# Online Privacy and Security

**A healthy Internet is private and secure.** Internet users should be able to have greater choice over what information they share with what organizations and for what benefit. They should have the freedom to express themselves online without unwarranted surveillance. And, they should be able to safeguard their information against attacks.

**From the Mozilla Manifesto:**

**#04: Individual's security and privacy on the Internet are fundamental and must not be treated as optional.**

**#09: Commercial involvement in the development of the Internet brings many benefits; a balance between commercial profit and public benefit is critical.**

The Internet powers countless aspects of society and the economy. As users, we create a lot of personal information in the course of living our everyday digital lives. We need to be able to trust the online companies and services that handle that data to safeguard our privacy interests.

The concept of "privacy" means different things to different people. It's personal and varies by the individual, and it's also context-dependent. It's an umbrella concept that encompasses a range of issues that all speak to Internet users' ability to trust and shape their online experience—security, transparency and control of data by and about us, when it is collected and/or used by private or public entities.

While the desire for privacy and security remains strong, many Internet users still find it difficult to protect their information effectively, and confidence in the organizations meant to provide that protection is eroding. **A recent Pew study** showed that 74% of Americans think it is "very important" that they be in control of who can get information about them. Yet, 91% of adults also agree or strongly agree that consumers have lost control of how personal information is collected and used by companies. And while 86% of Internet users have taken steps to remove or mask their digital footprints, 61% say that they would like to do more.

One of Mozilla's founding principles is the idea that security and privacy on the Internet are fundamental and must not be treated as optional. This core value underlines and guides all of Mozilla's work on online privacy and security issues—including our product development and design decisions and policies, and our public policy and advocacy work.

*This is part of a series of briefs intended to provide more depth into Mozilla's thinking and actions on five key issues that comprise Internet health. Their objective is to educate, to guide, and to inspire action. They are meant to be illustrative, rather than exhaustive.*

**Key topics in online privacy and security:**

Meaningful user control · Data collection and use · Government surveillance

Cybersecurity · Read more

# Meaningful user control

> People care about privacy. But many don't understand the threats to their privacy, or what actions they can take to be more secure.

For many years, the corporate approach to privacy wasn't innovative: companies would simply give users notice (about practices) and choice (about how they interact with the service, or whether they use it at all). But click-through wrappers and privacy policies for services that are often seen as mandatory have left some users feeling uninformed and powerless. Users lack meaningful choice because of a lack of transparency and understanding.

Putting control back in the hands of users requires investment in both technology and education. We need technologies and services that make it easy for everyday Internet users to understand how using those tools could impact their privacy—and what choices they have.  We work to build understanding and control into our own products, such as through **tracking protection in private browsing mode** and in **Firefox Focus**. We seek opportunities to go bigger, to make privacy the asset that it is.

Technology needs to be complemented by a bottom-up approach, focused on users through education, awareness and community building. At Mozilla, we build teaching kits, guides and other resources to help raise the level of understanding - and our global community localizes these resources and creates their own to have an even broader reach. Increasingly, powerful technologies like Tor are helping to return control to users; but broader awareness and understanding require significantly more work.

In the years to come, the challenges to understanding data collection will continue. More data is being generated by more devices that touch more parts of our lives. But that expansion also creates more opportunities for innovation, education and empowerment of Internet users. It's that gap Mozilla intends to help fill.

## Data collection and use

> The tech industry, too often, reflects a culture of 'collect and hoard all the data'. To preserve trust online, it's time to change that.

The technology industry has a long way to go on data privacy practices. Incentives in many corners of the industry reward collecting all possible data and storing it, with or without business use, in case it can be monetized to greater value later. This casual, even callous, attitude jeopardizes both users and businesses, and undermines trust online.

Paired with Mozilla's push for user awareness, we are working to get the industry on track. We lead by example with product innovation, such as tracking protection. We also educate and advocate industry and policymakers about the importance of better data practices for earning trust, and the significance of that trust for economic health and growth. We've also developed "**Lean Data Practices**" to offer a framework to new Internet businesses, to help them establish their data practices more thoughtfully from the get-go.

These challenges will continue, diversify and grow in the years to come, in part through the so-called "Internet of Things". In parallel, regulatory pressure will grow, creating a new source of pressure for companies and individuals to take data practices seriously. Mozilla will strive to build good practices into products, and lead the industry on privacy.

## Government surveillance

Public distrust of government is high as a result of broad surveillance practices. More transparency, accountability and oversight are part of much needed reform.

We expect our private data to be private, and government actions that encroach on our privacy and security to be legitimate and tailored to the technologies and needs of specific contexts. Since the Snowden revelations emerged in 2013, Internet users around the world have been calling for governments to rein in aggressive online surveillance practices. Yet national security, intelligence and law enforcement are powerful counterweights, with legitimate interests.

Mozilla's core approach is to focus on the security of users as a shared objective of businesses and government actors, recognizing that some forms of government surveillance and the mechanisms used for those practices undermine user security. We champion and engineer encryption to help protect data from interception. Where government surveillance practices undermine our security and privacy interests, we oppose them through policy and advocacy. We emphasize transparency, oversight and accountability as ways to unlock public policy discussions around government surveillance, and take the important conversations out from behind closed doors and classified systems, to the public.

Public reactions to the Snowden revelations have generated meaningful initial progress. In reaction to those reactions, though, many countries have introduced legislation that would make their surveillance environments worse. In particular, mandatory data retention, bulk data collection and various methods of undermining secure encryption are still heavily pushed by many government officials, putting companies in complicated positions of challenging these orders (where they can) or risking their users' trust and rights. We'll continue our diverse efforts to try to maintain or improve on the status quo substantively around the world, while delivering positive gains for transparency and public engagement with good government practices.

# Cybersecurity

Cybersecurity is user security. It's about our Internet, our data, and our lives online. And making it a reality is and must be a shared responsibility.

The Internet is not as secure as it needs to be. We see steady headlines of attacks, viruses, hacking, phishing and other breaches of the security of our data and our communications. Internet security is difficult - it's a long chain where each link needs to be tested and re-tested, and one weakness puts users at risk. The only sustainable way to improve cybersecurity is to treat it as a shared responsibility, where users, businesses, and government must work together.

At Mozilla, we work to encourage all three of these sectors to do their part. We build educational resources and campaigns to help teach users about passwords and encryption, and how to defend as best they can against attack. We build security into our products and develop it in standards bodies, and we support the security of the broader open source ecosystem through our **Secure Open Source Fund**. We engage actively with government officials in several countries around the world to get them to do their part, by opposing proposals that would undermine encryption and security, and by adopting transparent and accountable policies for handling of security vulnerabilities.

In the years to come, security problems will almost certainly continue, and even grow worse. Attacks will continue to be cheap to acquire and deploy, users will continue to take action (and inaction) that puts themselves and others at risk, and some policymakers will continue to seek intentional, myopic weakening of security online. So, Mozilla will continue to target policy, technical and market solutions to improve defense and encourage broad acceptance of - and delivery on - the shared responsibility of all parties.

# Read More

Ensuring people’s right to privacy and security is a big hill to tackle. But we’re working on closing gaps in understanding, and building public respect and expectation for the secure, open Internet. We frequently work with like-minded organizations when taking on these issues on behalf of and for Internet users, be it through our products, as part of the bigger movement, or advocating for change in the halls of government.

## You can explore their thinking below:

**Electronic Frontier Foundation (EFF)**

**Open Technology Institute (OTI)**

**Center for Democracy & Technology (CDT)**