Automated Privacy Compliance Auditing as a Service (DRAFT)

Benjamin J. Anderson

University of Wisconsin - Stephens Point

Stephens Point, Wisconsin

A Thesis Submitted in Fulfillment of the Requirements for the Degree Of

MASTER OF SCIENCE

in Data Science

December 2020

For my wife and son.

Contents

1 Executive Summary

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum (Anderson, 1983).

2 General Company Description

Cereus is a software-as-a-service company offering privacy compliance auditing tools and solutions for businesses that collect customer information through their websites.

2.1 Unique Value Proposition

Consent involves more than just cookies on your website. It involves all information you share with your vendors and partners including network traffic. Cereus actively scans, monitors, and analyzes your website to identify compliance infringements in accordance with your business rules.

2.2 Mission Statement

To remove privacy barriers between companies and their partners, and enable them to communicate in an efficient, compliant way.

2.3 Vision Statement

Proactively detect all privacy compliance infringements defined by our clients before they reach their customers.

2.4 Values Statement

- Reliability

- Transparency

- Growth

2.5 Company Goals and Objectives

Our primary goal is to establish ourselves as a thriving company that leads the privacy industry by providing automated, insightful, audits to ensure that companies and their partners are sharing customer information in accordance to their business rules.

2.6 Business Philosophy

Some companies spend millions to establish a privacy program. Everyone else gets Cereus.

2.7 Industry Overview

The privacy technology industry is a rapidly growing field. In 2020, it is the fastest growing technology sector that includes the fastest growing company in the U.S (Hughes, 2020). As more consumers become impacted by massive data breaches in which sensitive, personally identifying information (PII), is exposed; consumer awareness and the call for data processing regulations are expected to be on the rise.

There are already governmental regulations impacting businesses in the U.S. The Health Insurance Portability and Accountability Act (HIPAA) highly regulates patient information and how it is stored (Centers for Disease Control and Prevention, 2018). The California Privacy Protection Act (CCPA) regulates the selling of user data collected by a business for consumers in the state of California (California Legislature, 2018). The Children's Online Privacy Protection Act (COPPA) imposes requirements on website operators on collecting information from children under the age of 13 years old (FTC, 1993). Lastly, the General Data Protection Regulation (GDPR) gives European Union citizens the right to manage their information any business has collected on them and requires explicit consent before information is collected (Council of the European Union, 2018).

With all these regulations, foreign and domestic, companies that collect information from their customers are relying on the assistance of privacy technologies to operate within the bounds of new regulations and meet consumer privacy expectations (Meehan, 2019). This has attracted massive funding, and, in July of 2019, OneTrust raised $200 million in a Series A investment, TrustArc raised $70 million Series D, Privitar raised $40 million series B, and BigID raised $30 million Series B (Wood, 2019).

In four years since its founding, as of August, 2020, OneTrust is valued at $2.7 billion (Hughes, 2020).

2.8 Market Segment Overview

Any business that operates a website and collects data and analytics on their customers is subject to the regulations in which the customer originates. This also applies to the jurisdiction in which the business operates. Cereus can provide auditing for companies with a single website, to large enterprises with hundreds. It may prove difficult for small businesses with a single website to justify the expense of privacy audits when they are not often the subject of privacy lawsuits (LaNou, 2020). Our primary focus will be medium to large organizations maintaining multiple websites.

2.9 Legal Form of Ownership

Cereus will be organized as a small business corporation (S corporation). As an S corporation, we will be allowed to collect funding and pass off any business profits and expenses to its shareholders without the additional taxes applied to C corporations.

2.10 Guiding Principles

The "Living Principles for Design" framework (Hamlett, 2020) was applied to outline how Cereus can maintain a sustainable design while achieving our objectives along the following dimensions:

2.10.1 Environment

The direct environmental impact of Cereus is expected to be minimal. We will provide software-as-a-service (SAAS) and will rely on cloud services to manage our operations. Cloud services, such as Amazon Web Services (AWS), are composed of large computer networks in which infrastructure is shared with other AWS customers (Amazon, 2020). Our physical hardware is limited to the machines required to manage services running on the cloud platforms.

With Cereus's services operating in the cloud, a central office space for employees is not required and will further reduce the company's environmental impact.

2.10.2 People

The societal impact of our company and its services are restricted to the transparency of the companies that use it. We offer detailed reports from our audits that can provide insights into how customer information is shared between a website and its partners. If companies choose to share these reports, their customers will better understand how their information is used in exchange for the services the company provides. This has the potential to improve the relationship between a company and their customers – possibly making them more apt to sharing personally identifying information.

