

# State of Mozilla

## 2018

Ex. No.

UPX0979

1:20-cv-03010-APM

*The State of Mozilla 2018 is our annual report. This report highlights activities for 2018-2019 and is accompanied by detailed 2018 financials. This report is released when we submit the Mozilla non-profit tax filing for the previous calendar year.*

### **Putting People Back at the Center of Online Life**

Mozilla continues to believe that the internet can and should be a positive force for individuals and for societies. However, there are deep problems to be solved to make this true in an enduring way for the future. An obvious first step is to help people understand and protect ourselves from current online harms. This gives us better knowledge to address the problems at a deeper level — to create new and better experiences where respect and security for the individual are built into the core product.

Much of the optimism and openness that characterized the internet's development has given way to growing skepticism and fear from

Redacted

MOZ-000397



consumers. As a result, recent years have witnessed a reckoning for the tech industry. People have started coming to grips with the unchecked growth of data-driven online services. They've begun to question the ease with which information core to their very identities can be captured, monetized and used against them. This has been compounded in the last two years by a rash of high-profile data breaches and other incidents that have laid bare how individuals' data are being bought, sold and manipulated to influence everything from their buying habits to election results.

A central challenge is the implicit exchange of data for services that is the business model of so many online services. This dynamic presents a growing threat to people's privacy and ability to control their identities online. The problem has become even more acute with the advancement of Artificial Intelligence (AI) technology that can "learn" more about us than ever before and use this information to shape our digital experience, depriving us of the freedom that has historically defined how we use the internet.

But people have begun to resist the tradeoff of their data for convenient access to valuable and increasingly necessary online products and services. In response, companies have tried to reclaim users' loyalty by appearing to champion the cause of privacy. At Mozilla, we do more than just talk about privacy. From our founding, we have been motivated by a clear commitment to put people's privacy and security at the core of everything we build and everything we do.

As an innovator with decades of experience in privacy and data security, we at Mozilla have important insight to share, and we have a responsibility to do so. In 2018, we captured opportunities to address the challenges this moment presents and continued building on these efforts in 2019. This reports speaks to our efforts over the past two years.

Redacted

MOZ-000398



Our multi-pronged approach included consumer product and technology development that give end users and developers the tools they need to navigate today's increasingly complex digital landscape. We also drive a user-first agenda on the public policy and advocacy fronts, pushing for greater transparency, corporate accountability and technology standards that put people back at the center of online life.

To this end we brought a key privacy feature to our flagship Firefox browser—enabling tracking protection by default, because we believe that the price of embracing a digital lifestyle shouldn't be giving up one's identity. Our promise is to help make clear that privacy is non-negotiable, and we delivered on this promise in 2018 and 2019 by providing consumers with a range of tools beyond the browser that are built from the ground up to provide security and preserve privacy.

In addition to tackling privacy and security at the product level, we have pushed for changes at the ecosystem level over the past two years. Leveraging our significant experience and unique standing at the crossroads of tech, policy and advocacy to stand up for users by pressing for strong privacy and security standards and corporate accountability both within the industry and in public policy.

We publicly called on tech giants Facebook and YouTube to do better by their users and the web by bringing greater transparency to consumers and reevaluating the manner in which the content they recommend is served up. We also led the fight for Net Neutrality as the named plaintiff in the case against the FCC.

Our mission has always been to protect and shape the future of the internet as a global public resource, open and accessible to all; the present moment provides an opportunity and an obligation to deliver on this mission like never before. As our work continues to gain urgency, we look forward to building on the investments we made in the last two



years to win in a new era and write the next chapter of the internet for the benefit of all its present and future users.

## **How Mozilla Operates**

Mozilla is unique. Founded as a community open source project in 1998, Mozilla currently consists of two organizations: the 501(c)3 Mozilla Foundation, which backs emerging leaders and mobilizes citizens to create a global movement for the health of the internet; and its wholly owned subsidiary, the Mozilla Corporation, which creates products, advances public policy and explores new technologies that give people more control over their lives online, and shapes the future of the internet platform for the public good. Each is governed by a separate board of directors. The two organizations work in concert with each other and a global community of tens of thousands of volunteers under the single banner: Mozilla.

