitions are very broad and could hinder innovation.

And if AI, is not regulated, it has the potential of disparate impact; increasing the discriminatory divides that already exist. Regulation has to step in and level the playing field.

Recently, the Federal Trade Commission ("FTC" or "Agency") recently indicated that it considers initiation of pre-rule-making "under section 18 of the FTC Act to curb lax security practices, limit privacy abuses, and ensure that algorithmic decision-making does not result in unlawful discrimination."

The FTC's Recommendations Regarding the Use of AI

Those considerations entail (among others) the following:

Human Intervention : Human intervention is still needed, and perhaps always will be, in connection with monitoring the use and decisions of AI tools intended to address harmful conduct.

Transparency : AI use must be meaningfully transparent, which includes the need for these tools to be explainable and contestable, especially when people's rights are involved or when personal data is being collected or used.

Accountability : Intertwined with transparency, platforms and other organizations that rely on AI tools to clean up harmful content that their services have amplified must be accountable for both their data and practices and their results.

Data Scientist and Employer Responsibility for Inputs and Outputs : Data scientists and their employers who build AI tools—as well as the firms procuring and deploying them—must be responsible for both inputs and outputs. Appropriate documentation of datasets, models, and work undertaken to create these tools is important in this regard.

Concern should also be given to the potential impact and actual outcomes, even though those designing the tools will not always know how they will ultimately be used. And privacy and security should always remain a priority focus, such as in their treatment of training data.

AI – Risk Mitigations

Context Clarity

Most attention on regulating AI has been focusses on algorithms. But as GDPR demonstrates, constraining the context of use can be an effective way to regulate it.

Transparency

Automated Decision Making technologies are often opaque and to share the deep learning models that led to these conclusions, is of little value to the consumers. What could assist is the sources of data collection, and whether the data was collected legitimately.

Privacy enhancing technologies

Privacy enhancing technologies need to be utilized at the product prototype stage. Privacy must be practiced by design at every stage of the product development cycle. Once the product is ready to ship to market, it’s a bit late, to layer privacy principles. Getting it right at the get go, has advantages in terms of greater brand trust and loyalty, and fewer compliance costs and penalties.

Unified Platform for Sensitive Data governance

Not all data is equal. Sensitive Personal Information requires the greatest rigor in its use, processing and disposal. The challenge is that most companies don't know where that data resides. Vendors like LightBeam.ai have greatly simplified the task, by creating a unified platform for sensitive data governance.

Consumers Right to Delete and/or Amend

The AI training models need to provide for deletion and/or amending the consumer data for them to be meaningful. Consequently, there could be significant costs to retrain AI models, which is a contingency that needs to be planned for.

Industry Best Practice Standards

Regulatory understanding of technology is always a step behind. Given that, industry leaders need to create forums for best practices around use of this data and move forward for the greater good.

> To sum it up, Jeff Bezos says it best "We're at the beginning of a golden age of AI. Recent advancements have already led to the inventions that previously lived in the realm of science fiction – and we've only scratched the surface of what's possible".

Chapter 08.

Section : Innovative

Data Trustee Maturity Model: An Introduction

Priyadarshi [PD] Prasad (LinkedIn)

Priyadarshi (PD) Prasad is the co-founder and chief product officer at LightBeam.ai, the pioneer in data privacy automation.

An experienced tech industry professional with a passion for all things data including security, privacy and protection, PD is always on the lookout for interesting ways organizations use and secure their customers' data. Prior to LightBeam, he was a VP/GM at Nutanix, and helped replace complex tech stacks with 1-click simple solutions. PD sometimes brags that some of his code might still be controlling cars today. He has a Bachelor of Technology from NIT, Calicut and an MBA from S P Jain Institute, Mumbai, India

In the movie, "The Truman Show", Truman Burbank goes about living his life in an almost perfect, if boring, setting. Arguably his life is secure. Living your life as part of a reality TV show, watched by millions of people, is nothing if not secure in general. But privacy - that's another matter altogether. In 1998, the movie was quite ahead of its time in laying out the trade-off between privacy and other comforts of life. After realizing that his privacy has been traded off his entire life, Mr. Truman didn't like it one bit, and the movie viewers largely empathized with him. It is ironic though to reflect back and think that the movie came at the start of an era where nearly the entire world traded their privacy for such comforts like free email, free search, free video games et al. We all have been living in "The Truman Show", perhaps unbeknownst to most of us in the first two decades of the twenty-first century. It is only recently that consumer privacy has become a cause célèbre around the world (certainly pioneered by GDPR, and closely followed by CCPA in California, and CPPA in Canada).

