Privacy is Priceless, but Signal is Expensive

Meredith Whittaker and Joshua Lund on 16 Nov 2023

Signal is the world's most widely used truly private messaging app, and our cryptographic technologies provide extra layers of privacy beyond the Signal app itself. Since launching in 2013, the Signal Protocol—our end-to-end encryption technology—has become the de facto standard for private communication, protecting the contents of billions of conversations in WhatsApp, Google Messages, and many others. Signal also continues to invest in research and

underlies our recent work to add a layer of quantum resistance to the Signal Protocol, and our previous work on metadata protection technologies that help keep personal details like your contact list, group membership, profile name, and other intimate information secure. This singular focus on preserving the ability to communicate privately is one reason that we work in the open, documenting our thinking and making our code open source and open to scrutiny—so you don't have to take our word for it.

Signal is also a nonprofit, unlike almost every other consumer tech company.[1] This provides an essential structural safeguard ensuring that we stay true to our privacy-focused mission. To put it bluntly, as a nonprofit we don't have investors or profit-minded board members knocking during hard times, urging us to "sacrifice a little privacy" in the name of hitting growth and monetary targets. This is important in an industry where "free" consumer tech is almost always underwritten by monetizing surveillance and invading privacy. Such practices are often accompanied by "growth hacking" and engagement maximization techniques that leverage dark patterns to keep people glued to feeds and notifications. While Signal is also free to use, we reject this kind of

communications app. We also reject business models that incentivize such practices.

Instead of monetizing surveillance, we're supported by donations, including a generous initial loan from Brian Acton. Our goal is to move as close as possible to becoming fully supported by small donors, relying on a large number of modest contributions from people who care about Signal. We believe this is the safest form of funding in terms of sustainability: ensuring that we remain accountable to the people who use Signal, avoiding any single point of funding failure, and rejecting the widespread practice of monetizing surveillance.

But our nonprofit structure doesn't mean it costs less for Signal to produce a globally distributed communications app. Signal is a nonprofit, but we're playing in a lane dominated by multi-billion-dollar corporations that have defined the norms and established the tech ecosystem, and whose business models directly contravene our privacy mission. So in order to provide a genuinely useful alternative, Signal spends tens of millions of dollars every year. **We estimate that by 2025, Signal will require approximately $50 million dollars a year to operate—*and this is very lean compared to***

Here we review some of these costs and where this money goes, in the name of providing more transparency into Signal. But we hope to do more than that. Where money goes and how it's made is a bit of a taboo in tech, something that most tech companies avoid talking about. The actual costs of consumer tech are generally hidden behind stories of innovation and the word "free," and the connection between the product marketing of a highly profitable tech industry and the ingress and egress of profit and revenue is usually unclear. We believe a material map of these dynamics can help clarify just what is required to fulfill the dream of privacy-preserving alternative technology, and contribute to establishing a solid foundation from which we can grow alternatives that contest tech surveillance and the incentives behind it.

This is not a comprehensive overview—this post isn't meant to provide a full accounting or to review every line item in detail. Instead, we focus on illustrative examples, looking at infrastructure and labor in particular. We'll also explore average costs that in practice vary dynamically in relation to factors that are often outside of our control.[2]

We'll start with an overview of some of Signal's biggest infrastructural costs—what we pay for the utilities and services that let Signal reach you. These include the temporary storage of end-to-end encrypted data for message delivery; the global server network that processes billions of requests every day; the registration fees that cover the delivery of verification codes during the sign-up process to help verify phone numbers and prevent spam accounts; the bandwidth that is required to efficiently route end-to-end encrypted messages and calls around the world; and some of the additional services that keep everything running smoothly. We'll dive into each of these in more detail, but here's a quick breakdown:

Storage: $1.3 million dollars per year.
Servers: $2.9 million dollars per year.
Registration Fees: $6 million dollars per year.
Total Bandwidth: $2.8 million dollars per year.
Additional Services:[3] $700,000 dollars per year.