Because of its unique structure, Mozilla stands apart from its peers in the technology and social enterprise sectors globally as one of the most successful social enterprises.

## **Private by Default**

*In response to increasing public concern about data privacy and how people's personal information is being used, many technology companies have answered by putting the onus to protect their privacy on users. In some cases that has meant users being forced to change settings, pore over inaccessible terms of service, or take control of complicated product features. In other instances, companies have resorted to*

Redacted

MOZ-000400



*promising easy access to online safety and privacy only to those who stay within the confines of their closed operating and device ecosystems.*

While we're pleased to see privacy and online security, two issues we've long championed and backed up with product features, business practices and industry pressure, these other companies' approaches have had a deleterious effect—boxing in and overburdening users, limiting the web's interoperability and making the internet less trustworthy.

Still we welcome this attention to a critical issue because we understand that our mission—the success of the internet as a global public resource—depends on users trusting that their safety will be protected. While some of our competitors may be new to the notion of privacy, it has always been at the core of everything we do. Mozilla is secure by default; it always has been, and it always will be.

The pervasive and hidden nature of third-party, cross-site tracking has allowed companies virtually unfettered access to the data generated by people's online activities. This has enabled micro-targeting and predictive profiles to be built by companies which influence the types of ads, services and information people are presented online. Without the ability to curb this type of data collection, people's control over their online experiences is severely limited.

We backed up our commitment to making sure Firefox users are afforded privacy and control online by adding Enhanced Tracking Protection (ETP) to the browser on desktop and Android as a default feature in 2019. We made this move after first rolling ETP out as a browser setting users could enable in August 2018.

Redacted

MOZ-000401



But we started on this journey of figuring out a way to safely block third-party, cross-site tracking without disrupting the core internet browsing experience nearly a decade earlier with an effort that was then called Do Not Track.

Taking the lessons from this prior exploration, when we began developing ETP in 2018, we first engaged publishers and other content creators to fully understand the impact that turning ETP on by default would have on the user experience and the ability of web site owners to reach their desired audiences. After months of experimentation and user and developer testing and feedback, we successfully moved ETP to a default feature in the Firefox browser.

Since July 2019, the Firefox browser with ETP on by default has blocked more than 10 billion trackers—that's roughly 125 trackers per day, per Firefox user. But we didn't want users to just take our word for it; in 2019, we also added a Protections Report, which enables Firefox desktop browser users to see the types and volume of trackers (including cryptomining and fingerprinting) that have been blocked based on the personal browsing history stored on their devices.

We're bringing the ETP functionality to the development of future products and new technologies as well. In 2019, we began testing ETP in Firefox Preview, the beta version of our soon-to-be released Android browser, which is powered by the Mozilla-built GeckoView engine. Our AR/VR and mixed reality browser, Firefox Reality, was also built from the ground up with the same private-by-default approach.

In 2018, Firefox Reality became available in the Viveport, Oculus, and Daydream app stores and in 2019 we announced a partnership with HTC VIVE to power immersive web experiences through the Firefox Reality browser across Vive's portfolio of devices. As we enter this emerging



technology space, we do it with the core values and user-first commitment that have always been our hallmark.

This year, Mozilla Foundation began exploring the ways in which Artificial Intelligence is understood by internet users around the world and how the nascent technology's development should be shaped by human agency and ethics with a focus on the privacy and security and enriching people's lives.

Mozilla is helping developers build more trustworthy AI, including work with Omidyar Network and others to put \$3.5 million behind professors integrating ethics into computer science curriculum. We also encourage governments to promote trustworthy AI, including through work by Mozilla Fellows to map out a policy and litigation agenda that taps into current momentum in Europe.