Thanks to the emerging regulatory environment, consumer awareness, and internal realization, organizations are moving towards at least a checkbox compliance to privacy. Cookie Consent, Consent Management., Opt-out/ Unsubscribe, Privacy Policies, Annual Privacy Reminders etc. are all examples of that. Consider for a moment though that there is absolutely no privacy regulation in the world. Organizations don't have to care about giving consumers choices about using their data, sharing data, telling them about the data they carry or deleting that data upon consumers' request. In such a scenario, should organizations stop caring even if their consumers' data might become vulnerable and might get compromised?

Privacy and Security Interplay

It is easy to say that privacy and security are the two sides of the same coin. But let's dig into this a bit further, shall we, and consider two simple scenarios:

Scenario 1 - An organization does its utmost to adhere to privacy regulations. They care about their consumers' right to access their own data, and the right to be forgotten. They provide their consumers control over who all (partners) their data may be shared with. They manage and track consumer consent properly, so that their consumers are not getting bombarded with unwanted campaigns if they have already expressed their desires against that. However, **this organization routinely suffers from data breaches.** Consumers data is here, there and everywhere within the organization with little visibility, little control and little security. As a consumer, would you feel comfortable doing business with such organizations, and sharing your data with them?

Scenario 2 - An organization does its utmost to secure all sensitive data, including their consumers' data they have. They know exactly where all their consumers' data is present - across structured and unstructured data repositories. They know who has access to them within their organizations, and who that data is getting shared with external to their organization. Data is always encrypted at rest, and even in-flight to the extent possible without losing all utility of that data. With these controls in place, this organization rarely suffers from data breaches. However, **this organization is yet to implement all the necessary checkbox privacy compliance capabilities.** When it comes to giving consumers a choice to right to access/delete/sharing controls, this organization is left wanting.

The question is simple - which of these two organizations would you feel comfortable doing business with. Neither of them is in an ideal spot obviously but the question is do you care more about privacy checkboxes or about your data security? Looked at this way, at least I know what I'd prefer - an organization that can assure security of my data probably deserves my business more than someone adhering to all the checkboxes but failing on the most important, even if unregulated, duty.

A Model for Data Trustees based on Privacy and Security

Driven by privacy regulations, there has been a mad rush to get all the privacy checkboxes in place leaving the more important data security considerations under-served. Naturally this feels like a problem. Why is that - because we instinctively know that checkboxes help us CYA but our ability to be trustees of our customer's data is a function of both our privacy readiness and security readiness. Mathematically, this may be represented thus:

Data Trustee Index (DTI) = Data Security Readiness x (1 + Data Privacy Readiness); normalized on a scale of 0 to 100.

Data Trustee Index (DTI) for an organization can be between 0 and 100, both numbers inclusive.

Looked from this lens, data privacy readiness can be seen as a force multiplier to trust. However, if your data security readiness is missing, no matter how prepared you are for data privacy, customer trust in your business will be low. Note that one's overall trust score may be influenced by a variety of factors such as positive advertising, environmental, social, governance (ESG) readiness, corporate social responsibility initiatives, length and depth of customer relationships and so on. A lack of data security readiness leading to security breaches and sensitive data exposure can start to wean away the hard earned trust.

How do you get a quick understanding of your score as a data trustee from the perspective of data security and data privacy readiness? Let's look into that next.

Data Trustee Index (DTI)

=

Data Security Readiness

x

(1 + Data Privacy Readiness);

Normalized on a scale of 0 to 100.

Data Trustee Maturity Model

As noted above, we have broken the data trustee index into privacy and security readiness. Let's start with data privacy readiness. It's worth noting that there are elaborate exercises that may be done, and are done to assess an organization's privacy readiness (I am referring to the privacy impact assessments). Be that as it may, it is useful to keep a ready reckoner of your data privacy readiness with a simple model like this.

Data Privacy Readiness Assessment

Score your organization between a range of [0 - 4] on each of these data privacy readiness criteria:

01. Cookie Consent
On your website, visitors can opt out of accepting anything but the necessary cookies.

02. Consent Management
Customers' consent expressed through any channel is logged, managed and acted upon centrally.

03. Data Subject Access Requests
Your customers can make a request to you to share any and all data you are carrying about them.

