[DRAFT] — Hush Line: A Cross-Industry, Open-Source Whistleblowing Platform For Organizations and Individuals

A Flexible Product Suite That Meets Users Where They Are

Glenn Sorrentino

2024-08-01

Abstract

A whistleblower is an insider to an organization who exposes evidence of wrongdoing to authorities or the press with the intention of reforming it [1]. Not just an activity for exposing National Security secrets, whistleblowing can help make schools safer, businesses more compliant and ethical, and journalists more informed.

Disclosing secrets is vitally important and simultaneously one of the most dangerous things an individual can do, especially in the context of government and national security secrets. People who leak information often go into it without a plan, leading to exile, imprisonment, and even death. To protect against the discovery of someone leaking documents, many tools available today offer Tor-only solutions – meaning the tools they use to upload documents are only accessible through special software providing anonymizing connections to the internet. While an essential piece of the puzzle, requiring someone to download software that could make them look suspicious as the only way to share information is a non-starter, especially for people in countries where internet freedoms are restricted.

But what about the students who need to have a safe way to report information to educators about school safety, teacher misconduct, or struggles at home? Or the businesses that need methods for employees to report information that could lead to legal liabilities, including SEC violations or other lawsuits, without risking their careers and livelihoods? Or journalists who need an easy and safe way to receive infor-

mation without requiring the public to learn a new esoteric technology?

In this paper, we'll see how Hush Line can meet all threat models, from nation-states to neighborhoods, by providing a centralized service that is both usable by non-technical individuals and also highly resilient to censorship and surveillance.

Contents

1. Introduction

Most people will witness workplace harassment or discrimination, yet very few will speak up [2]. The fear of retaliation creates a chilling effect that enables bad behavior that could lead to SEC violations or other legal risks for the company. In schools, students today have to go through active shooter drills and worry about gun violence, yet are afraid to speak up if it'll risk their reputation. And the business of journalism is changing, with budgets shrinking by 25% over the last decade [3]. How too should our tools evolve?

In this paper, we present Hush Line, a new managed whistleblowing platform designed with usability, accessibility, privacy, and security in mind. Hush Line is designed to be a managed service, meaning anyone can come to the platform at https://hushline.app, create an account without providing any personally identifying information (PII), and have an anonymous tip line. Where others require specialized infrastructure to manage a tip line, Hush Line does this for you so that you can focus on the mission, not the machines.

One of Hush Line's strengths is its flexibility, deploying to both a clearweb address (https://hushline.app) and a Tor Onion Service (http://j5kv5…7g2ad.onion) for users who require advanced levels of anonymity. If, for example, a journalist only needs a Tor-only option, they may choose to never disclose our clearweb address to their audience and only share their onion address (http://j5kv5…7g2ad.onion/tips/submit_message/artvandelay). And for the cases where it is critical to offer an address reachable by regular browsers - Firefox, Sarafi, Chrome - a user may choose to only share the clearweb URL (https://hushline.app/tips/submit_message/artvandelay).

For users who do need complete control of their infrastructure, we offer a

product called the Hush Line Personal Server, a physical device that runs your own instance of the Hush Line platform and deploys as a Tor-only service. For those who want to host the Hush Line platform on their own infrastructure, we provide an official package of the software on the GitHub Container Registry [4]. Our product is free and open-source for those who want even more control of the code, allowing anyone to copy and modify it for their needs.

To understand our target audiences' needs and requirements, we interviewed former whistleblowers, lawyers specializing in whistleblowing law, journalists, educators, and business owners. In addition, we also ran a beta program for approximately six months to test an early prototype of the platform with real users and to gather first-hand feedback. During the beta period, we identified and successfully addressed vulnerabilities in the prototype with the community's support, leading to a stronger production application. We spoke to authors of previous research papers, former whistleblowers, and lawyers specializing in whistleblower law.

Hush Line will serve as a product that meets users' needs across threat models and use cases. We remove the need for technical proficiency or complex requirements and offer a platform and interaction model that people are already familiar with. We hope this approach, which focuses on usability, accessibility, privacy, and security will lead to a more informed public, safer schools, and more ethical businesses.

2. Background

2.1 The Problems We're Solving

2.1.1 Journalism It's not unique to Journalism, but from 2008 through 2020, there was a 26% decrease in newsroom headcount, totaling about 30,000 employees [5]. With the realities of the changing workplace, tools requiring significant people-time, training, and maintenance are hard to justify. The software offered to journalists must meet them where they are, not require they change their behavior. Hush Line delivers end-to-end encrypted messages directly in your inbox so you don't have to download another app.

2.1.2 Education A 16-year study of one school showed that when they implemented physical security measures, including metal detectors, gates, and removing decorative elements from campus, the feeling of safety went down. Peer violence increased, calls to the police quadrupled, and teachers grew increasingly concerned [6]. Speaking with students in West Oakland, California,

one 10-year old girl said that if necessary, she would report information, only if sure it wouldn't impact her reputation. How might schools be safer if there was a trustworthy way for students to privately communicate with trusted educators?

2.1.3 Business Up to 90% of women in the restaurant industry experience sexual assault or harassment [7], and 61% of all workers will witness or experience workplace harassment or discrimination. Stemming from fear of retaliation, fewer than 1 in 3 of those will make a formal complaint, and of those who do, fewer than 1% find victory in court [8].

Conversely, businesses can incur substantial penalties for SEC violations or other offenses that could have been caught sooner. In 2023, global tech company AAB Ltd. agreed to pay a $75 million civil penalty for charges relating to bribery. Goldman Sachs paid a $6 million civil penalty for a decade of fraudulent behavior where they made more than 22,000 deficient financial transactions [9].

2.2 The Price of Whistleblowing

Whistleblowing is risky endeavor. The examples below are included to illustrate that tools alone are never enough. We'll see stories highlighting different avenues individuals have taken and their outcomes.

2.2.1 Edward Snowden

Who They Are & What They Did One of the most influential whistleblowers of the last decades is Edward Snowden. He leaked a cache of documents he collected about NSA mass surveillance to journalists. His whistleblowing led to legislative reform in the USA, increased public awareness about whistleblowing and mass surveillance operations in America, and inspired the creation of new products designed to allow safer sharing of information for whistleblowers, including Signal, OnionShare, and even Hush Line.

What Went Wrong Snowden, easily one of the more technical whistleblowers of recent memory, was familiar with Tor and used Tails [10], an operating system that deletes all data when it shuts down, and whose traffic is completely tunneled through the Tor Network. Yet when he needed to securely contact journalists, he found the journalists lacked the technical ability to correctly setting up encrypted communications. Snowden couldn't find journalist

Glenn Greenwald's public PGP key, and even when Greenwald did get it configured with the help of Micah Lee [11], Snowden forgot to attach his own key in a message so Greenwald could privately respond. Snowden understood how the system worked and which technologies were resistant to surveillance, yet despite all of his knowledge, he is now exiled in Russia [12].