2.10.3 Economy

Cereus's operations are expected to reduce the amount of time required to conduct a compliance audit against websites. These actions will minimize the manual auditing cost and likelihood of our customers being subject to privacy lawsuits. Our customers can then focus and dedicate more resources towards achieving their goals and growing their business. Our

overall economic impact is limited to the the actions of our customers and is expected to be minimal.

2.10.4 Culture

Cereus has the potential to influence organizations to be more transparent about the sharing of information on their customers with their partners. Traditionally, data processing and sharing are often confidential and kept internal; but with privacy becoming a concern for consumer – transparency will soon be an expectation (Meehan, 2019).

3 Products and Services

3.1 Description of Products and Services

Cereus aims to become the leader in cutting-edge privacy compliance auditing tools. These tools will assist our customers to quickly and efficiently identify privacy and compliance issues on their websites. Most of our products will be offered as software-as-a-service with additional professional services also being made available.

3.1.1 Compliance Auditing

The Cereus compliance auditing system is a series of rules and processes configured by the user to ensure their websites meet the compliance standards that they have defined. It can be configured to scan websites during the businesses development cycle, automatically through the API services, or manually through the our user interface. There are five main components to the compliance auditing system: the confirmation system, crawler, rules engine, report, and recommendation engine.

3.1.1.1 Confirmation System

The Cereus confirmation system, Figure 3.1, prevents organizations from conducting audits on domains that they do not own or manage. This ensures that our customers cannot use the auditor to evaluate their competitors websites and privacy practices. When a new property (website) is added through the user interface, the user will be guided through a series of processes to confirm ownership of the domain before allowing an audit to be conducted. This process is dependent on the plan the customer is subscribed to. Any attempt to scan an unconfirmed domain will be rejected.

The free tier is a highly restricted plan that limits the capabilities of the auditor. This tier is intended for small business owners running a single website with limited content. For the initial confirmation of ownership of the domain, free tier users will be required to own an email address associated with the domain they are requesting to audit. In many instances, an email such as "webadmin@example.com" are dedicated to the management of the domain. Once the customer creates the property in our user interface, they can then request a validation email be sent to their inbox with a confirmation link. When confirmed, the customer will be provided an HTML metadata tag to be included on the pages they would like to be scanned.

In the event the property on the free tier expires or is sold, Cereus will no longer be able to audit the website due to the metadata tags not being present on the site.
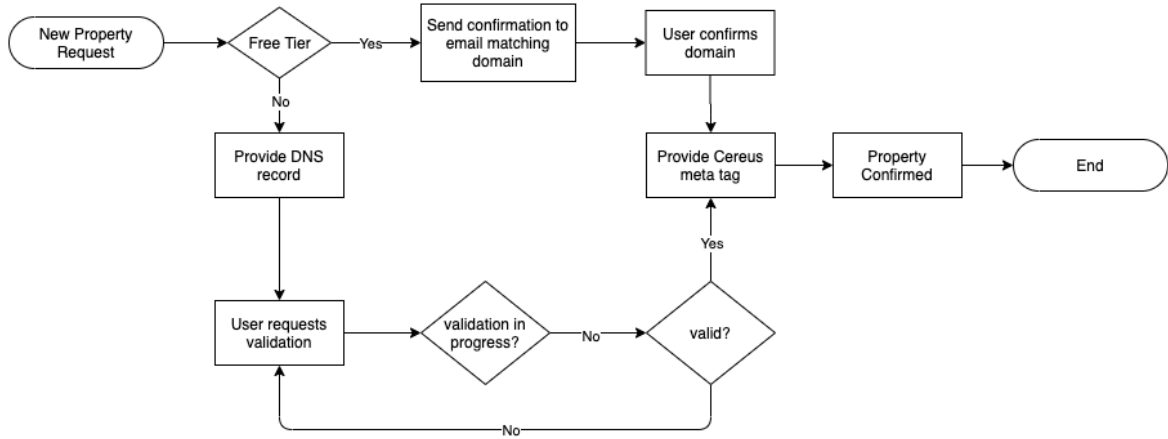
Figure 3.1: Property confirmation system - The Cereus website confirmation system to ensure the organization owns the domain prior to scanning.

All additional tiers offer unrestricted access to our services available in the tier. Our services can provide insights into the privacy operations of the company, so additional confirmation steps are required. To confirm ownership of the property, a TXT DNS record defined by our systems will be provided to the client. In the event a domain is acquired by a new party, through the sale or expiration of the domain, we will lock access to previous reports and disable auditing services when the TXT DNS record is no longer present. The initial client who set up the domain in Cereus will be notified of the change and can re-validate if the DNS record was removed by mistake.