It's our belief that the power to decide when and what people share about themselves online should be an explicit choice extended to people regardless of who makes the products and services they are using. It is with this in mind that Mozilla Foundation first launched the \*Privacy Not Included Buyer's Guide a few years ago with the main goal of helping people shop smart—and safe—for products that connect to the internet.

In 2018, the Guide was expanded to include a broader range of connected devices and services, reflecting increased buy-in from not only consumers, but companies recognizing the value of connected products that are safe, secure, and private. The 2018 \*Privacy Not Included Buyer's Guide product list grew to 76 connected products across six categories and included a "Creep-o-meter" to measure feedback about which products people thought were safe, and which products people felt were a bit creepy in their data handling.



Instead of offering “Do and Don’t” buying recommendations, we leveraged our technical expertise to create the Minimum Security Standards we think all products should meet in order to be sold in stores. We used these standards to rate the products in the Guide. They include using encryption, automatic security updates, requiring strong passwords, having a system to manage vulnerabilities, and having an accessible privacy policy.

Mozilla Foundation also pushed companies like Venmo to adopt private-by-default positions on transactions. Advocating for consumers with other companies and arming them with vital information at-a-glance was one way to empower people in their digital lives, helping them make better informed decisions about how and with whom they spend their time and money online.

## **Combating Misinformation**

The reputation of the internet as a public good continues to suffer from the impacts of rampant misinformation on the web. The major tech players have refused to accept editorial responsibility. Recognizing the threat, Mozilla mobilized efforts using our products and advocacy to improve news literacy, increase political ad transparency, and prevent the pervasive tracking that helps fuel the problem.

When experts identified The 2019 European Union Parliamentary Election as under threat from fake and misleading ads and suspicious social media accounts, Mozilla heard a call to action. Guided by our commitment to empower people, Mozilla Corporation and Mozilla Foundation joined forces in a multi-faceted campaign to bring greater transparency to political advertising on platforms and



help people across the continent participate in the election through an educational election's toolkit.

Beginning with a letter to the European Commission, Mozilla highlighted the lack of publicly-available data about political advertising on major platforms and the impact that would ultimately have on EU residents and the election. This led us to organize researchers to push the tech sector to adopt fully functional, open APIs that enable their research into political ads targeted to EU residents.

And when it became clear that was unlikely to happen by the platforms themselves before voting day, our own team went to work in creating an analysis dashboard that gathered data on the political ads running on various platforms and provide a concise “behind the scenes” look at how these ads were shared and targeted for researchers and journalists monitoring the elections.

While our contribution to this effort ended up looking very different than what we had first set out to do, our work documented every time the API failed and every roadblock encountered, creating a series of tips and tricks to help others use the API. It also led to national coverage of Facebook's broken promise to create a tool to fight track political advertising and disinformation. The Foundation continues to apply pressure and galvanize people around the world to force big tech to the table to increase transparency and fight misinformation.

In the run-up to the U.S. presidential elections next year Mozilla has taken a number of steps, led by Mozilla Foundation, to challenge its peers to support free and open discourse online. One step was calling on Facebook to live up to its promises to commit to truly transparent political advertising, and if it can't, stop its practice of

Redacted

MOZ-000405



running political ads altogether. Citing the ways in which microtargeting keeps ideas from being debated in the open, enabling fiction to parade as fact, Mozilla Foundation also called on Google and Facebook to ban the practice of micro-targeting in political advertising.

The work we've done in 2019 builds upon efforts that began in 2018 with the U.S. midterm elections. We gave users easy access to Firefox extensions designed to help spot propaganda bot patterns; the ability to install Facebook Container, a Firefox tool that prevents the social network from tracking across websites; tips to change their browser settings to avoid tracking; and more.

To unpack the full spectrum of the problem and outline solutions, Mozilla's popular podcast, IRL, created an original documentary short film, Misinfo Nation: Misinformation, Democracy, and the Internet. Featuring Scott Shane of The New York Times, Emily Thorson, of Syracuse University, and An Xiao Mina of the Credibility Coalition, the film prompts us to fact check and challenge our own beliefs.