2.2.2 Chelsea Manning

Who They Are & What They Did Chelsea Manning is a former Army private who, working with Julian Assange of WikiLeaks, leaked information that included evidence of war crimes committed by the US [13].

What Went Wrong While Chelsea had technical skills, she was living in the chaos of war, and was eventually caught because she shared information in an online chat with Adrian Lamo, a former hacker turned government informant, who reported the information to the FBI, which included evidence of Manning's crimes. Chelsea Manning spent seven years in prison before President Obama pardoned her in 2017 [14].

2.2.3 Andrew Aude

Who They Are & What They Did Andrew Aude [15] is a former Apple software engineer who shared confidential information to a journalist over the course of years using Signal on his work-issued device. Messages included trade secrets, financial information, and details about product roadmaps and launch dates.

What Went Wrong Despite his technical proficiency - passing the impressive standard of Apple employment - and using Signal, he was caught. Though the encryption was strong, and even if he were using an anonymizing VPN or Tor, his error was using a device issued by his employer.

Mobile device management (MDM) software allows your employer to provision and manage hardware devices like mobile phones, tablets, or computers. Especially for a company like Apple, which employs ~164,000 people, MDM software enables your employer, for example, to make sure proprietary apps for employee resources like HR or Legal are available to everyone immediately or apply consistent and timely security updates or make sure everyone's VPN credentials are correctly configured without hoping that hundreds of thousands

of employees to get it right on their own. MDM software can also take screenshots or live-monitor any device in its network. So despite doing a lot of things right, if your adversary can take a screenshot of your conversation, it doesn't matter what app or tech you use to protect your data.

2.2.4 John Barnett

Who They Are & What They Did John Barnett was a Boeing whistleblower and former quality manager who disclosed safety concerns using official governmental channels with the 787s being made in his factory [16]. He filed an official complaint with the US Labor Department under an official whistleblower protection program [16]. He'd eventually bring a lawsuit against the company for the retaliation he experienced after sharing information with the Labor Department.

What Went Wrong John Barnett was at no time anonymous in his reporting and disclosing safety concerns about the Boeing 787. He ultimately experienced retaliation from Boeing because of this information sharing, and filed a lawsuit against them. It was during this period of engaging in a public lawsuit with Boeing, with no anonymity, that he was found dead from a self-inflicted gunshot [16].

2.3 Security Goals and Principles

Through speaking to former whistleblowers, journalists, and lawyers, and by reading academic papers published worldwide, we arrived at a set of guiding goals and principles:

P1: Usability. No matter how technically advanced your software is, adoption will fail if a whistleblower can't use it.

P2. Authenticity. Whistleblowers must have confidence they're communicating with the right person.

P3: Deniability. Requiring whistleblowers to download software that could land someone in jail is a non-starter.

P4: Availability. Whistleblowers must be able to access your software when they need it.

P5: Anonymity. Software makers must do everything they can to protect source anonymity.

P6: Confidentiality. Messages must remain secret. Communication between whistleblowers and other parties is protected and not the business of the software makers.

2.4 Current Tools

To better understand why a tool like Hush Line is necessary, we should consider two things: 1. the needs of the whistleblower, and 2. the tools currently available (Table 1). In this paper, we'll focus on three leading tools that provide examples of managed services, self-hosted options, and on-prem solutions : Signal, GlobaLeaks, and Secure Drop.

Legend: *M: Managed Service, S: Self-Hosted, H: Hardware, P: On-Prem Only*

Product	Type	Open-Source	E2EE	Onion Service	Verification System	Free	Non-Profit	User Directory
Afri-LEAKS [17]	S (GlobaLeaks Instance)	Y	Y	Y	N	Y	N	Y
CaseIQ [18]	M	N	N	N	N	N	N	N
Castillo [19]	M	N	Y	N	N	N	N	N
Confide [20]	M	N	Y	N	N	N	N	N
FaceUp [21]	M	N	Y	Y	N	N	Y	
GlobaLeaks [22]	S	Y	Y	Y	N	Y	N	N
Hush Line [23]	M, S, H, P	Y	Y	Y	Y	Y	Y	Y
Say Something [24]	M	N	N	N	N	?	N	N

Product	Type	Open-Source	E2EE	Onion Service	Verification System	Free	Non-Profit	User Directory
Secure-Drop [25]	P	Y	N	Y	N	Y	Y	Y
Signal [26]	M	Y	Y	N	N	Y	Y	N

Table 1. A view of different whistleblowing platforms on the market today.

2.4.1 Secure Drop

What It Does SecureDrop [25] is a tool maintained by the Freedom of the Press Foundation [27], a 501(c)(3) focusing on defending journalism around the world. Created originally by Aaron Swartz and then inherited by FPF, it is a self-hosted system consisting of different servers for receiving, viewing, and handling files on dedicated network connections and air-gapped devices. Customers are responsible for finding and purchasing compatible hardware.

To help simplify their approach, a new product called the Secure Drop Workstation is being developed and built on top of Qubes OS, a new security-focused desktop operating system [28]. The software provides functionality that, in effect, compartmentalizes all of that physical infrastructure on a single computer. The Workstation swaps servers with virtual machines serving similar purposes. While more streamlined, Qubes OS is only compatible with limited hardware, which customers must also find and purchase.

Limitations A whistleblower who uses Secure Drop faces a few obstacles. First, it is a Tor-only solution, which presents significant risks to anyone in countries where the internet is surveilled and free speech is limited. Recently, activists have even been arrested for having Tor on their mobile devices, as with Ola Bini in Ecuador.

2.4.2 Signal

What It Does Signal [26] is considered a gold standard for secure communication. We use it internally at Science & Design for team collaboration and

trust it to keep confidential messages safe. Signal is a messaging app available primarily as a native mobile application for iOS and Android, just like WhatsApp. Desktop apps exist, but they require pairing with a registered phone. Signal is one of the few open-source apps, aside from Firefox and Tor, that have penetrated the public consciousness. Signal collaborated with WhatsApp to integrate Signal's encryption protocol into WhatsApp, instantly providing strong encryption for billions of WhatsApp users globally. Signal is a tool many on the Hush Line team have contributed to.

Limitations However, the problem arises with the lack of anonymity because in order to use the Signal app, one must download it from an app store like Apple's App Store or Google's Play Store. To do this, users must create an account using PII, leaking their identities to at least one party in the exchange. It's commonplace for these companies to comply with requests from law enforcement, both foreign and domestic. Then, to register an account, a user needs a cell phone number. Acquiring a cell phone requires more PII, this time with your ID likely scanned for know your customer (KYC) regulatory requirements, another scenario where the company must comply with law enforcement requests for customer information. Now, at least two parties know who you are. While advanced workarounds exist to approximate anonymity, they are not doable for non-technical users or individuals without extensive programming skills, ultimately rendering anonymity impossible for the broader general public.

2.4.3 GlobaLeaks

What It Does GlobaLeaks [22] is a project out of Italy and is a self-hosted platform that's easy to install and use. It allows a developer to set it up on standard hardware and provides a rich and customizable platform for creating forms that meet your needs. GlobaLeaks, because of its relative ease of installation, is one of the most ubiquitous tip lines used by organizations worldwide today. There are forks, or, copies and modifications of the code, like AfriLeaks that host more instances of GlobaLeaks for other news organizations.