3.1.1.2 Crawler

The Cereus crawler is a highly intelligent and configurable service that uses artificial intelligence to scan, monitor and classify information from validated websites. This includes all network traffic, cookies set on the page, call-trace information, performance data, request type, response status codes, headers, and redirect flags. This data is then processed by our rules validator and aggregated by the report generator. Our recommendation engine will then suggest what actions should or must be taken to bring the website back into compliance. Unlike our competitors, this includes the exact line and position of code where the non-compliance occurred.

Configuration

The crawler can be configured in a variety of ways to meeting an organization's auditing and compliance needs. From a set or random schedule, organizations can ensure their publicly accessible website are scanned on regular basis to ensure compliance and to verify the websites

are only updated through approved channels. Once the data has been processed by the rules validator and the report has been generated, the customer will receive an email notification with the audit report. Audits may also be conducted manually by a user through the Cereus user interface or triggered through the API services.

Our customers may also specify a geographic location for which the crawler will originate from. Depending on the geographic location of the visitor, privacy regulations can differ and the company may apply a different set of business rules. Running the crawler in a targeted geographic location allows our customers to validate their website's behaviors.

Actions

In many instances, features of a website may require an authorized user or action to be taken in order for functionality to trigger. Our customers can specify actions the crawler can take in order to trigger the specified site functionality. This includes clicking the specified components, scrolling, or waiting for an event to trigger.

Data Extraction and Transformation

The network and cookie data are extracted in a semi-structured format that can be translated to a flat SQL tables for processing by the report generator. Data received by the proxy server can be consolidated with debug information sent by the browser. Figure 3.2 outlines the data collection and transformation process.

The crawler captures the requested URL for users to construct rules on the domains, locations, and query parameter. The requested URL is broken down into the requested protocol, domain, path, query, and location hash. This fragmentation significantly reduces the amount of processing required by the rules and recommendation engines. It also allows our customers to optimize their reports by establishing aggregation or exclusion rules based on part of the URL. In the instance data is sent to the server, for example, in a POST request: the data is converted to a HashMap and stored as JSON in the metadata column.

All request and response header information, depending on the browser meta event, is formatted as JSON and stored in the headers column. Signals such as the Do Not Track header signal (DNT) can be sent from the browser to indicate that the user would prefer privacy rather than personalized content (Mozilla, 2020). Site partners may respond to the DNT header, or some other setting, that the customer can monitor with the Cereus rules engine.

Figure 3.2: Crawler data transformation - The extraction and transformation of data received by the Cereus crawler.

3.1.1.3 Rules Engine

Our customers have the option to establish rules associated with a network request or cookie to determine whether or not they meet compliance standards. These rules can be configured to target specific geographic location to determine if an entire URL, domain, protocol, query path, or parameter, based on the specified condition, meets compliance expectations (Figure 3.3).

Multiple conditions may be applied to a single URL or cookie as an OR conditional. Rules may also be grouped to establish an AND conditional between two or more rules. Cereus's rules engine supports matches for values that: contain a value, equal a value, does not contain a value, does not equal a value, or whether or not the value matches a regular expression. Based on specified conditions, the user can specify whether or not to flag the request as compliant or not.

Figure 3.3: Rules definition interface - The Cereus rules engine can be configured to determine whether or not a request meets compliance standards based on the conditions specified by the user.

These rules, by default, are set at an organizational scope. All properties under the organization, when the rules engine processes a crawl, will have the same rules applied. Rules may also be overrode at a property level when exclusions are needed.

3.1.1.4 Reporting

Once processed by our proprietary Artificial Intelligence and patent-pending algorithms, the Cereus audit provides insights into the requests made on the site. This incorporates the response status code, the type, size of the information exchanged, the amount of time for the request to complete, and whether or not the request met compliance expectations (Figure 3.4). Any information that has no data or rules associated with it appears as a question mark (?) icon.

Each row can be broken down to dive into the information associated with the request. The deep dive includes the headers associated with the request, a cache of the original rules

associated with the request (and their validation status), query parameters, data sent to the server, cookies, and the initialization chain. Web administrators and compliance managers will be able to quickly reference the audit report and identify where the compliance infringement originated.

The report filters can be used to dynamically query information from it. Users can check for specific URLs, whether or not requests were compliant, the associated category with a URL, or the page in which the information was found. Our customers will receive a notification when the audit identifies requests out of compliance and can use the filter functionality to quickly pull up the request and rules information.

3.1.1.5 Recommendation Engine

Cereus can make suggestions for requests and cookies that have yet to be classified by the organization. This classification system is powered by the categorizations of requests and cookies by other organizations. The system will also crawl the domains, paths, and cookie hosts to grab meta information to improve the accuracy of the recommendations. A risk score will also be assigned to the requests and cookies based on whether or not other organizations have flagged it as necessary to their operations.

