Whitepaper published January 7, 2019

Managing Your Personal Privacy Program

Businesses, government agencies, and non-profit organizations are obliged to protect your personal information.

Many of these organizations have tools and processes to fulfill their privacy obligations. Due to the complexity of privacy rights and technology, these obligations are typically managed through a privacy program.

One important principle of a good privacy practice is: *transparency*.

Transparency offers visibility into how organizations protect the privacy rights of individual data subjects.

Programs are designed to achieve general goals, such as privacy, or more specific objectives, like transparency.

Transparency is the idea is that we, as individual data subjects, have the right to see into an organization's tools and processes, so we can know first-hand how our personal data is being governed. However, we don't really see this – all we can see is what an organization reveals in publishing information about their policies and programs.

This whitepaper is intended to help us, as individual data subjects, develop and manage our own privacy programs.

It will be apparent *why* we need our own privacy program, and *what* it should consist of, after offering a transparent glimpse into how organizations run their privacy programs.

Best Case

Leading privacy advocates, auditors, and tool vendors comprise "the top tier" of organizations which have established standards for what good privacy programs consist of. To summarize, a privacy program consists of:

- Policy objectives and standards
- Documentation of tools and processes designed to implement and enforce policy
- Responsibilities assigned to participants and stakeholders for accountibility
- Reporting on how effective the program is in fulfilling its objectives

Your personal privacy program would also have each one of these program components – because, *our strategy for being effective, depends upon organizations' willingness and technical capabilities to agree with our privacy requirements.*

From a pragmatic standpoint, what we really depend upon is successful resolutions between different parties by negotiating *mutual agreements*. For this we need compatibility, alignment, integration, and automation capabilities.

Best Case Test Scenario #1

”PerfectPrivacyCorporation” is a leading vendor of privacy program management software, sold to commercial enterprises, government agencies, non-profit organizations, and auditing firms.

“ProtectedPrivateIndividual” is just an ordinary consumer looking for tools to protect his or her privacy.

Mr. ProtectedPrivateIndividual visits the website of ”PerfectPrivacyCorporation”. He reads the banner that says, “By visiting this site you agree to abide by all the provisions of our privacy policy”.

Unsure of whether this vendor offers what he is looking for, Mr. ProtectedPrivateIndividual wants to download a whitepaper to learn more before spending much time on it, and is confronted with a web form requiring personal data to be submitted. If this was an essential service, like the only water or energy utility serving his area, Mr. ProtectedPrivateIndividual has no choice but to provide whatever data is asked for, whether he has read or has agreed to the privacy policy is essentially meaningless.

This is what happens when individual consumers don’t have their own privacy policy and program: only one party dictates the terms and the party who makes the rules is most likely to prevail in any dispute.

Here is a scenario mock-up for the alternative:

Mr. ProtectedPrivateIndividual visits the website of ”PerfectPrivacyCorporation”. He reads the banner that says, “By visiting this site you agree to abide by all the provisions of our privacy policy”.

Mr. ProtectedPrivateIndividual has a tool that saves a copy of PerfectPrivacyCorporation’s privacy policy and terms of service in a repository. This tool can also send an email to the contact listed in the privacy policy, asking if PerfectPrivacyCorporation would be willing to enter into a mutual privacy agreement.

The privacy team at PerfectPrivacyCorporation responds favorably by replying that they would consider it, but first they need more information about it before they can proceed.

That’s great, because Mr. ProtectedPrivateIndividual has a default policy and a default personal data profile for use in these initial stages of forming a relationship, or when establishing an exchange of information on a pure transactional basis. So his tool automatically responds to PerfectPrivacyCorporation with a link to a website where they can see his default policy and register for access to his default personal data profile. Mr. ProtectedPrivateIndividual receives a notification upon occurrence of this event.

The tool used by Mr. ProtectedPrivateIndividual, is simple to use, but quite sophisticated and powerful. When PerfectPrivacyCorporation downloads his default privacy policy and data profile, aka “contact info”, they also see an automatically-generated draft of a mutual privacy policy: a structured document containing rulesets for specific policy provisions which are common to both parties.

Mr. ProtectedPrivateIndividual has his own privacy policies and his own useful tools to automate these processes, but most important, he has his own *Personal Privacy Program*.