Limitations While easier than Secure Drop, GlobaLeaks still requires a developer and hosting your own infrastructure, making it less likely to be understood or used by the general public or individuals who do not have developer specialty knowledge. While the platform installs relatively simply, HTTPS is not available by default, and additional work must be done to deploy it to your

domain name. Some users have reported issues about the platform's usability, while others suffer downtime from misconfigurations.

2.4.4 Other Tools Other tools in Table 1 include both closed-source and for-profit options. We believe that a tool catering to higher-risk use cases must be open-source and verifiable so that the public can trust the software to protect them to the best of its ability. One noteworthy closed-source option is Say Something [24], a tip line from the survivors of the Sandy Hook massacre focused on school safety and gun violence.

3. Threat Model

3.1 What's Different About Hushline

Hush Line is unique in whistleblower products, as the only managed service that is free and open-source. Where other models distribute the risk to the individual customer, we are a centralized service, offering some liberties and other constraints: we can allow anyone to create an account, but consistent with other tip line / whistleblower platforms, we're also open to attacks online like denial of service or hacking attempts.

3.2 Challenges With Scale and Centralization

Because of SecureDrop's decentralized nature - meaning there isn't one central server running all of the instances - an attack on one server is not an attack on all. Though that means that when there is an attack on three to thirty servers, there are three to thirty servers to defend, maintain, and fix. More directly, there are ~70 Secure Drop instances worldwide, but only one instance of Hush Line, managed by Science & Design. Among other benefits of centralizing our services, it allows us to have more users; at the end of the beta period we had >10x more than all active instances of Secure Drop. Other things Hush Line needs to consider are traffic, bad actors, and paying for and maintaining the app's infrastructure.

3.1 Users

User Type	Goal
Submitter	Individual who sends a message.
Receiver	Individual or organization representative who reads messages.

User Type	Goal
Verifier	Staff member who verifies account owners (journalists, public figures, businesses).
Service Provider	Individual or organization who provides Hush Line services.
Server Admin	Individual who maintains the server operating Hush Line.

Table 2. All users of the Hush Line platform.

3.2 Adversaries

User Type	Goal
Passive Observer	Passively logs client IP addresses and their corresponding inbound/outbound connections (school/work networks, ISPs, DNS providers).
Active Observer	Targets specific connections.
Passive Attacker	Scans the internet for vulnerabilities to take advantage of.
Active Attacker	Seeks persistence, exploitation of known vulnerabilities, and seizure of physical equipment.

Table 3. Adversarial users of the Hush Line platform.

3.3 Assumptions

The following assumptions are accepted in the threat model of the Hush Line product:

3.3.1 Assumptions About the Individual Submitting a Message

- The individual submitting a message does so in good faith.
- The individual submitting a message wants to remain anonymous against a network observer, forensic analysis, or to Hush Line servers.

- The individual submitting a message is accessing the official Hush Line site.

3.3.2 Assumptions About the Person or Organization Receiving a Message

- The receiver operates Hush Line in good faith.

3.3.3 Assumptions About the Hush Line Server

- The server is operated in good faith.
- The server is single-use and configured with the official scripts on the GitHub main repo.
- The server has no other software other than what is required for the operation of Hush Line.

3.3.4 Assumptions About the Source's Computer

- The computer has an updated version of a popular browser including Chrome, Firefox, or Safari, and for anonymous connections, an updated version of Tor Browser.
- The computer is not compromised by malware.

3.3.5 Assumptions About Science & Design

- Science & Design wants to preserve the anonymity of its sources.
- Science & Design acts in the interest of allowing sources to submit messages, regardless of their contents.
- The users of the system, and those with physical access to the servers, can be trusted to uphold the previous assumptions unless the entire organization has been compromised.
- Science & Design is prepared to push back on any and all requests to compromise the integrity of the system and its users, including requests to deanonymize sources, block message submissions, or hand over encrypted or decrypted submissions.

3.3.6 Assumptions About the World

- The security assumptions of `passlib` and `scrypt` with randomly generated salts are valid.
- The security/anonymity assumptions of Tor and the Onion service protocol are valid.

- The security assumptions of Hush Line dependencies, application packages, and application dependencies, are valid.

3.3.7 Other Assumptions or Factors

- The level of press freedom may vary in both geography and time.
- The number of daily Tor users in a country can greatly vary.

3.4 Threats, Failure Points, Impacts and Mitigations

3.4.1 Threat: Server Compromise

- **Impacts:** If an attacker obtains the database encryption key, its contents may be decrypted. Still, we do not require PII. If you have SMTP delivery configured, your forwarding address will be visible. If you haven't added your own public PGP key to your account, message content will be visible.
- **Mitigation:** Hush Line does not require PII, including an email address, to use the service. To protect message content, users are encouraged to add their own PGP key. We store data encrypted in our database, and do not store timestamps or associate member data in any way. The database key is never hardcoded, is isolated from both app and database environments, and is stored in Terraform platform environment variables, removing the chance of exposure to the source code.

3.4.2 Threat: Network Observers

- **Impacts:** Adversaries who monitor network connections to our server can see your IP address and the domain you're visiting.
- **Mitigation:** All data in transit is encrypted using TLS, and users are encouraged to access Hush Line via Tor for additional anonymity. This prevents network observers from deciphering the content or metadata of communications.

3.4.3 Threat: Account Compromise

- **Impacts:** Disruption of Hush Line usage, impersonation which could lead to reputational harm or other damages.
- **Mitigation:** Strong password policies, optional 2FA, and secure password reset mechanisms are in place to protect user accounts. Users are educated on best practices for maintaining account security.

3.4.4 Threat: Legal and Coercive Pressure

- **Impacts:** Science & Design, Inc. and Hush Line must comply with legitimate legal requests, which could result in the forfeiture of data that includes your username, SMTP information, public PGP key, or other information you provide to Hush Line. No PII is required to use the Hush Line service, but if you've donated to our Open Collective or purchased anything from our Shopify store, potentially identifying information, including your shipping and billing address, name, email address, and IP address, could be tied back to you with sufficient analysis.
- **Mitigation:** Hush Line is designed to hold minimal information that could be of interest in legal contexts.

3.5 Failure Points

3.5.1 The Human Element The human element encompasses anything a person can touch. For developers, it means the code they write; for journalists, it means the tools they use and how they are used. Bugs are always part of software engineering, and we should never assume there is a "perfect" state of security or anonymity. If you give users a robust and well-considered privacy policy, we know they won't read it. And it's safe to assume that humans will look for shortcuts when presented with complex workflows. This includes using work-issued devices or networks to communicate with journalists or exfiltrate secret information.