Risk Score

When a new request or cookie is identified on a website, through an initial or later scan, an associated risk score with allowing it to load in a list of geographic locations. This score is merely a suggestion based on the operations of other organizations and no action needs to be taken.

$$s_{risk} = \frac{r_n}{O_r}$$

The risk score is computed as the number of records classified as necessary r_n divided by the number of organizations in which r_n is found (O_r). This will always result in a ratio between 0 and 1 in which intervals of $\frac{1}{3}$ will determine if the request will be rated as: low, intermediate, or high risk.

To reduce the possibility of organizations incorrectly flagging a request due to the scoring system, the risk score will only be provided when a sample size of at least 20 organizations have classified the request or cookie.

Categorization Recommendation

Cereus will provide categorization recommendations for requests and cookies based on meta information extracted from the request or cookie's origin. The recommendation engine will
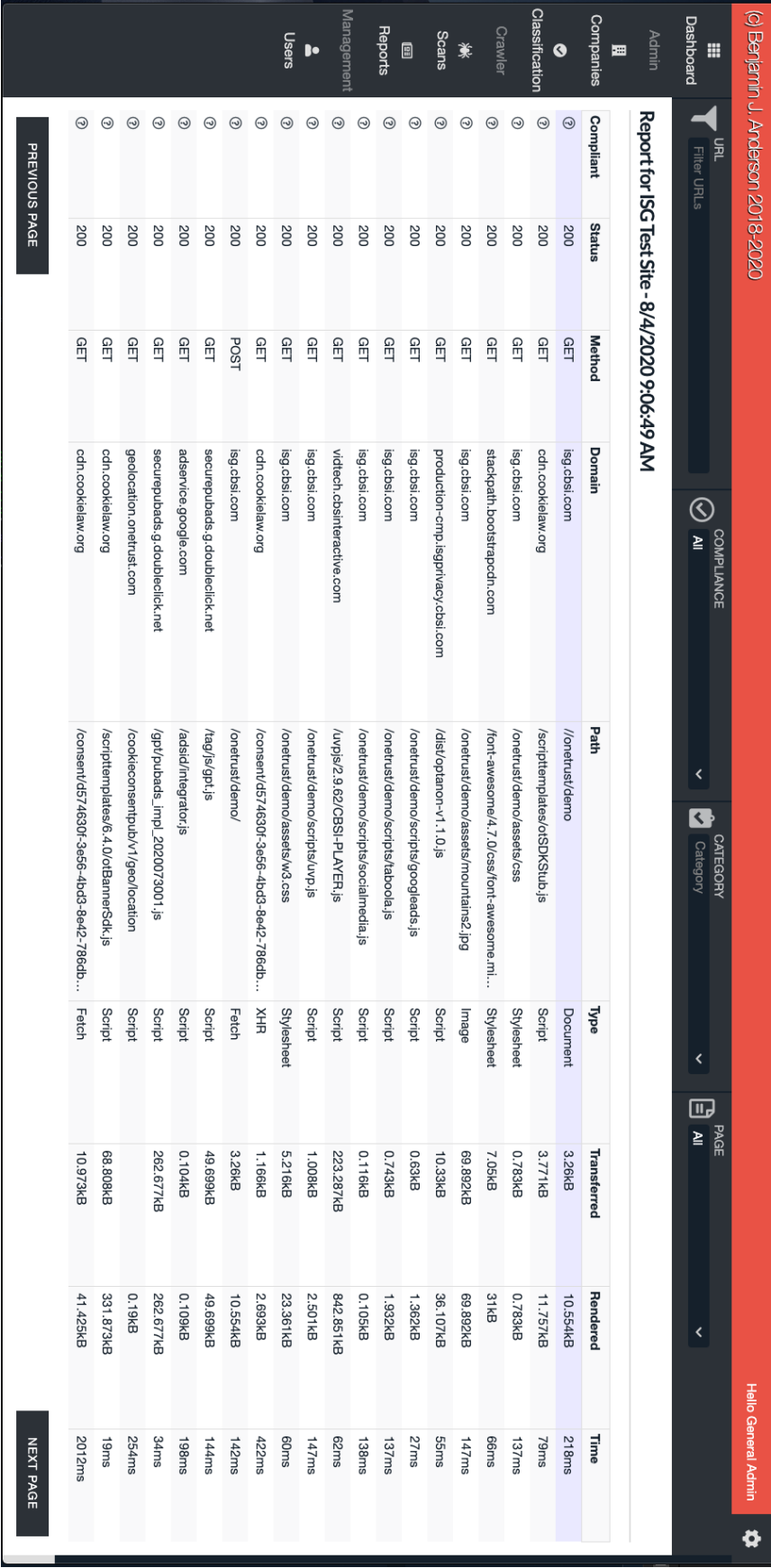
Dashboard
Admin