Mozilla also released Ad Analysis for Facebook for the 2018 U.S. midterm elections, part of our solution to the lack of transparency around political advertising on the web. The tool was an important resource for users and researchers to learn how they were micro-targeted. Facebook changed its settings, breaking the tool, but Mozilla is pursuing solutions to shine a light on political ad targeting.

The Mozilla Foundation welcomed dozens of new fellows, including two internationally known for their work to thwart dis/misinformation. Camille Fancois works on mitigating online targeted threats and disinformation campaigns, exposing their impact on civil society and vulnerable users globally. Renee DiResta

Redacted

MOZ-000406



is working closely with platforms, researchers, and the Mozilla Open Innovation team to explore how we can address dis- and misinformation online.

## **Beyond the Browser**

In the early days of Mozilla, a web browser was the primary, and in many cases the only, way to access the internet. Today, that has changed; we use mobile apps, location-based services and embedded systems to access the internet—sometimes without even realizing we're online. Traditional desktop browsers are only one piece of the puzzle, so in 2018 and 2019, we expanded our product and service offerings to keep users secure no matter how they access the internet.

Recognizing that part of what threatens the health of the internet today is the lack of clarity about the value being exchanged for access to products and services, we're exploring paid and subscription service offerings as a complement to the free services we already provide. In both cases, we are maintaining our unwavering commitment to ensuring transparency with easily accessible and digestible terms of service and explicit consent to take in only the information needed to provide products and services.

In 2018, we began testing a new paid virtual private network (VPN) service in Firefox as well as a password manager called Lockwise, which is currently being offered for free. We also launched Firefox Monitor, another free service, which allows people to check whether their email address has been a part of a recent security breach.

This year, we took these product explorations further, deepening our engagement with Firefox users by making added service benefits like being able to check multiple email addresses with Firefox Monitor and

**Redacted**

MOZ-000407



password generation through Firefox Lockwise, accessible through the Firefox browser with a free Firefox account.

We also rolled the Firefox VPN testing we kicked off in 2018 into a Firefox Protection Network beta offering for U.S. Firefox users that combines secure proxy and VPN functionality. Our eventual goal is to offer a seamless free or paid hybrid subscription service globally to Firefox users globally across any of their connected devices.

In 2019, Mozilla Corporation expanded our product presence in Asia with the launch of Firefox Lite 2.0 in Taiwan, India and Indonesia. Firefox Lite is specifically designed to meet the unique needs of users in these geographies. Previously in market as Firefox Rocket, Firefox Lite 2.0 puts the focus on lightning-fast browsing and privacy, blocking ads and trackers by default, and working fast with decreased bandwidth. A search bar for comparison shopping, full-page screenshots and access to games on the home screen and a bare-bones news page are several of the features that set Firefox Lite apart.

## **Changing Standards**

The freedom of expression that has been foundational to the internet, allowing for unprecedented creativity and connection, means that it is easy to mislead users, manipulate their online experiences and violate their privacy. Maintaining our commitment to this freedom of expression, Mozilla advocates for standards of engagement designed to protect users.

Our approaches include calling out bad behavior when we see it; equally importantly, we advocate for high standards, particularly with respect to the disclosures companies must make about how

**Redacted**

**MOZ-000408**



they are using our data, and we push for protocols, policies and legislation that make the internet more private and secure.

In 2019 Mozilla continued its fight for Net Neutrality in the U.S. as the named plaintiff in the federal case Mozilla v. Federal Communications Commission (FCC). After years of battling over this issue, the opinion that came down in October 2019 opened a path for states to put net neutrality protections in place, even as the fight over FCC federal regulation is set to continue. Though disappointed that the court's decision failed to restore net neutrality protections at the federal level, Mozilla will remain a key player in the fight for these essential consumer rights as they continue to play out in the states, in Congress, and in the courts.