3.5.2 Compromised Devices The human element includes compromising devices. There are few guardrails on Android to protect users from installing malware from unknown sources, and even Google's own Play Store hosts applications containing malware [29]. It doesn't have to be as obvious as installing suspicious software from suspicious sources. It can be as simple as clicking a link and loading a URL, or even loading images in your email client [30]:

> "As described in the proof-of-concept attack released by the researchers, the attacker uses one of the encrypted messages you are supposed to receive or might have already received and then turns it into a multipart HTML email message, as well as forges the return address, so it appears to come from the original sender. In the newly composed email, the attacker adds an unclosed image tag, like this, as clearly shown in the screenshot. When your vulnerable email client receives this message, it decrypts the encrypted part of the message given in the middle, and then automatically

> tries to render the HTML content, i.e., the image tag with all the decrypted text as the new name of the image, as shown below. Since your email client will try to load the image from the attacker-controlled server, the attacker can capture this incoming request, where the filename contains the full content of the original encrypted email in plaintext."

3.5.3 Compromised Infrastructure Hush Line uses cloud providers to manage our application and database. Our distributed approach increases security by isolating our database from the application environment and limiting access. But with this convenience comes the risk of our providers receiving a gag order and being forced to install monitoring software, lest they want to face prison or time-consuming legal proceedings.

3.6 Hush Line's Additional Protections

3.6.1 Verification System Hush Line employs a verification system to ensure that users can trust the source of communication. This system is particularly important for users who are public figures or have a wide audience. The verification system includes:

- **Display of Verification Status:** Hush Line indicates verified accounts with a distinctive **Verified** badge. This visual indicator helps users distinguish authentic accounts from potential impersonators, reducing the risk of phishing attacks.
- **Data Retention:** The information used to verify you is never saved, even temporarily.

3.6.2 User Education

- **Encryption Indicators:** The platform informs users whether their messages will be encrypted. For accounts with a public PGP key, messages are encrypted, ensuring that only the intended recipient can decrypt and read them. This feature is highlighted through messages on the submission form, emphasizing the importance of encryption for sensitive information.

3.6.3 User Guidance

- **Informative Messages for Senders and Receivers:** Hush Line educates its users about the significance of encryption and the steps required

to ensure message confidentiality. This includes prompts for receivers to add a public PGP key if they haven't already, and notifications for senders about the encryption status of their message.

4. Hush Line Overview

4.1 Our Users

User Group	Needs	Pain Points
Whistleblowers	- Helpful guidance- Trustworthy tools- Legal protection- Confidential communication	- Trust in tools and people- Gathering evidence- Financial support- Career risks
Lawyers	- Low-effort tools to receive whistleblower messages- Tools to help analyze technical data- Evidence to support claims	- Overwhelming amounts of data- Not enough time or staff to handle all clients- Hard to use tools requiring specialized training
Journalists	- Secure communication channels with whistleblowers- Access to verified information- Tools for verifying the authenticity of documents	- Protecting sources' identities- Verifying information under tight deadlines- Risk of legal repercussions
Educators	- Educational materials on whistleblowing- Case studies and real-world examples- Tools for facilitating anonymous reporting within educational institutions	- Lack of awareness about whistleblowing- Ensuring students understand the importance of confidentiality- Integrating whistleblowing topics into the curriculum

User Group	Needs	Pain Points
Businesses	- Anonymous reporting channels for employees- Tools for monitoring and managing reports- Support for legal and compliance requirements	- Building trust in the reporting process- Managing and responding to reports efficiently- Balancing transparency with confidentiality

Table 4. Our users, their pain points, and needs.

4.2 System Requirements

We built Hush Line as a managed service designed for high availability, usability, and security. While Hush Line is intended for users to create an account on `hushline.app`, we encourage people and organizations to self-host if they prefer. For consistent implementation, we provide full documentation on getting it started for your organization.

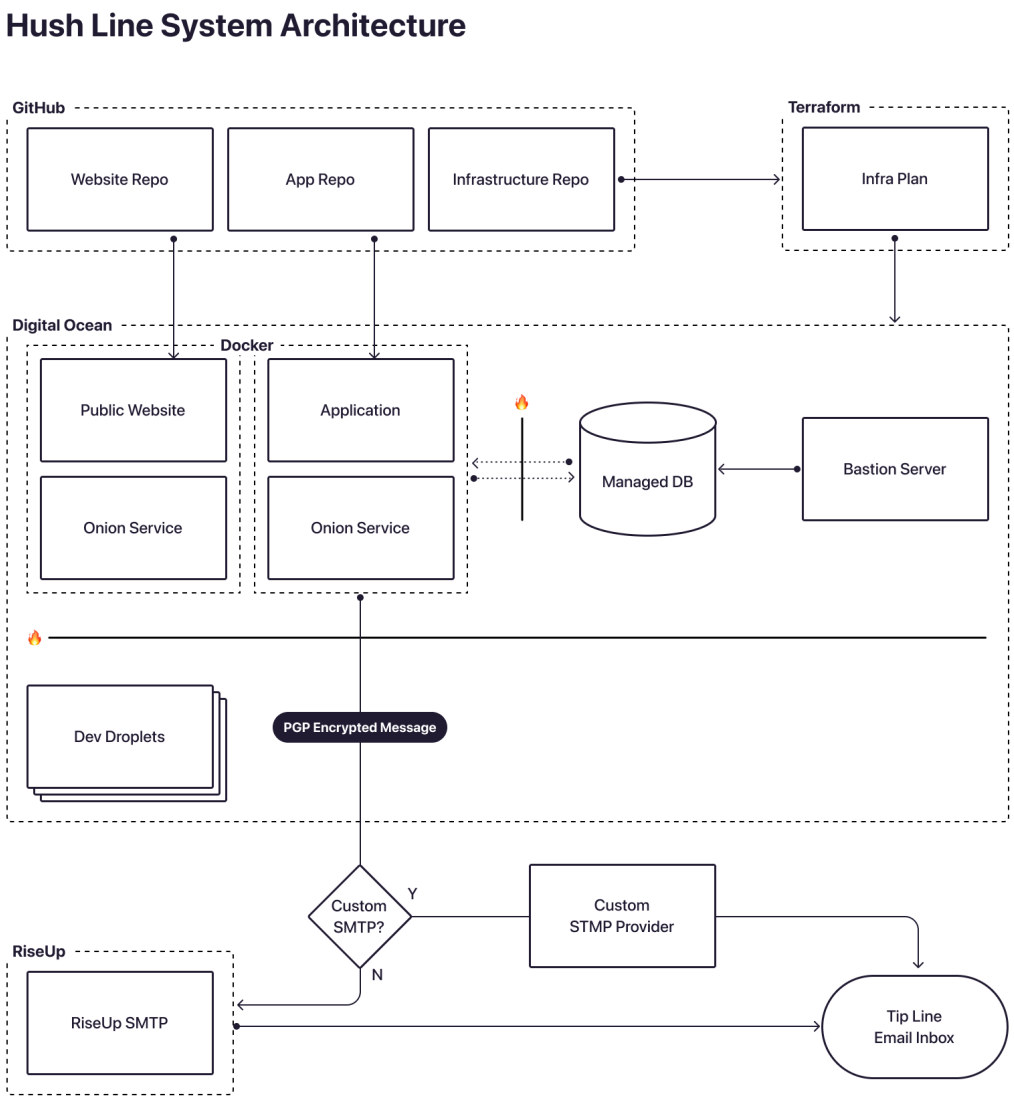

Diagram 1. Hush Line System Architecture

We use a combination of Digital Ocean, Terraform, GitHub to automate our build and release pipeline as well as disposable development environments.