Companies
Classification
Crawler
Scans
Reports
Management
Users

URL — Filter URLs
COMPLIANCE — All
CATEGORY — Category
PAGE — All

Hello General Admin

Report for ISG Test Site - 8/4/2020 9:06:49 AM

Compliant	Status	Method	Domain	Path	Type	Transferred	Rendered	Time
✓	200	GET	isg.cbsi.com	//onetrust/demo	Document	3.26kB	10.554kB	218ms
✓	200	GET	cdn.cookielaw.org	/scripttemplates/otSDKStub.js	Script	3.771kB	11.757kB	79ms
✓	200	GET	isg.cbsi.com	/onetrust/demo/assets/css	Stylesheet	0.783kB	0.783kB	137ms
✓	200	GET	stackpath.bootstrapcdn.com	/font-awesome/4.7.0/css/font-awesome.mi...	Stylesheet	7.05kB	31kB	66ms
✓	200	GET	isg.cbsi.com	/onetrust/demo/assets/mountains2.jpg	Image	69.892kB	69.892kB	147ms
✓	200	GET	production-cmp.isgprivacy.cbsi.com	/dist/optanon-v1.1.0.js	Script	10.33kB	36.107kB	55ms
✓	200	GET	isg.cbsi.com	/onetrust/demo/scripts/googleads.js	Script	0.63kB	1.362kB	27ms
✓	200	GET	isg.cbsi.com	/onetrust/demo/scripts/taboola.js	Script	0.743kB	1.932kB	137ms
✓	200	GET	isg.cbsi.com	/onetrust/demo/scripts/socialmedia.js	Script	0.116kB	0.105kB	138ms
✓	200	GET	vidtech.cbsinteractive.com	/uvpjs/2.9.62/CBSI-PLAYER.js	Script	223.287kB	842.851kB	62ms
✓	200	GET	isg.cbsi.com	/onetrust/demo/scripts/uvp.js	Script	1.008kB	2.501kB	147ms
✓	200	GET	isg.cbsi.com	/onetrust/demo/assets/w3.css	Stylesheet	5.216kB	23.361kB	60ms
✓	200	GET	cdn.cookielaw.org	/consent/d5746630f-3e56-4bd3-8e42-786db...	XHR	1.166kB	2.693kB	422ms
✓	200	GET	isg.cbsi.com	/onetrust/demo/	Fetch	3.26kB	10.554kB	142ms
✓	200	POST	isg.cbsi.com	/tag/js/gpt.js	Script	49.699kB	49.699kB	144ms
✓	200	GET	adservice.google.com	/adsid/integrator.js	Script	0.104kB	0.109kB	198ms
✓	200	GET	securepubads.g.doubleclick.net	/gpt/pubads_impl_2020073001.js	Script	262.677kB	262.677kB	34ms
✓	200	GET	geolocation.onetrust.com	/cookieconsentpub/v1/geo/location	Script	0.19kB	0.19kB	254ms
✓	200	GET	cdn.cookielaw.org	/scripttemplates/6.4.0/otBannerSdk.js	Script	68.808kB	331.873kB	19ms
✓	200	GET	cdn.cookielaw.org	/consent/d5746630f-3e56-4bd3-8e42-786db...	Fetch	10.973kB	41.425kB	2012ms

PREVIOUS PAGE   NEXT PAGE

Figure 3.4: Cereus audit report - The Cereus audit report provides clean, familiar, interface for privacy compliance teams.

also incorporate organization classification information pertaining to the request or cookie. Classification within Cereus's internal systems are expected to be single words or small phrases, much like meta tag information present on a web page. This information can best be represented as a bag of words. There's no context to meta tag data or the collection of classifications entered by users, so the representation of language or order has no meaning (Manning, 2008).

The recommendation engine is powered by a Bernoulli document model. The model takes a document and partitions it into a feature vector of binary elements. If a word is found in the document, it will receive a value of 1, otherwise 0. It does not take into account the frequency of a word, but whether or not the word is present. The model can then calculate the probability of a word occurring in a document with a specific classification, as well as taking into account the probability of it not occurring.

To save reduce the computational power required to provide recommendations, the model calculates estimated probabilities for a request or cookie belonging to a category.