Current Infrastructure Costs (as of November 2023): Approximately $14 million dollars per year.

Data is profitable, and we're a nonprofit focused on collecting as little data as possible.

Most tech companies collect and create as much data as they can. They build large data warehouses, and then later invent new terms like "data lake" when their unquenchable thirst for more of your private information can no longer fit within the confines of a single warehouse. Their default move is to store everything for as long as they can in an easily accessible and unencrypted format, suffering data breach, after data breach, after data breach, hoping to monetize this data by indirectly (or directly) selling it to advertisers or using it to train AI models. Again, data is profitable.

In contrast, Signal's default move is to end-to-end encrypt everything that we possibly can and to store as little as possible—all while making sure your messages are delivered promptly and your calls are clear and free of delays. We do this by taking advantage of globally distributed hosting infrastructure and by paying for significant amounts of bandwidth from some of the top providers in the world.

Just like everything else in Signal, messages and files are always end-to-end encrypted.

As soon as your message is delivered, that small bundle of encrypted data (i.e. your message) can be dropped from the queue. The storage of end-to-end encrypted files is temporary too, and any undelivered end-to-end encrypted data is automatically purged after a period of inactivity. Even though everything is only temporary, **this storage still costs Signal around $1.3 million dollars per year**.

This is a lot of money, although it's less than it would cost if we stored everything forever. But unlike the tech companies that collect and store everything, we don't have (and do not want to have) any surveillance data to sell or use to recoup these costs. We can't read or access any end-to-end encrypted messages because the keys that are required to decrypt them are in your hands, not ours. And it's not just about your messages. Signal also uses our metadata encryption technology to protect intimate information about who is communicating with whom—we don't know who is sending you messages, and we don't have access to your address book or profile information. We believe that the inability to monetize encrypted data is one of the reasons that strong end-to-end encryption technology has not been widely deployed across the commercial tech industry.

communications service for the many millions of people around the world who depend on Signal, it's necessary for Signal's servers to be globally distributed. Having a geographically distributed network of servers is particularly important for end-to-end encrypted voice and video calls, because latency can result in audio delays or degraded video connections that quickly make the app unusable for real-time communication.

Because everything in Signal is end-to-end encrypted, we can rent server infrastructure from a variety of providers like Amazon AWS, Google Compute Engine, Microsoft Azure, and others while ensuring that your messages and calls remain private and secure. We can't access them, and neither can the companies that provide any of the infrastructure we rent. As a small nonprofit organization, we cannot afford to purchase all of the physical computers that are necessary to support everyone who relies on Signal while also placing them in independent data centers around the world. Only a select few of the very largest companies globally are still capable of doing this, which is a hallmark of a troublingly concentrated industry.[4]

Signal's addition of novel privacy-preserving features also affects our server costs. To

that uses a trusted execution environment. This made us the first large-scale messaging app to let people automatically find their friends and contacts without revealing their address book to us, keeping these connections private. Because other mainstream apps don't have this layer of privacy protection in place, they can often access details about your network and relationships without restrictions, and many of them store this highly sensitive information for later use.[5]

When we first deployed this system in 2017, only a few servers were necessary. But as the number of people using Signal increased, the number of servers required to support private contact discovery also rose. At its peak, nearly 600 servers were dedicated to private contact discovery alone, at a total cost of **more than $2 million dollars per year**.

This significant cost would have continued to rise. However, thanks to algorithmic research advances and hardware updates, we've been able to reduce the total number of private contact discovery servers to around 10 total —despite the fact that the service is handling more traffic than ever. A significant amount of money and engineering resources have been dedicated to ensuring that your address

and introduce new techniques to enhance your privacy even when the initial costs are high.

Registration Fees

Signal incurs expenses when people download Signal and sign up for an account, or when they re-register on a new device. We use third-party services to send a registration code via SMS or voice call in order to verify that the person in possession of a given phone number actually intended to sign up for a Signal account. This is a critical step in helping to prevent spam accounts from signing up for the service and rendering it completely unusable—a non-trivial problem for any popular messaging app.