4.3 Database Isolation

To help defend against database compromise we isolate resources as seen in Diagram 1. In the event that the application server become compromised, lateral movement to the database is not possible. We use TLS encryption for

connections to and from the database, and restrict access to application and bastion servers.

4.4 Bastion Server

The only way to access the database is through a Bastion server - an isolated server that infrastructure owners SSH into, and then connect to the database. Access to the Bastion server is restricted to relevant members of the technical staff, and SSH is completely disabled to the database server.

4.5 Mail Forwarding

Email forwarding is a convenient and user-friendly feature. Our integration of Mailgun allows a tip line owner to enter their email address, and forwarding will work. Alternatively, a user may use a custom SMTP provider or have no SMTP forwarding at all. Custom configurations mean end users must have technical proficiency in finding their SMTP server, port, username, and password if their email provider supports it.

4.6 Onion Services

We use Onion Services for users with advanced privacy needs. An Onion Service issues our app and website a `.onion` address, making it accessible anonymously using the Tor Browser. Onion Services bypass DNS by never exiting the Tor Network to reach its destination. Our Onion Services are run in isolated containers for increased security.

4.7 Managed Services

Using managed services always comes with tradeoffs. On one hand, they add a layer of risk by trusting a third party. On the other hand, they allow us to minimize risk by offloading server and database maintenance. Hush Line addresses this by requiring a PGP key to enable email forwarding and ensuring plaintext messages are never shared outside of our hosting platform, Digital Ocean, in our case.

4.8 Product Design

Whistleblowing is a scarey, unfamiliar process, and the software you use should be disarming while doing all it can to keep you safe. We're a text-only service and encourage users to begin with a plan rather than grabbing and dumping

loads of information. We think that through guidance and education, users can keep themselves safe while engaging in responsible disclosure.

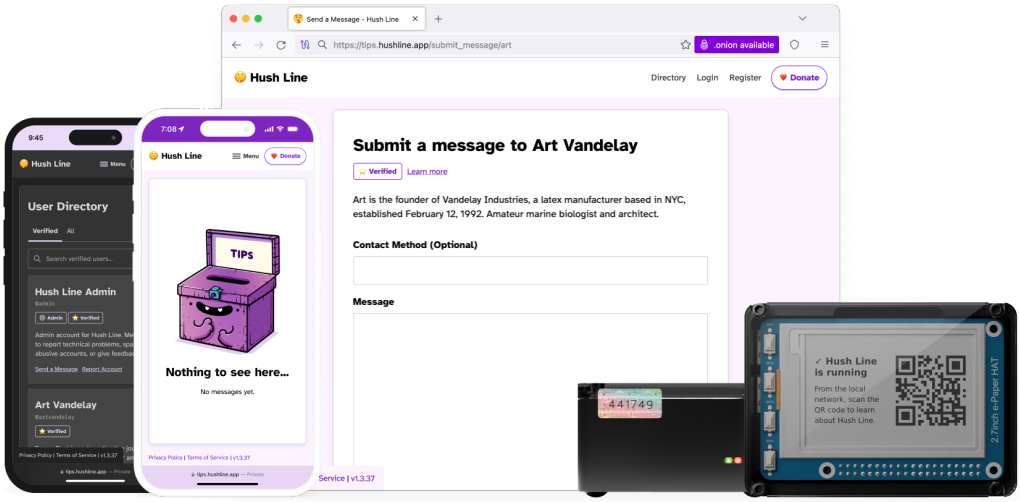

Image 1: The Hush Line Product Suite

4.8.1 Interface Design The UI of the application leans into conversational conventions with a sense of levity, using emoji throughout the interface text. It tries not to rush the user, but rather present information in a friendly way that helps educate the whistleblower, while maintaining a high standard for usability.

4.8.2 Interaction Design Perhaps what differentiates Hush Line the most is that we're a centralized service, and rather than depending on individual self-hosters to configure their own instance correctly, we manage all of the services, so users don't have to worry about specialized tech, and instead can focus on their work.

Like any modern web service, including Instagram, Google, or Signal, a user may go to the Hush Line app and create an account to use the platform. In a Settings panel, individuals can add their own PGP key, set up email forwarding, add a display name, or enable two-factor authentication.

4.8.3 Accessibility Hush Line received a service grant from Open Tech Fund in the form of an accessibility audit. The goals of the audit were to make the screen-reader experience usable, descriptive, and intentional.

4.8.3 To CAPTCHA? Throughout the beta period users received spam messages, and since messages can be end-to-end encrypted, combined with using custom SMTP settings, client-side filtering is an imperfect solution.

hCaptcha

An analysis of an hCaptcha integration showed multiple external site connections, increasing IP leakage just to send a message. There are also security trade-offs since "it loads `https://newassets.hcaptcha.com//captcha/v1/988e468/hcaptcha.js` along with multiple other javascript source files, and it executes them in the browser."[31]

