

Privacy in a Future that is Forever

by [Alissa Cooper](#) [1]
June 7, 2012

The Internet is running out of address space and it appears that the solution has narrowly avoided a technical issue that carried serious implications for consumer privacy.

The Internet's inventors never imagined it would explode to become a global tool linking billions of computers and phones. As a result the addressing format they originally designed – known as IPv4 – has nearly maxed out the possible number of addresses it can supply. So a new system—[IPv6](#) [2]—was designed to provide an almost endless number of addresses.

Yesterday began the [World IPv6 Launch](#) [3], with Internet service providers, web sites, and equipment vendors around the globe turning on IPv6. Some companies are further along in their adoption of the new addresses than others, but ultimately we will all need to transition to IPv6 to ensure that all Internet devices can talk to each other.

As part of World IPv6 launch, Internet companies large and small – including AT&T, Cisco, Comcast, Facebook, Google, Microsoft, Verizon Wireless, and Yahoo! – committed to turning on IPv6 and leaving it on (the launch's tag line is "the future is forever"). A small fraction of Internet users and devices have started communicating via IPv6, with more and more making the transition over the coming months and years.

As our devices make the switch to IPv6, they will be assigned new IP addresses in the IPv6 format. IPv6 addresses can be generated in a number of different ways and the choice of how they are created has potentially wide reaching effects for privacy. One of the original methods for assigning new addresses involved using a unique device identifier (known as a MAC address) as the suffix of the [IPv6 address](#) [4]. This method creates a permanent, unique address for a device, potentially allowing any server that the device communicates with to indefinitely track the user.

IPv6 designers soon realized the potential privacy problems of MAC-based addresses; as a result, they created an [alternate method](#) [5] known as "privacy extensions" or "privacy addresses." The privacy extensions use a randomly generated number instead of a MAC address. The random number is unrelated to any device identifier and in practice lasts no more than a week (and often much less time), ensuring that the user's IP address cannot be used for long-term user tracking.

It is up to operating system vendors to choose which IP address assignment method will be the default on their devices. Fortunately they have made good choices, particularly within the last year. Microsoft has long led the charge on IPv6 privacy, with privacy extensions on by default in all versions of Microsoft Windows since the release of Windows XP nearly a decade ago. Apple followed suit last year, with privacy extensions activated by default in all versions of Mac OS X since 10.7 (Lion) and with the release of iOS 4.3 for iPhone and iPad. Google did likewise in its Android 4.0 release last year.

As long as Internet users choose to upgrade their operating systems to the latest versions, they should be protected against perpetual tracking by IP address as the Internet moves into the IPv6 future.

-
- [IPv6](#)



- [Internet](#)
- [Consumer Privacy](#)

The copyright © 2013 by the Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL: <https://cdt.org/blogs/alissa-cooper/0706privacy-future-forever>

Links:

- [1] <https://cdt.org/personnel/alissa-cooper>
- [2] <http://en.wikipedia.org/wiki/IPv6>
- [3] <http://www.worldipv6launch.org/>
- [4] <http://tools.ietf.org/html/rfc2464>
- [5] <http://tools.ietf.org/html/rfc4941>