Signal's registration service routes registration codes over multiple telephony providers to optimize delivery across the globe, and the fees we pay to third-party vendors for every verification code we send can be very high. This is in part, we believe, because legacy telecom operators have realized that SMS messages are now used primarily for app registration and two-factor authentication in many places, as people switch to calling and texting services that rely on network data. In response to increased verification traffic from apps like Signal, and

significantly raised their SMS rates in many locations, assuming (correctly) that tech companies will have to pay anyway.

The cost of these registration services for verifying phone numbers when people first install Signal, or when they re-register on a new device, currently averages around $6 million dollars per year.

These costs vary dramatically from month to month, and the rates that we pay are sometimes inflated due to "toll fraud"—a practice where some network operators split revenue with fraudulent actors to drive increased volumes of SMS and calling traffic on their network. The telephony providers that apps like Signal rely on to send verification codes during the registration process still charge their own customers for this make-believe traffic, which can increase registration costs in ways that are often unpredictable. Of course, Signal does everything we can to reduce or eliminate the impact of toll fraud. We work closely with our voice and SMS verification providers to detect and shut down fraudulent registrations as quickly as possible. But it's still a game of cat and mouse, with unavoidable expenses along the way.

You are probably familiar with the concept of paying for bandwidth in the form of buying a data plan from your cellular provider or signing up with an Internet Service Provider (ISP) for your home. But it may surprise you to learn that every website, app, and service also pays for the bandwidth they use whenever you connect to them.

Some pay more than others. Most of the major tech companies (like Amazon, Google, and Microsoft) own and operate their own data centers. After spending billions of dollars to build massive hosting facilities, they install their own fiber optic cables and custom networking equipment. This also means they get to earn a lot of money by charging others for the privilege of using that equipment.[6] Smaller organizations like Signal can't afford to build matching infrastructure from scratch, so we (along with almost every startup and tech company) pay rent to the big players in order to access the bandwidth we need.

Millions of people use Signal every day, and it takes a *lot* of bandwidth to provide a fast and reliable service. **Signal spends around $2.8 million dollars per year on bandwidth** to support sending messages and files (such as photos, videos, voice notes, documents, etc.) and to enable voice and video calls.

Signal's end-to-end encrypted calling functionality is one of the most expensive services that we provide. Signal also goes far beyond other messaging apps when it comes to protecting your privacy during voice and video calls, and we do this in ways that substantially increase how much bandwidth we use in order to provide a high-quality calling experience.

To take one example, Signal always routes end-to-end encrypted calls from people who aren't in your contacts through a relay server that obscures IP address information.[7]

Almost none of our competitors do this, and Signal's default behavior is much more expensive than the alternative. Automatically relaying 1-on-1 voice and video calls from unknown contacts (instead of always using a peer-to-peer connection whenever possible) provides an extra layer of privacy, but results in considerably higher bandwidth costs for Signal's calling-related relay servers. At current traffic levels, the amount of outbound bandwidth that is required to support Signal voice and video calls is around 20 petabytes per year (that's 20 million gigabytes) **which costs around $1.7 million dollars per year in bandwidth fees *just for calling***, and that figure doesn't include the development costs associated with hiring

infrastructure to support those calls.

The Human Touch

Signal isn't just a collection of privacy-preserving services that route end-to-end encrypted messages and calls around the world. It's also a set of cross-platform apps and modular development components (commonly called libraries) that make this type of private communication possible in the first place. Because the norm is surveillance, we're often required to create or modify our own libraries from scratch, swapping in privacy instead of using more common frameworks that assume surveillant defaults. Swimming against the tide of an ecosystem whose incentives and infrastructure promote surveillance and privacy invasions is, of course, more time-intensive and more expensive, and requires dedicated and experienced people.

First, we have three distinct client teams, one for each platform (Android, Desktop, and iOS). These teams are constantly working: adjusting to operating system updates, building new features, and making sure the app works on a wide variety of devices and hardware configurations. We also have dedicated engineering teams that handle the development and maintenance of the Signal

libsignal. These also need constant development and monitoring.