04. Right to be Forgotten (RTBF)
Your customers can easily make a request to have you delete any data about them, subject to legal/regulatory reasons for data retention.
Consumer Control over Data Sharing
Your customers control what data you share and with whom.

05. Records of Processing Activity (RoPA)
Your ability to conduct a regular sensitive data audit and generate a RoPA report.

Rate your organization "0" if you have not had an opportunity to implement a process described above yet. On the other hand, if your process is largely automated, your consumers have the option to express choices and you can adhere to each consumer's choices, rate your organization "4" on that parameter. On this scale, overall Data Privacy Readiness will fall in the range of "0" and "24",

Data Security Readiness Assessment

Once completed, move on to the next step of rating your Data Security Readiness. Score your organization between a range of [0 - 4] on each of these data security readiness criteria:

01. Attribute 360 (the WHAT)
A complete view of all sensitive data your organization carries within its premises.

02. Structured Data Map (the WHERE part I)
A complete view of all sensitive data stored in structured data repositories.

03. Unstructured Data Map (the WHERE part II)

04. Entity 360 (the WHO)
Whose data it is that you are carrying within your company.

05. Partner 360
How is your sensitive data getting shared (or getting leaked) outside of your organization.

06. Data Automation
How are risks contained within your organization once detected?

07. Access Automation for Structured Data

Policy based authorization granting data access to the right individuals.

08. Access Automation for Unstructured Data

Continuous monitoring of unstructured content being accessed by individuals.

Data Trustee Index (DTI)

With this framework, your organization's data trustee index should come between 0 and 100 (both numbers inclusive).

Data Trustee Readiness = Data Security Readiness x (1 + Data Privacy Readiness).
Data Trustee Index (DTI) = Data Trustee Readiness x 100 / 800.
Where, 800 is the maximum score possible for data trustee readiness.

For a perfect organization scoring a "32/32" on data security readiness and a "24/24" on data privacy readiness:
Data Trustee Readiness (DTR) = 32 x (1 + 24) = 800.
Data Trustee Index (DTI) = DTR x 100/800 = 100.

For an organization that has implemented good privacy practices scoring a high of "16/24" but has given data security a short shrift scoring "16/32":
DTI = 16 x (1+16) x 100/800 = 27.

If you'd like to assess your organizational readiness and maturity towards becoming a data trustee, download this Data Trustee Index model here.

Conclusion & The Way Forward

Privacy is too important to be left to checkboxes. The data privacy journey to winning your customers' trust doesn't and shouldn't stop with cookie checkboxes for visitors to your website, or checkbox based manual data mapping exercises or even putting a comprehensive privacy policy for your customers. One can say those are necessary but not sufficient conditions. Truly caring about customers' sensitive data will take you to places where you will ask for observability into every nook and cranny of your organization where data might be stored including engineering, marketing, finance, and operations systems amongst others. *It will lead you down a path of figuring out WHAT data you carry, WHOSE data you have, WHERE is that data stored, WHY do you have that data, WHO has access to that data, WHO are you sharing it with, and WHEN can you get rid of it.*

But observability is just the first step. Next, you can implement policy based automation such that any data risk gets contained before it can do any damage. Unwarranted exposures will get acted upon automatically before a malicious actor can get their hands on that data. Furthermore, with a tabulated view of all sensitive data your organization might have shared with each partner of yours, you can automatically send notices to each of your partners asking them to delete precisely the data you would have shared with them 90 days (or "xx" days) back.

The manual processes that we all put in place to manage and adhere to data privacy regulations over the last decade were necessary for they were the best we could do. This decade though, the need of the hour is to focus on data security with the same rigor we apply for network security. If network security is the first line of defense (firewall), data security discipline is the last line that can help you keep your sensitive data secure on an ongoing basis even when the first line of defense falters.

Consider data privacy and data security as your twins needing your love and support in equal measures!

- Priyadarshi Prasad

Co-founder & Chief Product Officer, LightBeam.ai

Brought to you by the

PRIVACY AND SECURITY
INNOVATORS CIRCLE

Join us on LinkedIn

Published by

LightBeam.ai

Our vision is to help create a privacy-first world where customers' data is treated with the same respect as one would treat customers. We are on a mission to help you DISCOVER | ENFORCE | AUTOMATE sensitive data governance so you can focus on growing your business.

Contact us : **+1 (650) 224 8706 I info@lightbeam.ai**