Abine Fact Sheet

About Abine

Your privacy is our business.

The web is an amazing place, but like water on stone, it slowly erodes your privacy with every site you visit. It’s a delicate balancing act to ensure both a rich, full web experience and protect your privacy, but that’s what we do every day at Abine. Whether you’re shopping, learning, playing, or creating, we strive to make your web experience better by preserving all the Internet has to offer, while putting you in control of your personal information. Millions of people have taken action using Abine’s simple tools and services to control how their information is collected, stored, shared, and sold.

So whether you’re looking to learn a little bit more about improving your privacy or ready to take big action, we’d love to help. Because at Abine, online privacy starts here.

What We Believe

● We believe that people should get to choose when to share their information.

● We believe people care deeply about their privacy and have a right to protect it.

● We believe technology solutions that improve online privacy should be accessible to everyone.

● We believe that the web is better when you have more control over your personal data.
Fast Facts

- **2009**: Founded by MIT engineers and financial experts
- **2011**: Received $6 million in Series A funding from General Catalyst Partners and Atlas Ventures (now Accomplice)
- **May 2012**: 1 million DoNotTrackMe downloads
- **March 2013**: 4 million DoNotTrackMe downloads; 3 billion+ tracking attempts that DoNotTrackMe has blocked advertisers from carrying out against our users
- **July 2013**: Launched MaskMe with a “spectacular” 5-star review on CNET
- **January 2015**: Launched Blur; a combined and streamlined version of DNTMe + MaskMe
- **January 2016**: Partnered with multiple fortune 500 companies to provide DeleteMe service as an employee benefit
- **Today**: Millions of monthly active Blur users; tens of thousands of DeleteMe subscribers

Why Online Privacy Matters Today

Privacy lets us be ourselves. It’s the ability to control our information. It gives us power over what people know about us.

With privacy, we can speak more freely and explore our curiosities. We don’t worry that what we say today might come back to hurt us in the future. We know who has our data and how they’re using it, from hiring to credit determinations to online dating.

Privacy is about having power and control over one’s personal information, which gives us the protection to act freely. It’s not about having something to hide, but having something to live for.

We love the Internet, and we want the Internet of the future to be one where people have much more control over how their information is collected and stored. That’s why we’re at the forefront of a movement to protect consumers’ fundamental right to privacy at a time when it’s dwindling away. Online tracking, consumer profiling, and data collection are happening wherever consumers go on the web, usually without their knowledge or approval. We’re on the side of consumers, helping them get the control they want over their personal information while still being able to use the web they love.
Research & Resources

Tracking

- **Tracker**: A tracker is a connection that your browser makes when it loads a webpage that’s intended to record, profile, or share your online activity. Usually these connections are made to entirely different companies than the website you’re actually visiting. The most common types of trackers are:
  - JavaScript: 43%
  - Images, such as 1-pixels: 14%
  - iFrames: 14%
  - Flash cookies: 5%

Abine collaborates with the UC Berkeley Center for Law and Technology on a recurring Web Privacy Census. The most recent Census found:

- The use of third-party tracking cookies on the 100 most popular websites
  - Increased by 13% from 2015 to 2016.
  - If present trends continue, the amount of online tracking will *double* in about 2 years.
- Google has a presence on 712 of the top 1,000 websites
  - 26.3% of what your browser does when you load a website is respond to requests for your personal information, leaving the remaining 73.7% for things you actually *want* your browser doing, like loading videos, articles, and photos.
    - Google makes 20.28% of all tracking requests on the web
    - Facebook makes 18.84% of all tracking requests on the web
    - 75% of the top 1,000 websites use social networking code that can match users’ online identities with their web browsing activities, and nearly 25% of the web’s 70 most popular sites shared personal data, like name and email address, with third-party companies. (Wall Street Journal).

Consumer Feelings about Privacy

- Privacy isn’t binary, no matter how much experts try to convince you it is. Individuals have a nuanced sense of privacy, and the degrees to which it matters in certain circumstances. Our willingness to share data with others -- from people to government to businesses -- isn’t static, and our motivations to share information vary widely. (Forbes, Forrester, 12/14, 2016)
- A majority of people are willing to share their personal information -- when there’s a value exchange. In fact, 67% of consumers are willing to share some information with companies, although the types of companies they trust vary, as do the benefits they expect in exchange. Sadly, those who are unwilling to share simply don’t understand the depth and breadth of the consumer data ecosystem, and for them, privacy breaches and "creepy" experiences can be particularly distressing and badly damaging to brand loyalty. (Forbes, Forrester, 12/14, 2016)
- 64% of Americans have personally experienced a major data breach. (Pew Research, 1/26/17)
- 49% feel that their personal information is less secure than it was 5 years ago. (Pew Research, 1/26/17)
- 41% of Americans have dealt with fraudulent charges on their credit card. (Pew Research, 1/26/17)
- 16% of Americans say that someone has taken over their email accounts, and 13% say someone has taken over one of their social media accounts. (Pew Research, 1/26/17)
- 15% of Americans have received notices that their Social Security number had been compromised. (Pew Research, 1/26/17)