Product and design teams help shape the future of the app and determine how it will look and function, while our localization team coordinates translation efforts across more than sixty languages. We even have a full-time, in-house support group that interfaces with people who use Signal and provides detailed technical feedback and real-time troubleshooting information to every other team. This is an essential function, particularly at Signal, because we don't collect analytics or telemetry data about how people are using Signal.

This is a lot of work, and we do it with a small and mighty team. In total, around 50 full-time employees currently work on Signal, a number that is shockingly small by industry standards. For example, LINE Corporation, the developers of the LINE messaging app popular in Japan, has around 3,100 employees,[8] while the division of Kakao Corp that develops KakaoTalk, a messaging app popular in Korea, has around 4,000 employees.[9] Employee counts at bigger corporations like Apple, Meta, and Google's parent company (Alphabet) are much, much higher.[10]

budget goes towards recruiting, compensating, and retaining the people who build and care for Signal. When benefits, HR services, taxes, recruiting, and salaries are included, this **translates to around $19 million dollars per year.**

We are proud to pay people well. Our goal is to compensate our staff at as close to industry wages as possible within the boundaries of a nonprofit organization. We know that we can't provide equity, expensive playpen offices, or other benefits common to large tech companies. We also know that we need to recruit and retain a highly experienced and specialized workforce in an extremely competitive industry if we're going to offer a service that provides a meaningful alternative to apps with far more people and resources. And we don't believe that precarity should be the cost of doing good. Compared to most tech companies, Signal's numbers are a drop in the bucket.[11]

Growth in Signal translates into increased infrastructure costs, and having more infrastructure requires more labor. As of November 2023, Signal's server network is regularly responding to around 100,000 requests per second, and we routinely break our previous records. A funny thing happens when a globally accessible service starts

longer unique or rare, and unlikely situations become more and more common as Signal grows. It's not unusual for our engineers to do things like write custom code to reproduce an esoteric and complicated IPv6 connectivity issue that's affecting people running an arcane operating system configuration in specific regions, but only when connected via a certain set of internet service providers.[12] Troubleshooting such infrastructure issues can be very expensive, because isolating a problem and developing a fix can take a lot of time and expertise.

Identifying and fixing arcane problems is not the only thing that takes time and skill. In the context of building for privacy, adding a common feature or service in a way that avoids surveillance frequently requires significant work and creativity. To take one example, profile pictures and profile names are always end-to-end encrypted in Signal. This means that Signal does not have access to your profile name or chosen profile photo. This approach is unique in the industry. In fact, it has been more than six years since we first announced this additional layer of protection, and as far as we know none of our competitors have yet adopted it. Other messengers can easily see your profile photo, profile name, and other sensitive information that Signal cannot access. Our

that it took Signal more effort to implement support for profile photos. Instead of a weekend project for a single engineer, our teams were required to develop new approaches and concepts within the codebase (like profile keys), which they worked to roll out across multiple platforms after an extended testing period.

The same dynamic played out again when Signal introduced support for animated GIF searches on Android and iOS. Instead of quickly and easily integrating the standard GIF search SDK that most other apps were using, engineers spent considerable time and creativity developing another unique privacy-preserving technique that hides GIF search terms from Signal's servers, while also hiding who is searching for those terms from the GIF search engine itself. We later expanded those techniques to further obfuscate GIF search information by obscuring the amount of traffic that passes through the proxied connection.

When Meta acquired GIPHY, and many other apps were scrambling to contend with the privacy implications of the deal, Signal employees slept soundly knowing that we had already built this feature correctly several years earlier.[13]

future threats by adding post-quantum resistance to the Signal Protocol. The financial costs associated with these research and development initiatives are substantial. They're also essential for building privacy-preserving technology in a dynamic industry where surveillance is the norm.