$\hat{P}(w_t|C_k)$ defines the estimated probability that the word w_i occurs in a document, D, with the classification (C) k. The estimated probability that the word w_i not occurring is $1 - \hat{P}(w_i|C_k)$. V represents the model's vocabulary and v consists of the feature vector of the document. The product of the probability of each item (i) in the feature vector occurring or not occurring determines the overall estimated probability of the document being classified as class k $(\hat{P}(v|C_k))$.

$$\hat{P}(D|C_k) = \prod_{i=1}^{V}[v_i\hat{P}(w_i|C_k) + (1 - v_i)(1 - \hat{P}(w_i|C_k))]$$

There are two parameters for this model: the probabilities of each word in the document class $(\hat{P}(w_i|C_k))$ and its prior probabilities $P(C_k)$. The estimated probability that a word w_i occurs in a document is the number of documents n classified as k divided by the total number of documents N classified as k.

$$\hat{P}(w_i|C_k) = \frac{n_k(w_i)}{N_k}$$

Where the prior probability of class k can be estimated as the relative frequency of documents containing class k.

$$\hat{P}(C_k) = \frac{N_k}{N}$$

The output of the model will be an array of estimated probabilities. Each probability in the array is associated with a category defined within Cereus's system. The category with the highest probability is recommended to the user.

3.1.2 Notifications and Alarms

Users can configure Cereus to notify the specified stakeholders in the event that an audit discovers new requests or cookies, compliance checks fail, or when a new scan is scheduled. To reduce the likelihood of users ignoring these notifications, they can be configured on an organizational level or per property. These settings ensure that notifications are sent only to the significant parties and reduce email clutter.

3.1.3 API Services

Professional and Enterprise customers may use Cereus's application programming interface (API) services to automate their privacy operations. Our customers who actively curate new content, use a continuous integration (CI) system to control website deployments, or those who may not follow a strict deployment schedule can use the API to integrate Cereus into their daily business processes.

Crawl Requests

The crawl request endpoint allows customers to trigger a crawl against a property. By default, this will scan all paths defined on the property. Our customers also have the option to specify the path(s) they would like to crawl in the event they want to target only new or updated pages.

Web Hooks

When an audit has completed, it will notify stakeholders stating whether or not compliance checks were successful. Cereus can also notify other computer systems. Through web hooks, our customers are able to configure Cereus to send audit status messages to their computer systems. The customer can then process the message and take action against the messages.

3.1.4 Professional Services

Our professional services will serve a clientele requiring guidance on privacy regulations applicable to their operations. We will consult the client to identify the best plan for the client and assist with the configuration of our tools to reflect their needs. Training services for Cereus's products will also be offered.

3.2 Competitive Advantages and Disadvantages

The privacy industry, though relatively new, already consists of some large organizations servicing a significant amount of the market share. In April of 2020, OneTrust had a 35.5%

stake in the data privacy management software market (OneTrust, 2020). We intend to enter the privacy software market by automating an otherwise manual process: compliance auditing.

3.2.1 Competitive Advantages

1. **Founders are experienced software engineers**

   Cereus's founders are experienced software engineers. Providing software-as-a-service requires the software to be developed, maintained, and readily available. Cereus's founders will be able to construct its systems to be scalable and maintainable to accompany organizations of any size.

2. **Founders are experienced product managers**

   Cereus's founders are experienced product managers. The founders are able to clearly define Cereus's product vision and prioritize feature requests to meet customer requirements.

3. **Founders have a background in data science**

   Cereus's founders have a background in data science. Cereus will collect, process, and store large amounts of information for their customers. When large datasets come into play, storage costs, data integrity and performance issues are common. With a formal background in data science, Cereus's founders are able to mitigate all of these problems.

4. **Cereus provides actor stack traces**

   In the event a request or cookie fails to meet company compliance standards, Cereus provides stack trace information that allows the user to locate the file and exact line of code that triggered the validation failure. This saves the company time and money from having to manually trace the source.

5. **Cereus extends cookie compliance**

   In addition the industry standard of cookie compliance (user consent is required only for cookie tracking), Cereus also provides insights into network requests. This provides a full-scope audit of the website and how information is shared between it and its partners.

3.2.2 Competitive Disadvantages

1. **Cereus is not a consent management platform**

   Cereus does not provide consent management services for its customers; it augments existing consent management platforms and solutions. Cereus's customers will need to purchase a consent management solution or implement their own.

2. **Adoption requires legal support**

   Tools used to automate legal compliance often require privacy attorneys to validate whether or not the tools are effective (Merken, 2019). Cereus will require legal support in order for companies to adopt its services.

3.3 Pricing Structure

We aim to serve medium to large-sized organizations managing multiple websites. We do, however, offer a flexible pricing structure, including a free tier, to accommodate companies of any size. Table 3.1 provides an overview of each tier and services provided.

3.3.1 Free

We offer our auditing services, with limitations, for free. Free-tier users are authorized to register one website but will not be able to benefit from the company's API, web hook, recommendation, notification, or professional services. They are limited to running 10 audits per year against a running total of 12 pages.