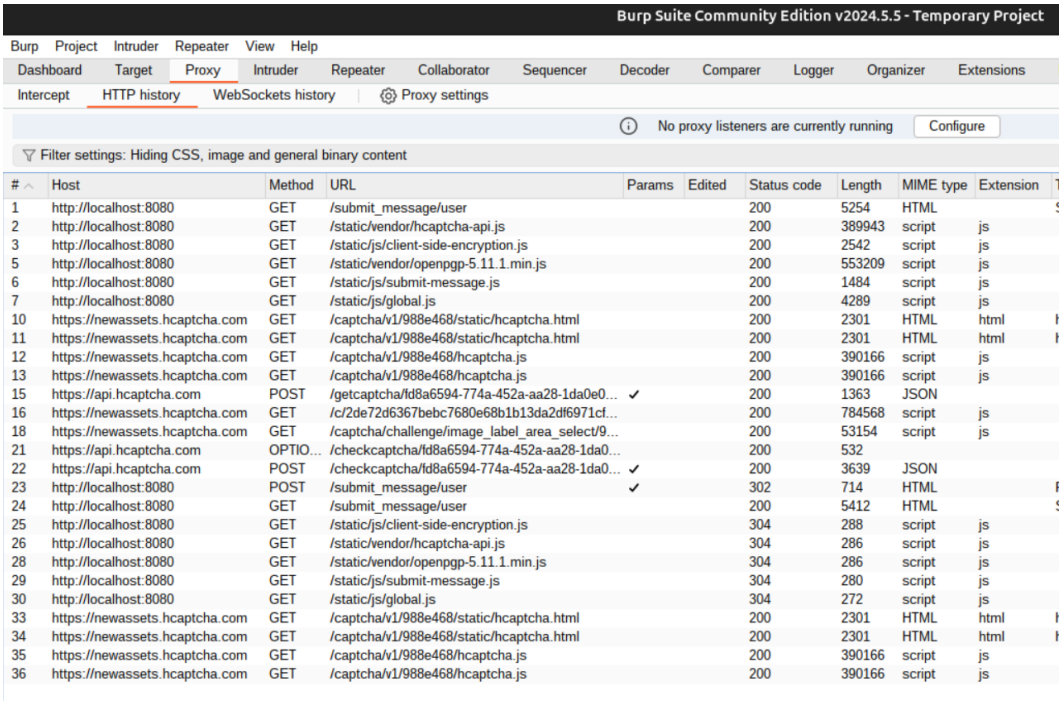

Figure 1: image

Image 4: Network calls when using hCaptcha

Local Captcha

We explored CAPTCHA options including creating an image with letters and numbers obstructed by randomly drawn lines and presenting a basic math problem. Using an image was a blocker due to accessibility limitations: a bling user won't be able to read the image, even with assistive technology, and therefore wouldn't be able to submit a message. A math problem, while not

perfect, only needs to catch most bots, and since it's an accessible solution, it was our best option.

```
@app.route("/submit_message/<username>", methods=["GET", "POST"])
def submit_message(username: str) -> Response | str:
    form = MessageForm()
    user = User.query.filter_by(primary_username=username).first()

    if request.method == "GET":
        # Generate a simple math problem
        num1 = secrets.randbelow(10) + 1
        num2 = secrets.randbelow(10) + 1
        math_problem = f"{num1} + {num2} ="
        session["math_answer"] = str(num1 + num2)  # Store the answer

    if form.validate_on_submit():
        captcha_answer = request.form.get("captcha_answer", "")
        if not validate_captcha(captcha_answer):
            return redirect(url_for("submit_message", username=username))

        # Save the message or handle encryption (omitted for brevity)

    return render_template(
        "submit_message.html",
        form=form,
        user=user,
        math_problem=math_problem,
    )

def validate_captcha(captcha_answer: str) -> bool:
    if not captcha_answer.isdigit():
        flash("Incorrect CAPTCHA. Please enter a valid number.", "error")
        return False

    if captcha_answer != session.get("math_answer"):
        flash("Incorrect CAPTCHA. Please try again.", "error")
        return False

    return True
```

4.9 Making PGP Slightly Easier

Pretty Good Privacy (PGP)

PGP works using public/private key encryption. Think of your public key as envelopes made just for you, and the private key as a special letter opener that is the only thing in the world that can open those envelopes.

Most of the time PGP works by two people individually creating a public/private keypair. They first exchange public keys, then may begin sending encrypted messages. Only the sender and receiver's private keys, which are never shared with anyone, can decrypt the messages.

Proton

The way we recommend using Hush Line is in conjunction with Proton. Proton provides encrypted productivity tools, with Proton Mail being their flagship application. Proton Mail is an email provider like Gmail, but is encrypted so only you can read their contents, and not the company or even an attacker with access to their servers. Like Hush Line, Proton uses PGP for message encryption, so in Mail settings, a user may download a copy of their Proton public PGP key. A user adds that key to their Hush Line settings, and also adds their Proton Mail address for email forwarding, and now any tips submitted to your Hush Line will be delivered to Proton, and since you have the private key already there, they'll automatically be decrypted for you!

Mailvelope

For users of other email services including Gmail, we've integrated Mailvelope, a powerful browser extension that enables PGP encryption and decryption directly in the browser. Users may install the Mailvelope browser extension on Chrome or Firefox, and once configured, can read decoded messages without any other application.

5. Limitations

5.1 Money

Scale and money are the main limiters for a web application. Currently, at ~$1,500/yr, it's a manageable number, even if the hosting organization took it on entirely. However, as we scale, costs may significantly increase to more than is sustainable without a financial model to support the service.

5.2 User Error

We also cannot account for the operational security or online behavior of individuals using our platform. For example, if a whistleblower is using a com-

promised device that can record their screen, Hush Line cannot protect their communications.

5.3 Governments

Our services are hosted in the United States, which has National Security laws that may force a provider, including us, to remain silent about orders received. This means that if Digital Ocean received an order to monitor Hush Line's servers, they may not be allowed to tell us about it. This is one reason we encourage all users to add a PGP key to their account.

5.4 Developer Error

Humans will make errors. The developers of Hush Line, despite their expertise, are still prone to errors. Hush Line is proudly open source, and we encourage the community of users, hackers, security researchers, and more to find ways we can improve.

6. MVP Maintenance Cost and Resource Overview

Item	Specs	Monthly Cost	Annual Cost
Managed Database	512 MB, 10 GB Disk	$60	$720
Email Forwarding		$35	$420
App - Production App	1 GB RAM, 1 vCPU, 150 GB Bandwidth	$12	$144
App - Onion Service	512 MB RAM, 1 vCPU, 50 GB Bandwidth	$5	$60
Website - Public Website	512 MB RAM, 1 vCPU, 50 GB Bandwidth	$5	$60
Website - Onion Service	512 MB RAM, 1 vCPU, 50 GB Bandwidth	$5	$60
Bastion Server	512 MB RAM, 1 vCPU, 10 GB Disk	$4	$48

Item	Specs	Monthly Cost	Annual Cost
Dev Droplets	512 MB RAM, 1 vCPU, 50 GB Bandwidth	$4	$48 per droplet
Total		$130	$1,560

Table 5. Cost overview for running a Hush Line instance.

7. Personal Server

As we've seen, the convenience of centralized web applications provides opportunities for high availability, scalability, and usability, we know that sometimes a user's threat models include not trusting any third parties. In this situation, we offer the Hush Line Personal Server. It hosts the entire Hush Line platform on a self-hosted device. We designed a custom case milled from solid aircraft-grade aluminum that physically closes access to all ports except power and ethernet, making it resistant to Evil Maid attacks. Additionally, we disable SSH, USB, and Wifi on the device. A user boots it up, and an e-paper display will show a QR code with the address to their Hush Line Onion Service instance.

Figure 2: personal-server

Image 2: The Hush Line Personal Server Top and Side Views

7.1 System Requirements

The Personal Server is designed to be deployable to hardware with limited resources, specifically the Raspberry Pi. Using a pre-built image using docker for containerization of the app, onion service, and database. The Personal Server is a consumer device that packages a Raspberry Pi 4 with 1 GB RAM with an e-paper display and custom, security-focused case.

Item	Specs	Cost
Internet Service	100 Gbps - 1,000 Gbps	~$50/mo
Raspberry Pi 4B	1GB RAM	$35
Waveshare E-Paper HAT	264x176, 2.7inch	$18.99
Personal Server Security Case	Milled A606 Alloy	Indiv. Cases Not Available
Ethernet Cable	CAT 5-8	~$20
One-Time Costs		$73.99
Recurring Costs		~$50/mo

Table 6. One-time and recurring costs associated with running a DIY Personal Server.