2019 brought to a close another legal battle in which Mozilla played a key role: the fight for copyright reform in the EU. After almost three years of debate and activism, in 2019 EU lawmakers approved the EU Copyright directive. We had hoped that the new rules would provide an opportunity to bring European copyright law in line with the realities of the 21st century.

Sadly, that did not turn out to be the case, and we expect copyright to return to the political agenda in the years to come, as the real underlying issues facing European creators and press publishers persist. Mozilla's focus remains on minimizing the negative impact of this law on Europeans' internet experience and the ability of European companies to compete in the digital marketplace.

Another arena in which Mozilla took an active stand for consumers in 2019 was on the issue of encrypted DNS traffic. Currently, the internet relies on outdated architecture that allows almost all of the most basic online traffic—the addresses you pull up when you visit a website—to flow unencrypted, making this information to attack

Redacted

MOZ-000409



and leaving user data open to access by Internet Service Providers (ISPs) who are largely responsible for directing this traffic today. Since 2017, Mozilla has been pushing to change this internet protocol with the adoption of a new standard DNS over HTTPS (DoH) which would encrypt this traffic.

In 2019, Mozilla released a set of clear guidelines for a Trusted Resolver Program that spells out publicly the terms for handling this data securely. We began testing in the protocol with Firefox users in the U.S. only. The effort has been met with pushback from the large ISPs, whose ability to monetize and control this data would be severely limited if DoH were to become the new standard. The discussions about DoHs advancement continue with lawmakers, ISPs and other companies who are exploring joining Mozilla's trusted resolver program as we expand testing of the protocol.

In addition to pushing for change at the system level, Mozilla also works primarily through the efforts of its separate policy and Foundation teams to drive lawmakers and other companies to adopt practices that improve consumers' online safety and the overall health of the web.

To that end, in 2019 Mozilla Foundation launched a petition urging Apple to automatically reset iPhone users' unique Identifier for Advertisers (IDFAs) every month. The IDFA is a random device identifier assigned by Apple to a user's device. Advertisers use this to track data so they can deliver customized advertising. The IDFA is used for tracking and identifying a user (without revealing personal information), allowing advertisers to access aggregated data. While iPhone users can currently disable the IDFA manually, automatic resets would make it harder for companies to build profiles of users over time.

Redacted

MOZ-000410



Mozilla Foundation also urged YouTube to rethink its algorithmic recommendation system by encouraging YouTube users to share their stories about misdirection to unintended and unwanted content through a YouTube Regrets campaign.

Mozilla continued its work to bring privacy protections to people across the globe through advocacy and policy work with the passage of data protection laws in both California and Kenya and a published blueprint for strong federal privacy legislation in the United States.

While Mozilla believes government must play a role in protecting its citizens, regulation is not the only way to promote privacy online. Mozilla also brought our Lean Data Practice workshop to New Delhi and Bangalore India, and Nairobi, Kenya. The workshops educate companies that implementing best practices for data privacy, protection, and management is not only good for their users, but also good for business by creating less risk and increasing trust with users.

Mozilla also supported two pieces of legislation aimed at putting rules in place to create a better future online. Mozilla's support for the Deceptive Experiences To Online Users Reduction (DETOUR) Act hopes to make the internet a more transparent place by banning the use of deceptive practices that trick users into handing over their personal data. The second, the Access Act, will encourage competition by requiring the largest companies to make user data portable and their services interoperable with other platforms, a key piece of Mozilla's own framework for tech competition policy.

Redacted

MOZ-000411



## **Building Our Teams Today for Tomorrow**

Building and fostering a diverse and inclusive organization is core to who we are at Mozilla. Mozilla also believes that attracting diverse talent that is motivated, creative and passionate is crucial to our success. In our ongoing efforts to make inroads in creating a more visibly diverse workforce, we continue to measure and report on our progress, evolve our policies and practices, and take public stands that foster and make clear our commitment to building a more inclusive environment.