3.3.2 Personal

The Personal tier enhances the Free tier by incorporating our notification system into the audit process. It expands auditing to five pages of the customer's website once per month. The recommendation engine will further assist our customers by offering insights into the categorization of requests and cookies found in the audit. One user may be set up to access the organization's information within Cereus.

   This is a monthly subscription that can be canceled at any time.

3.3.3 Professional

The Professional tier provisions up to five users to be set up to access the organization's information within our systems. It expands the Personal tier to allow the our customers to register up to five of their websites. Each website can have up to ten pages audited twice a

month with the option to integrate web hooks into their auditing processes. Our professional services are also offered for an additional fee.

This is a monthly subscription that can be canceled at any time. A yearly subscription is also available at a 5% discount.

3.3.4 Enterprise

Enterprise customers have access to all of our services in addition to 40 hours of professional services per year. The option to have the auditor crawl a sitemap as opposed to manually defining pages, with a limit of 100 pages, is available. 25 websites can be registered and audited up to 4 times a month. 25 users may be set up to access the organization's information.

This is a yearly subscription that cannot be canceled.

3.3.5 Select

There is no one-size fits all pricing model that fits every customer's needs. Our Select tier offers customers the ability to tailor a customized experience at a fixed, yearly, rate.

3.4 Industry Background

With new governmental regulations, data breaches, fines, and growing awareness of how personal data is collected and processed, the privacy technology industry is growing rapidly – with one company being valued at over $2.7 billion after being founded only 4 years since its valuation (Hughes, 2020). With rising successes of privacy software vendors, we also see large data collection and processing companies being hit with record-breaking fines. In 2019, the FTC fined Facebook $5 billion and imposed strict privacy restrictions (FTC, 2019). This set a new precedent that all companies are accountable for the decisions they make about their users' privacy.

As customers are becoming more aware and passionate about what companies are doing with their data, the need for privacy technology is expected to continue to grow (Meehan, 2019). Governmental regulations will continue to focus on making companies accountable for the data they collect and require them to follow various guidelines. In instances where the regulations are too complicated for companies to implement or manage on their own, privacy vendors can step in and assist.

Tier	Subscription	Price	Users	Websites	Pages	Scans/Mo	Prof.Services	API	Web hooks	Notifi.	Rec.
Free	Monthly	$0.00	1	1	1	1	✗	✗	✗	✗	✗
Personal	Monthly	TODO	1	1	5	1	✗	✗	✗	✗	✗
Professional	Monthly	TODO	5	5	25	2	Additional	✗	✓	✓	✓
Enterprise	Yearly	TODO	25	25	100	4	✓	✓	✓	✓	✓
Select	Yearly	Custom	N	N	N	N	Opt.	Opt.	Opt.	Opt.	Opt.

Table 3.1: Cereus pricing tier and services provided.

3.5 Target Market Segment

At Cereus, we offer flexible subscriptions for any sized organization that's looking for privacy compliance auditing. It may, however, be difficult to market smaller companies that our services are worth mitigating the risk of being fined. We will focus our marketing efforts towards medium-to-large organizations, with multiple websites, who are currently, or will be, working with a consent management system.

Medium-to-large organizations will often attract a larger, more diverse, customer base. Their customers determine the privacy regulations the company has to adhere to. As a company grows, collects, and process more information, it may attract the attention of customers or governmental agencies – making the company more subject to fines or legal action should they be found out of compliance. With more regulations, our customers would have to dedicate resources towards manually auditing their websites for each regulation to mitigate the risk of lawsuits or fines. At Cereus, we automate this process and follow the rules defined by our customers without any margin of error, making our costs more justifiable in contrast to smaller companies.

4 Marketing Plan

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.1 Industry Background

4.1.1 Market Size

According to QY Research, North America and Europe are currently holding the largest share for the privacy management software market (QY Research, 2020). In 2019, this market size was estimated at a US $808.8 million and estimated to reach a US $6.1 billion by the end of 2026 with a compound annual growth rate of 33.1% from 2021 through 2026. These estimates were based on privacy management software trends in North America, Europe, China, Southeast Asia, India, and Central and South America.

4.1.2 Market Trends

With the passing of the General Data Protection Regulation (GDPR) for European Union citizens and large data breaches exposing the personal information of hundreds of millions of consumers, privacy awareness has led to the passing of privacy regulations across an increasing amount of countries (PrivacyPolicies, 2019). Since the passing of GDPR, Brazil, Canada, Australia, and various U.S. states have enacted, or began enforcing, their privacy laws with heftier fines or sanctions. The primary difference between regulations being passed now, in contrast to the past, are the heavy fines and sanctions regulators can impose on companies who are non-compliant (Matteson, 2020). These sanctions and fines are designed to force businesses to comply with regulations and how they process their customers information.