- Policy objectives and standards
- Documentation of tools and processes designed to implement and enforce policy
- Responsibilities assigned to participants and stakeholders for accountability
- Reporting on how effective the program is in fulfilling its objectives

Mr. ProtectedPrivateIndividual’s first privacy policy rule is this:

“The only valid agreements between me as an individual data subject and any organizational entity, are in writing, and explicitly authorized by me.”

[in other words, “just because you say I agree to your policy, does not mean that I actually agree.”]

While some people might argue that this is a totally unreasonable expectation, here is Mr. ProtectedPrivateIndividual’s second privacy policy rule:

“I maintain a copy of every agreement I enter into.”

The third policy rule is:

“I retain the right to monitor and enforce compliance with any privacy policy I agree to.”

There’s no point in having policies which are not enforcable, and this may require scanning a website for changes in cookies and policies, detecting deviations, and pursuing remedies intended to encourage mutual negotiation and settlement of any differences.

Why would any organization agree to these policies?

As it is now, PerfectPrivacyCorporation dictates all the terms, and if someone objects, they don’t have to use PerfectPrivacyCorporation’s service. It’s enough of a burden to answer to regulators and auditors; being accountable to individual data subjects is a *completely unreasonable demand*.

An organization could have millions of users whose personal data must be protected. Organizations don't have the capability to negotiate unique agreements with everyone using their services, and if even they did, it would be prohibitively expensive.

Recall the statement: "*our strategy for being effective, depends upon organizations' willingness and technical capabilities to agree with our privacy requirements.*"

This is similar to the statement: *"There's no point in having policies which are not enforcable…"*

We must be pragmatic about what we're trying to accomplish, if we're really serious about it.

Punitive measures don't work well for individual consumers who lack the leverage required to influence a change in an organization's practices. Carrots are among our best tools for inducing organizations to change their ways.

Best Case Test Scenario #1 – Alternative (continued)

PerfectPrivacyCorporation has entered into a mutual privacy policy agreement with Mr. ProtectedPrivateIndividual.

In exchange, (the carrots):

PerfectPrivacyCorporation no longer collects Mr. ProtectedPrivateIndividual's personal information through insecure and inaccurate webforms over their application exposed to the Internet. Instead, they utilize a cryptographically-secure API service to directly access the data they are entitled to in Mr. ProtectedPrivateIndividual's PII Vault.

PerfectPrivacyCorporation no longer stores Mr. ProtectedPrivateIndividual's personal information in a variety of disparate information silos and applications. Instead, they get his personal information in real-time, a tested technique no different from authenticating a user through a third-party single-sign-on service.

PerfectPrivacyCorporation is no longer the data custodian for maintaining the accuracy of Mr. ProtectedPrivateIndividual's personal information. That's Mr. ProtectedPrivateIndividual's responsibility: he is the data custodian, and when his address or legal name changes, he updates it in his repository and sends notifications to subscribers who opt-in to them.

Mr. ProtectedPrivateIndividual has other means to monitor, detect, and enforce deviations from policy, having established a communications protocol to address issues. This reduces the risk of having complaints filed with regulators or causing other unwanted problems for PerfectPrivacyCorporation. For social media sites, this could potentially support and encourage user communities to police themselves.

These “carrots”, while not used by individual end users, actually do exist today, in the form of Data Processing Agreements, Business Contracts, etc. usually between two organizations within a “Third-Party Risk” context. Automating this process between organizational entities could be done, but currently these are usually executed through time-consuming audits, assessment questionnaires and late-night “redlining” sessions with legal counsel.

Any personal privacy program must work for organizations who *claim* they don’t have sufficient resources to manage it on behalf of their individual consumers (who *really* don’t have the time, the money, and the expertise) to manage their personal privacy rights.

This whitepaper is a starting point for re-imagining how privacy rights could be protected. Over the upcoming months, additional whitepapers will be published on different tools and techniques that individuals can use to “operationalize” their policies. Privacy can get quite complex. Without effective tools, no privacy policy can be implemented and enforced.

PrivacyPortfolio offers services designed to assist you in establishing and maintaining a privacy rights program. We are committed to providing our tools free of charge as open source projects based on industry standards to facilitate adoption. If you establish a program to protect your privacy rights, you can choose whatever tool or method that supports or fulfills your objectives. The program governs how and when you will use such tools. It is our hope and vision that we can inspire others to do better, providing individual data subjects with the best privacy rights technology the world has to offer.