7.2 Defending Against Physical Access

7.2.1 Unique Identification The only access to the device is by removing the lid, and to help defend against physical access, uniquely numbered, tamper-evident tags seal the lid to the body. Personal Server owners are encouraged to copy their cover numbers down, and if tampering is ever suspected, they may verify that they match.

7.2.2 Custom Case We designed custom cases that are milled from solid A606 alloy. All ports, expect for power and ethernet, are sealed from physical access. The lid is a 5mm piece of smoked acrylic, giving a clear view to the epaper display which shows a QR code embedded with the device's onion address.

Everything is plug-and-play, and the owner needs no specialized training to set up and operate the Personal Server. Our custom cases are not for sale individually, and we are the exclusive distributors.

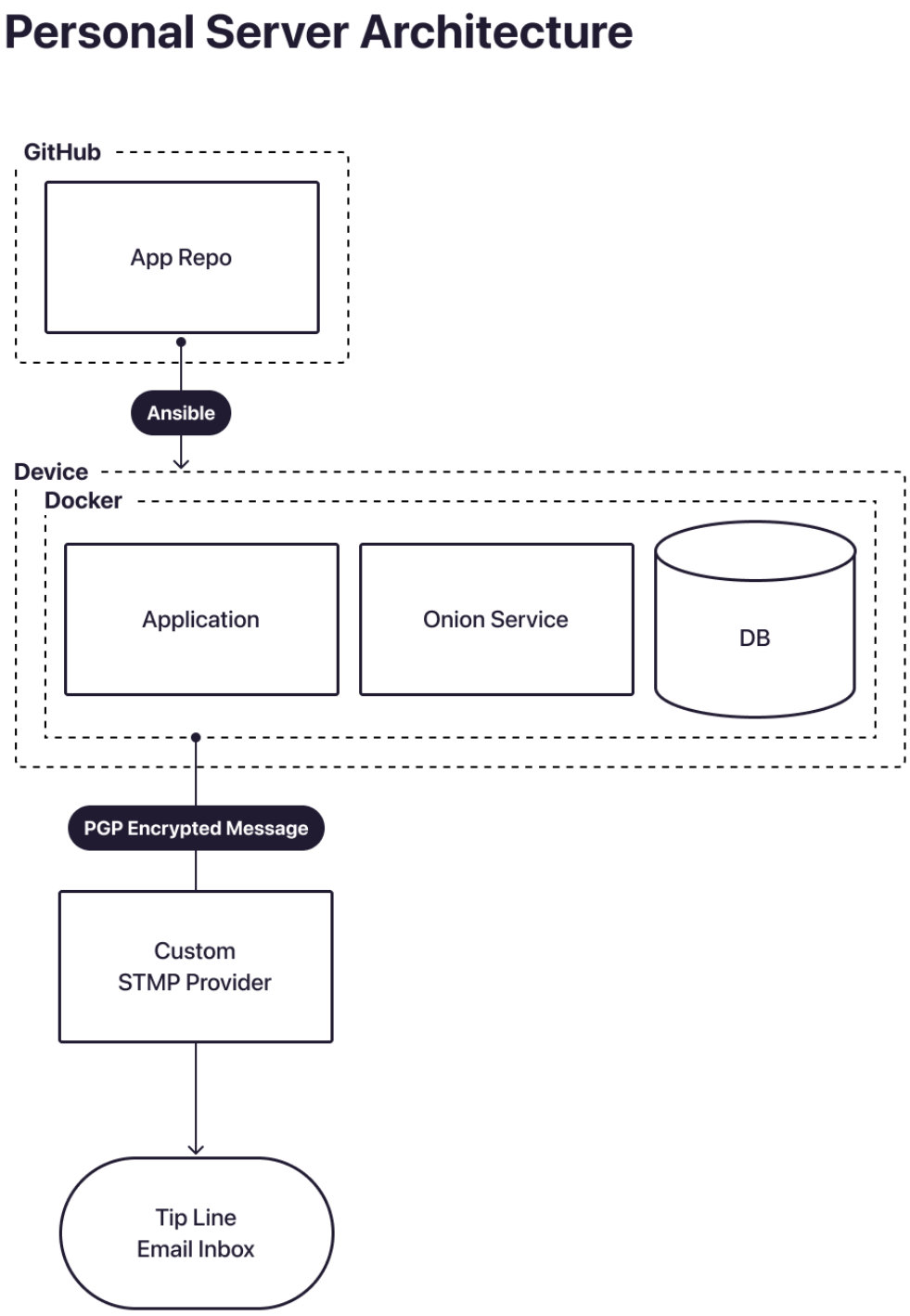
Personal Server Architecture
GitHub
App Repo
Ansible
Device
Docker
Application
Onion Service
DB
PGP Encrypted Message
Custom
STMP Provider
Tip Line
Email Inbox

Diagram 2. Personal Server System Architecture

8. Ethical Monetization

Hush Line is proudly supported by the Data Empowerment Fund, but Science & Design, Inc. is a 501(c)(3), and as a non-profit receives most financing through grant cycles that are both inconsistent and insufficient. Understanding the cost associated with web services, Science & Design understands the need to seek product sustainability through financial sustainability. We are seeking a path toward ethical monetization through paid tiers of features targeted at business users. We will always provide our core services for free, and will continue researching how to make Hush Line more valuable for paying customers while maintaining our non-profit principles.

Feature	Free	Pro	Business
Daily Messages	20	100	Unlimited
BYOK	Y	Y	Y
2FA	Y	Y	Y
No Logging	Y	Y	Y
Auto-Deleting Msgs	Y	Y	Y
Simple SMTP		Y	Y
Aliases		Y	Y
Custom Subjects		Y	Y
Files			Y
Custom Fields			Y
Custom Domain			Y
Branding			Y
File Size	-	10 GB	Unlimited
Aliases	0	5	15
Custom Subjects	0	5	15
Monthly Price/User	$0.00	$9.99	$19.99
Annual Price/User	$0.00	$119.88	$239.88

Table 7. Hush Line's Speculative Pricing Model

9. The Path to Launch

9.1 Pre-Release Beta

Before asking funders for support, having a minimum-viable product was an important milestone. And to understand how we could make the service better we ran a 6-month beta program. During that time we conducted interviews with participants who included former whistleblowers, journalists, researchers, and more.

9.1.1 Feedback & Findings PGP Key Length

Depending on the encryption algorithm and other factors, PGP keys can differ in length significantly. Quickly after kicking off the beta, a participant tried using a key greater than 10,000 characters long an was unable to.

User Directory

After a suggestions from one of our subject matter experts, Dr. Martin Shelton, we included an opt-in user directory. The allows whistleblowers to find who they need in a centralized place without hunting around the internet.

Bios

One prominent whistleblower suggested adding additional social proofs, including a bio for the whistleblower: "making sure the whistleblower can confirm at each step that they're talking to the right person is incredibly important for the person's safety."

Better Message Forwarding

We leaned on manual SMTP configuration during the beta, asking users to add their SMTP username, password, port, and server. A query at the end of the beta period showed only 1.35% of participants configured message forwarding.

