What is Tor? A beginner's guide to the privacy tool

The anonymity software has sparked controversy but who built it, what is it used for, what browser does it use – and why is the NSA so worried by it?

Stuart Dredge

Tuesday 5 November 2013 07.47 EST

Until this year, the internet privacy tool Tor was scarcely heard of outside the tech community. Since revelations about the surveillance strategies of US and UK spies, Tor has become a focus of criticism, accused of facilitating a dangerous "dark web" of paedophiles, drug dealers and arms traders.

But while the NSA has tried to crack its security, Tor's principal source of funding has been other parts of the US government. While a criminal contingent may use the site to disguise identities, its creators point to a wider group of legitimate users including journalists, activists, law enforcement professionals, whistleblowers and businesses.

In a year Tor has grown from 500,000 daily users worldwide to more than 4 million users, provoking an increasingly public debate along the way.

What is Tor?

The Tor project is a non-profit organisation that conducts research and development into online privacy and anonymity. It is designed to stop people – including government agencies and corporations – learning your location or tracking your browsing habits.

Based on that research, it offers a technology that bounces internet users' and websites' traffic through "relays" run by thousands of volunteers around the world, making it extremely hard for anyone to identify the source of the information or the location of the user.

Its software package – the Tor browser bundle – can be downloaded and used to take advantage of that technology, with a separate version available for Android smartphones.

There are some trade-offs to make: for example, browsing using Tor is slower due to those relays, and it blocks some browser plugins like Flash and QuickTime. YouTube videos don't play by default either, although you can use the "opt-in trial" of YouTube's HTML5 site to bring them back.

Who created Tor?

The original technology behind Tor was developed by the US navy and has received about 60% of its funding from the State Department and Department of Defense, although its other backers have included digital rights lobbyist the Electronic Frontier Foundation, journalism and community body Knight Foundation and the Swedish International Development Cooperation Agency.

When it launched in 2002, the Tor project's emphasis was on protecting internet users' privacy from corporations rather than governments.

"We were increasingly concerned about all these websites - in the 2000/01 dotcom bubble, everyone was offering free services, and by free they meant 'we take all your information and sell it as many times as possible'," executive director Andrew Lewman told the Guardian in April 2012.

"We wanted a way to: one, put some of our research into practice and see how it would work; and two, we wanted to give the control over your information to you, the user, not to have all these companies take it by default. And let you take decisions about do you trust Google, do you trust Amazon, do you trust the BBC, whatever."

Who uses Tor?

The Tor project team say its users fall into four main groups: normal people who want to keep their internet activities private from websites and advertisers; those concerned about cyberspying; and users evading censorship in certain parts of the world.

Tor notes that its technology is also used by military professionals – the US navy is still a key user – as well as activists and journalists in countries with strict censorship of media and the internet. Campaigning body Reporters Without Borders advises journalists to use Tor, for example.

Tor also cites bloggers, business executives, IT professionals and law enforcement officers as key users, with the latter including police needing to mask their IP addresses when working undercover online, or investigating "questionable web sites and services".

For more mainstream users, it could mean running Tor so that your children's location can't be identified when they are online, or could mean a political activist in China, Russia or Syria could protect their identity.

After the NSA surveillance revelations in 2013, a new wave of users joined the service. Between 19 August and 27 August alone the number of people using Tor more than doubled to 2.25 million, according to Tor's own figures, before peaking at nearly 6 million in mid-September. It has since slipped back to just over 4 million.

The dark side of Tor

The cloak of anonymity provided by Tor makes it an attractive and powerful for criminals. Another NSA document described it thus: "Very naughty people use Tor".

Tor can mask users' identities, but also host their websites via its "hidden services" capabilities, which mean sites can only be accessed by people on the Tor network. This is the so-called "dark web" element, and it's not unusual to see Tor pop up in stories about a range of criminal sites.

In August, a service provider called Freedom Hosting went offline after the FBI sought the extradition of a 28-year-old Irish man for charges relating to distributing and promoting child abuse material online.