In a survey conducted by Auxier, Rainie, Anderson, Perrin, Kumar, and Tuner, 62% of Americans believe it is not possible to go through daily life without having their data collected, 81% believe that they have very little to no control over their information companies collect about them, and 72% feel that all, or almost all of what they do online is being tracked (Auxier, 2019). The survey also revealed that most Americans are not confident that companies would publicly admit to misusing their customers data, but still say data collection and usage is acceptable for processing in some ways.

4.1.3 Growth Potential and Opportunity

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.1.4 Market Barriers

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.1.5 Market Changes

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.2 Products and Services

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.2.1 Auditor and Reporting

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Unique Selling Proposition

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Features and Benefits

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.2.2 Notifications and Alarms

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Unique Selling Proposition

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Features and Benefits

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.2.3   Rules Engine

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Unique Selling Proposition

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Features and Benefits

4.2.4   Classification and Recommendation Engine

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Unique Selling Proposition

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Features and Benefits

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.2.5   API

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Unique Selling Proposition

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Features and Benefits

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.2.6   Professional Services

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Unique Selling Proposition

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Features and Benefits

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.3   Customers

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.4   Proposed Location

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.5   Pricing and Positioning Strategy

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.5.1   Operational Costs

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.5.2 Competitive Analysis

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.5.3 Return on Investment

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.6 Sales and Distribution

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.6.1 Sales Strategy

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.6.2 Distribution Methods

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.6.3 Transaction Process

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.7 Advertising and Promotion

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.7.1 Advertising

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.7.2 Sales Promotion

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.7.3 Publicity

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

4.7.4 Web

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

List of Figures

References

Amazon. (2020). *What is aws.* Retrieved 2020-09-23, from `https://aws.amazon.com/what-is-aws/`

Anderson, J. R. (1983). *The architecture of cognition.* Mahwah, New Jersey: Lawrence Erlbaum Associates.

Auxier, B. (2019, 11 15). *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information.* Retrieved from `https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/`

California Legislature. (2018, 09 24). Retrieved 2020-09-30, from `https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121`

Centers for Disease Control and Prevention. (2018, 09 14). Retrieved 2020-09-30, from `https://www.cdc.gov/phlp/publications/topic/hipaa.html`

Council of the European Union. (2018, 05 23). Retrieved 2020-09-30, from `https://gdpr-info.eu/`

FTC. (1993, 04 27). Retrieved 2020-09-30, from `https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule`

FTC. (2019, 07 24). *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook.* Retrieved from `https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions`

Hamlett, P. (2020). *Your roadmap for sustainable design.* Retrieved 2020-09-23, from `https://www.aiga.org/roadmap/`

Hughes, J. T. (2020, 08 12). *Reflecting on the growth of the privacy industry.* Retrieved 2020-09-23, from `https://iapp.org/news/a/reflecting-on-the-growth-of-the-privacy-industry/`

LaNou, C. (2020, 09 22). Personal interview.

Manning, C. D. (2008). *Introduction to information retrieval.* Cambridge University Press.

Matteson, S. (2020, 01 29). *Data privacy: Top trends to watch in 2020.* Retrieved from `https://www.techrepublic.com/article/data-privacy-top-trends-to-watch-in-2020/`

Meehan, M. (2019, 11 26). *Data privacy will be the most important issue in the next decade.* Retrieved 2020-09-23, from `https://www.forbes.com/sites/marymeehan/2019/11/26/data-privacy-will-be-the-most-important-issue-in-the-next-decade/`

Merken, S. (2019, 08 12). *Companies turning to tech vendors for privacy compliance tools.* Retrieved from `https://news.bloomberglaw.com/privacy-and-data-security/companies-turning-to-tech-vendors-for-privacy-compliance-tools`

Mozilla. (2020, 05 21). Retrieved 2020-09-27, from `https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/DNT`

OneTrust. (2020, 05 27). *Idc releases first worldwide data privacy management software market shares report.* Retrieved from `https://www.onetrust.com/idc-releases-first-worldwide-data-privacy-management-software-market-shares-report/`

PrivacyPolicies. (2019, 09 04). *What's Data Privacy Law In Your Country?* Retrieved from `https://www.privacypolicies.com/blog/privacy-law-by-country`

QY Research. (2020, 01 14). *Global Privacy Management Software Market Size, Status and Forecast 2020-2026.*

Wood, N. (2019, 05 11). *New privacy tech industry attracts massive funding.* Retrieved 2020-09-23, from `https://fpf.org/2019/07/11/new-privacy-tech-industry-attracts-massive-funding/`