By offering a competitive compensation package, Signal helps make it easy for people to choose to develop privacy-preserving technology that benefits the world instead of going to work for the surveillance-advertising-industrial complex. We're proud of our healthcare plans, family-friendly policies like extended parental leave, flexible schedules, and the many other benefits that help make Signal a great place to work.

These things cost money, but a world where Signal can attract talented people to work on privacy-preserving technology is a world that looks a lot more attractive.

Future Tense

We hope that this cursory tour of some of Signal's operations and costs helps provide a greater understanding of Signal's unique place in the tech ecosystem, and of the tech ecosystem itself.

sustained by small donations is both highly ambitious and, we believe, existentially important. The cost of most consumer technology is underwritten by surveillance, which has allowed people to assume that “free” is the default, and a handful of industry players have accrued eye-watering amounts of personal data and the unprecedented power to use that data in ways that are shaping our lives and institutions globally.

To put it another way, the social costs of normalized privacy invasion are staggeringly high, and maintaining and caring for alternative technology has never been more important.

Signal is working to show that a different approach is possible—an approach that puts privacy at the center, and where organizations are accountable to the people who use and rely on their services, not to investors, or to the endless pursuit of growth and profit.

Thank you for your support. It’s an honor and privilege to work on Signal every day, and we —very literally—couldn’t do it without you. Please consider donating to Signal via our website or learn how to give using the app.

Foundation. ↩

2. For example, millions upon millions of new people suddenly switched to Signal in January 2021 after WhatsApp updated their Terms of Service. ↩

3. Uptime monitoring, outage alerts, redundant capacity for disaster recovery purposes, maintenance contracts, etc. ↩

4. Alphabet, the parent company of Google, reported that "Capital expenditures, which primarily reflected investments in technical infrastructure, were $31.5 billion for the year ended December 31, 2022." Just one of Meta's new data centers in Huntsville, Alabama has a budget of $1.5 billion, and Meta already has so many other data centers in operation that they could easily "pause" construction and redesign the Huntsville location to make it better suited for AI workloads. Suffice it to say, Signal does not have this kind of cash laying around. ↩

5. Unlike Signal, many big tech companies know who you are talking to and can easily correlate messaging activity with social media activity. The European Commission, for example, imposed a fine of €110 million euros because Facebook

acquisition process. ↩

6. In their 2022 annual report, Alphabet announced that "Google Cloud revenues increased $7.1 billion from 2021 to 2022." Not all of this revenue comes from bandwidth fees, but there's a reason why "Networking Egress" gets its own tab on the Google Cloud Pricing Calculator. ↩

7. Signal also includes an optional feature that will use a relay server for every call—even when an incoming call is from someone you know: *(Privacy > Advanced > Always Relay Calls)*. ↩

8. "About," LINE Corporation, accessed November 9, 2023, https://linecorp.com/en/company/info. ↩

9. Kakao's Q3 2023 Earnings Presentation (page 14) also specifies an overall employee count of 17,208. ↩

10. Neither Alphabet, nor Apple, nor Meta break out specific employee counts for the individual business units that work on their messaging and calling platforms. Alphabet reported an employee count of 182,381 in their Q3 2023 fiscal results, Apple has "more than 100,000 employees" according to their 2023 fourth quarter

11. As of their Q3 2023 financial report, Meta "had $37.22 billion available and authorized for [share] repurchases" alone. ↩

12. For the networking enthusiasts out there, a piece of networking infrastructure operated by a major cloud provider was responding to SYN packets in a way that indicated it supported connections without TCP window scaling when that wasn't actually the case. TCP windows then appeared to the client as being 8 times smaller than the value that the cloud provider thought they were, which led to the clients being unable to send data because they were running out of receive windows. The cloud provider wasn't refilling the windows, as they appeared to be almost full on their side. ↩

13. Meta has since sold Giphy to Shutterstock, losing over $260 million dollars in the process. In this era of expanding consolidation, you never know where your data may end up. The only winning move for services that care about your privacy is to not collect any sensitive data in the first place. ↩

Don't have Signal? Give it a try!

For media inquiries, contact press@signal.org