We want to attract and retain that talent while ensuring total compensation is competitively reasonable and aligned with Mozilla's culture and mission. While the compensation philosophy is similar between the Mozilla Foundation and the Mozilla Corporation, the market frameworks used to benchmark total compensation are different given the nature of work and the talent required.

### **Mozilla Corporation**

With over 1,000 full-time employees worldwide, Mozilla Corporation employee compensation is benchmarked to market by role and level balancing total compensation between individual and company performance with a pay-for-performance compensation model.

For non-executive roles, we employ a market framework of 20 top public and private tech companies that we compete with for talent.

For VPs and above, we benchmark compensation against a blended peer group comprised of 70% similarly-sized public and private tech companies and 30% non-profit organizations. This approach serves to reinforce our mission-first orientation. Consistent with market

Redacted

MOZ-000412



best practice, at least 70% of compensation for senior leadership is “at risk” and tied to individual and company performance.

## **Mozilla Foundation**

Mozilla Foundation non-profit programs are carried out by 80 employees and thousands of volunteers around the world. For the Mozilla Foundation, the core goal of the compensation philosophy is to attract, motivate and retain top talent while ensuring total pay is competitive and reasonable in relation to our nonprofit status. We benchmark against a peer group that reflects the unique nature of our organization and aim to provide an appealing, flexible and market-appropriate total compensation package.

## **Mozilla Corporation and Mozilla Foundation: Fostering Growth: Financials (990 & Audit)**

The combined efforts of the Mozilla Foundation and Mozilla Corporation contribute to the overall sustainability and health of the internet. As always, revenue from Mozilla Corporation and donations to Mozilla Foundation are reinvested into advancing the Mozilla mission of protecting internet health. Firefox users and Mozilla Foundation contributors also have the knowledge that they are supporting the Mozilla mission with their payments and contributions.

This annual report includes the below links that detail audited 2018 financial statements for Mozilla.

Redacted

MOZ-000413



Today, the majority of Mozilla Corporation revenue is generated from global browser search partnerships, including the deal negotiated with Google in 2017 following Mozilla's termination of its search agreement with Yahoo/Oath (which was the subject of litigation the parties resolved in 2019.)

In CY 2018, Mozilla Corporation generated \$435.702 million from royalties, subscriptions and advertising revenue compared to \$542 million in CY 2017. 2017 was an outlier, due in part to changes in the search revenue deal that was negotiated that year. Despite the year-over-year change, Mozilla remains in a strong financial position with cash reserves to support continued innovation, partnerships and diversification of the Firefox product lines to fuel its organizational mission.

A portion of search revenue combined with grants and donations is used to fuel the advocacy and movement building work of the Mozilla Foundation and its broad network of supporters of Mozilla's mission.

## **Join Mozilla**

Our mission is to ensure the internet is a global public resource, open and accessible to all. This mission is as important now as it has ever been. We urge everyone who is interested to find a way to contribute to protecting the internet. We invite you to download Firefox or volunteer to be part of Mozilla or donate to support the work of internet health leaders around the world. Learn more at mozilla.org.



## 2018 AUDITED FINANCIAL STATEMENT

[Download PDF](#)

## 2018 FORM 990

[Download PDF](#)

**moz://a**

### Company

[About](#)

[Press Center](#)

[Careers](#)

### Developers

[Test New Features](#)

[MDN Web Docs](#)

[Tools](#)

### Resources

[Privacy](#)

[Contact](#)

### Product Help

[Support](#)

[File a Bug](#)



Redacted

MOZ-000415



Visit [Mozilla Corporation's](#) not-for-profit parent, the [Mozilla Foundation](#).

Portions of this content are ©1998–2020 by individual mozilla.org contributors. Content available under a [Creative Commons license](#).

[Privacy](#)

[Website Privacy Notice](#)

[Cookies](#)

[Legal](#)

[Community Participation Guidelines](#)

Redacted

MOZ-000416