Underground illegal-drugs marketplace Silk Road, which was shut down in early October, was another hidden site only accessible through Tor, as was another store called Black Market Reloaded which has been accused of facilitating illegal arms dealing as well as drug purchases.

Sites such as these are why Tor was recently described by British MP Julian Smith as "the black internet where child pornography, drug trafficking

and arms trading take place" during a parliamentary debate on the intelligence and security services.

Smith went on to criticise the Guardian for reporting in detail on the claims that the NSA had been trying to crack Tor's security, suggesting that "many people in the police world feel will cause major issues in terms of picking up people engaged in organised crime".

Law enforcement co-operation

In the past, the team behind Tor has responded to exactly this question, denying that the anonymity tool is an obstacle to police investigating criminal activities.

"We work with law enforcement a lot," Lewman told the Guardian. "They are fully aware of bad guys on Tor. However, the criminals already have all the privacy they could ever need, because they're willing to break the laws: they're willing to steal identities, they're willing to hack into machines, they're willing to run botnets."

"People sort of hear 'Tor' and think 'forget it, I'll never solve this case', but really there's a human at the other end, and that's what the law enforcement targets most of the time. Humans make mistakes, they do silly things, trust the wrong things, and that's how they've caught nearly everyone who uses Tor as part of their illegal schemes."

In the UK, law enforcement agencies had been investigating hidden services on Tor for some time before the Guardian's reports. On 22 July, David Cameron delivered a speech to the NSPCC talking about plans to integrate the UK's Child Exploitation and Online Protection Centre (CEOP) into the national crime agency.

"Once CEOP becomes a part of the national crime agency, that will further increase their ability to investigate behind the paywalls, to shine a light on this hidden internet and to drive prosecutions and convictions of those who are found to use it," said Cameron. "So we should be clear to any offender who might think otherwise, there is no such thing as a safe place on the internet to access child abuse material."

In a recent blogpost responding to the Freedom Hosting news, Tor also pointed out that hidden services aren't just used by criminals, pointing to organisations using the technology to "protect dissidents, activists, and protect the anonymity of users trying to find help for suicide prevention, domestic violence, and abuse-recovery."

Does Tor still work?

Questions about Tor's use by good and/or bad guys are one thing, but as more people become aware of it, another sensible question is whether it works, particularly in the light of the NSA repeatedly developing attacks against Tor. That appears to have been a frustrating task.

"We will never be able to de-anonymise all Tor users all the time," said "Tor Stinks", an NSA presentation from June 2012. "With manual analysis we can de-anonymise a very small fraction of Tor users, however, no success de-anonymising a user ... on demand."

For its part, Roger Dingledine, the president of the Tor project, said following the Guardian's publication of that presentation that "there's no indication they can break the Tor protocol or do traffic analysis on the Tor network", while reminding users that humans remain the weak links in online communications.

"Infecting the laptop, phone, or desktop is still the easiest way to learn about the human behind the keyboard. Tor still helps here: you can target individuals with browser exploits, but if you attack too many users, somebody's going to notice. So even if the NSA aims to surveil everyone, everywhere, they have to be a lot more selective about which Tor users they spy on."

The NSA's attacks against Tor included targeting security holes in the Firefox web browser. Tor encourages users of its Tor Browser Bundle to upgrade to the latest version regularly, to ensure they have the latest security fixes for the software.

What next?

Security expert Bruce Schneier recently made anonymisation tools such as Tor the first step in his advice on "how to remain secure against the NSA". But this kind of technology will not stand still in the coming months and years, as the attempts to crack it get smarter and more persistent.

Though Tor is likely to appeal to more sophisticated internet users, public concern over government and corporate surveillance and tracking is likely to mean it becomes more widely used by mainstream internet users.

"Browser exploits, large-scale surveillance, and general user security are all challenging topics for the average internet user," Dingledine said.

"These attacks make it clear that we, the broader internet community, need to keep working on better security for browsers and other internet-facing applications."

Tor 'deep web' servers go offline as Irish man held over child abuse images

Topics

Internet Data protection Software Computing Privacy Surveillance