End-to-End Encryption

Initially we encrypted messages on the server before sending, but a researcher working on a different whistleblowing product recommended strongly recommended implementing end-to-end encryption.

9.1.2 By The Numbers Enrollment numbers for features like two-factor authentication appear low, but are actually consistent with what we see with major platforms like Twitter, where the 2FA enrollment was 2.5%, slightly lower than Hush Line's beta.

Measurement	Amount	Percentage
Total Testers	815	
2FA Enrolled	25	3.07%
PGP Enabled	23	2.82%
SMTP Enabled	11	1.35%

9.2 Our First Grant

Hush Line was awarded a $100,000 grant from the Data Empowerment Fund to bring the app from prototype to production. We hired our first engineers, who included Micah Lee, the creator of OnionShare and core Tor Project and SecureDrop developer.

9.2.1 Tentative Grant Budget

Category	Allocation	Amount
Engineering	60%	$60,000
Infrastructure	10%	$10,000
Product Management	10%	$10,000
Org Admin	10%	$10,000
Sales	9%	$9,000
Swag	1%	$1,000

Table 3: Grant Budget

- **Engineering:** Infrastructure dev, front and back-end engineering, accessibility, and cryptography.
- **Infrastructure:** Costs for hosting on various platforms.
- **Product Management:** Roadmap, UX, UXR, Project Management.
- **Org Admin:** 10% organization administative fee.
- **Sales:** Delivery of an open-source sales palybook.
- **Swag:** Stuff to show thanks to our community.

9.2.2 Delivered Features

1. Production infrastructure - XL (~40 hours)
2. Development infrastructure - L (~20 hours)
3. App Accessibility - L (~20 hours)

4. Personal Server Readiness - XL (~60 hours)
5. Better Message Forwarding Infrastructure - L (~20 hours)
6. OCR Vision Assistant - S (~4 hours)
7. Stripe Integration - S (TBD)
8. Paid Features - XL (TBD)
9. Guided Disclosure - L - (TBD)
10. More TBD

10. Related Academic Research

- Roth, V., Güldenring, B., Rieffel, E., Dietrich, S., & Ries, L. (2013). A secure submission system for online whistleblowing platforms. Freie Universität Berlin, FX Palo Alto Laboratory, Stevens Institute of Technology.
- Agrikola, T., Couteau, G., & Maier, S. (n.d.). Anonymous whistleblowing over authenticated channels. CNRS, IRIF, Université de Paris; Karlsruhe Institute of Technology.
- Uddholm, J. (2016). Anonymous Javascript cryptography and cover traffic in whistleblowing applications. KTH Royal Institute of Technology, School of Computer Science and Communication.
- Jayakrishnan, H., & Murali, R. A simple and robust end-to-end encryption architecture for anonymous and secure whistleblowing. Department of Computer Science and Engineering, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India.
- Ahmed-Rengers, M., Vasile, D. A., Hugenroth, D., Beresford, A. R., & Anderson, R. CoverDrop: Blowing the whistle through a news app. Department of Computer Science and Technology, University of Cambridge.

11. Conclusion

This paper highlights critical areas where Hush Line is differentiated from its peers. We believe that a trustworthy, easy-to-use, cross-industry tool can help journalists get better leads, educators increase school safety, and business avoid compliance penalties.

Thanks and Acknowledgements

- Abbey Ripstra, Research
- Alex Rojas, Industrial Design

- Dr. Ashley Di Battista, Research, Paper Editor
- Brassy, Engineering
- Chirayu Desai, Privacy Consulting
- David McKinney, Security Auditor
- David Mirza Ahmad, Security Auditor
- Elijah Waxwing, Subject Matter Expert, Security
- Ese Udom, Mobile Engineering
- Em, Privacy Consulting
- Glenn Sorrentino, Design, Engineering, Architecture
- Grant Birkinbine, Engineering
- Jeremy Moore, Engineering, Infrastructure
- Kenny Krosky, Accessibility, Software Engineering
- Dr. Martin Shelton, Subject Matter Expert, Journalism
- Micah Lee, Engineering, Infrastructure, Architecture
- Ricchi Machado, Engineering, Cryptography
- Ritik Shah, DevSecOps Intern
- Sam Schlinkert, Documentation, Engineering
- Saptak Sengupta, Eng Consulting
- Scott Jenson, Usability Consulting
- Simon Wörpel, Engineering
- Subgraph, 2024 Security Audit
- Sooraj Sathyanarayanan, DevSecOps Intern
- Stefanie Daehler, Subject Matter Expert, Education
- Ura Creative, Production Design, Packaging

References

1. Stanger, A. (2019). Whistleblowers: Honesty in America from Washington to Trump. Yale University Press. Page 9.
2. https://hbr.org/2020/10/do-your-employees-feel-safe-reporting-abuse-and-discrimination
3. https://www.pewresearch.org/short-reads/2021/07/13/u-s-newsroom-employment-has-fallen-26-since-2008/ft_2021-07-13_newsroomemployment_03/
4. https://github.com/scidsg/hushline/pkgs/container/hushline%2Fhushline
5. https://www.pewresearch.org/short-reads/2021/07/13/u-s-newsroom-employment-has-fallen-26-since-2008/
6. https://theconversation.com/culture-of-trust-is-key-for-school-safety-92731
7. https://hbr.org/2018/01/sexual-harassment-is-pervasive-in-the-restaurant-industry-heres-what-needs-to-change

8. https://hbr.org/2020/10/do-your-employees-feel-safe-reporting-abuse-and-discrimination
9. https://web.archive.org/web/20240711021747/https://www.sec.gov/newsroom/press-releases/2023-234
10. https://tails.net/
11. https://harpers.org/archive/2017/05/snowdens-box/
12. https://www.nytimes.com/2013/08/02/world/europe/edward-snowden-russia.html
13. https://www.nytimes.com/2010/04/06/world/middleeast/06baghdad.html
14. https://www.aclu.org/news/free-speech/president-obamas-commutation-chelsea-mannings
15. https://github.com/scidsg/project-info/blob/main/hush-line/5.%20Research/2.%20Legal/apv-andrew-aude.pdf
16. https://www.nytimes.com/2024/03/12/business/john-barnett-boeing-whistleblower-dead.html
17. http://f3mryj3e2uw2zrv3zv6up6maqosgzn27frz7xodvpl7pkestoyigtkad.onion/#/
18. https://www.caseiq.com/
19. https://www.projectcallisto.org/
20. https://getconfide.com
21. https://www.faceup.com/en
22. https://www.globaleaks.org
23. http://hushline.app
24. https://www.sandyhookpromise.org/our-programs/say-something-anonymous-reporting-system/
25. https://securedrop.org/
26. https://signal.org/
27. https://freedom.press
28. https://www.qubes-os.org
29. https://www.darkreading.com/endpoint-security/90-malicious-apps-55-million-downloads-google-play
30. https://thehackernews.com/2018/05/efail-pgp-email-encryption.html
31. https://github.com/scidsg/hushline/pull/461