ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

# 8 Considerations for Building a Strategic Privacy Program

**Technology, Privacy, and eCommerce**

Some readers might remember the Rubik's Cube, a 3D combination puzzle invented in 1974, which required the player to align the squares of the cube so that each of the six sides were one color. The difficulty in solving the puzzle was, after aligning all squares of the same color on one side of the cube, trying to align the colors on another side would result in mixing up the colors on the side the player had just completed!

Much like the Rubik Cube's frustrating set-up, a privacy program can cause the same level of exasperation. After developing a privacy plan to comply with the privacy laws of one country or state, along comes a privacy law from another jurisdiction that requires personal data to be treated differently and perhaps in conflict with how personal data is treated in the first jurisdiction.

The goal of this article is to provide building blocks for developing a strategic privacy program that deals with data privacy laws from different jurisdictions, as well as several other considerations.

## 1. Data mapping and data inventory

Abraham Lincoln said, "Give me six hours to chop down a tree, and I will spend the first four sharpening the axe." If we had only six hours to develop a data privacy program, we would spend the first four inventorying and mapping our company's personal data.

Until you know what personal data you have, how it is received, where it goes, and who has access to it, you cannot know what privacy laws apply, how to secure the personal data, and how the data can be used, to name just a few considerations. Creating a data inventory and data map can be tedious work. All personal data must be accounted for, classified, and mapped from when it is first received or created through the time of destruction.

Oftentimes, personal data is shared with third parties outside the company. Data sharing must be

included in the data map to adequately respond to customer or consumer data requests. Additionally, companies should have an accurate privacy policy and comply with the latest data privacy laws. This may require companies provide individuals the opportunity to opt-out of their personal data being sold or shared. Time spent in this process will pay dividends later.

## 2. Business alignment

A data privacy program should not exist in a silo without consideration of your company's vision, business goals, and objectives. A privacy plan that has tunnel vision and only considers privacy compliance or security, while ignoring other business considerations, can be a roadblock to achieving business goals.

Privacy should not compete with other business interests. When embedding privacy into a system or service, it should not impair full functionality. Privacy embraces non-privacy objectives and accommodates them in a win-win manner. Trade-offs should be rejected in favor of finding a solution that enables the achievement of multiple goals. Developing a strategic privacy program requires involving various business sectors and stakeholders so privacy is aligned with organizational culture, vision, and goals.

## 3. Privacy team

Develop a privacy team and areas of responsibility. The privacy team will be responsible for all aspects of the privacy program. The team may have a chief privacy officer, data protection officer, legal counsel, privacy managers, and technology professionals. Each person's roles and responsibilities should be defined, including the handling of specific situations.

For example, who will lead the investigation of a security incident, and what are the lines of communication? This might be a different person than who will lead the investigation of a consumer complaint regarding a data access request. Identify the lines of communication for persons on the team, especially for key functions and interfacing with other departments within the company.

## 4. Legal team

The legal team is responsible for monitoring ever changing and new data privacy laws and maintaining compliance. This may include evaluating new business initiatives for compliance with existing privacy laws. This will require an understanding of business plans and objectives to avoid the trap of privacy requirements becoming a roadblock to achieving goals.

Solving the Rubik’s Cube of privacy requires developing a compliance program that accommodates state, federal, and global regulations and laws. The legal team should be aware of and prepared to deal with investigations, complaints, and subpoenas from oversight agencies such as attorneys general, the US Federal Trade Commission, and supervisory authorities.

> Appropriate security is dependent on the size of your company, the type of personal data involved, the flow of data, and relationships with business partners and third parties.

The legal team may be tasked with monitoring internal compliance with implemented privacy practices such as the response to consumer or customer data access requests. The legal team will

also work with third parties such as vendors whose services involve the processing of personal data on behalf of your company. This will involve negotiating contracts with vendors for compliance with data privacy laws and protecting the company's interests through indemnity and other risk issues.

## 5. Data security

Data security is a close cousin to data privacy. It has been said you can have data security without having data privacy, but you cannot have data privacy without data security. Data security must be present throughout the personal data lifecycle, from collection through destruction or deletion.

A list of security considerations is too long for this article.  Appropriate security is dependent on the size of your company, the type of personal data involved, the flow of data, and relationships with business partners and third parties.  A data inventory, data mapping, and a privacy impact assessment can be invaluable in identifying and implementing appropriate data security measures.

## 6. Documenting privacy

Documentation is an important part of a privacy program and ensures everyone keeps going in the right direction. Technology, laws, and the people in your company will change over time. Written policies, standards, and procedures serve to maintain your company's vision and the formation of your privacy program through these various changes.

It is important that documentation be practical. Unreasonably long policies can lend to confusion and frustration, which could lead to the policy being completely ignored. This will defeat the very purpose of the policy in the first place.

## 7. Operationalizing privacy

Determine the mechanisms by which your privacy program will be implemented. For example, if your company is likely to receive a large volume of data requests from customers or consumers, will those data requests be handled by an in-house team, or will this function be outsourced to a vendor? How will privacy education be implemented?

A company should create awareness of its privacy program and develop a communication plan to document privacy plan activity.

## 8. Monitoring privacy

Develop a plan for monitoring your company's privacy plan compliance. Use this plan not as a "gotcha" but an opportunity to compliment colleagues on their privacy compliance. When gaps or incidents of non-compliance are discovered, redirect those responsible so the problem is remediated.

Document the findings of any monitoring program by establishing metrics by which compliance can be measured over time. You may "borrow" controls from established standards such as PCI, DSS, SOX, and/or SOC2, which suit your environment and industry.

Every company that processes personal data should have a strategic privacy program. Programs may vary widely based on industry, the type and amount of personal data at issue, size of the

company, and other factors.

A well-planned privacy program will reduce risk and save a company time and money in the long run.  Most importantly, it will let you sleep better at night!

## Tony Stewart

Chief Legal and Privacy Officer

ParkMobile

Tony Stewart is the Chief Legal and Privacy Officer at ParkMobile.

## Rich Sheinis

Partner

Hall Booth Smith, P.C.

Rich Sheinis is partner and leader of the Data Privacy & Cyber Security Practice at Hall Booth Smith.