access accessnow.org

The Rise of Mobile Tracking Headers: How Telcos Around the World Are Threatening Your Privacy

Access is an international organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

For more information or assistance, please contact info@accessnow.org.
For media inquiries, contact press@accessnow.org.

Mobile broadband serves as a crucial means of accessing the internet for hundreds of millions of people around the globe. And for many users, mobile devices provide the only way of going online. Their devices serve as gateways to information, resources, and innovation, but they can also leak intimate details about the users themselves. In 2014, security researchers provided a key insight into how companies were using these data when they revealed that mobile carriers in the U.S. were secretly monitoring the web browsing habits of their users.[1] The researchers found Verizon Wireless and AT&T using so-called supercookies — special tracking headers that the carriers inject beyond the control of the user. These revelations led to an investigation by the U.S. Federal Communications Commission,[2] action by legislators in the U.S. Congress,[3] and several lawsuits.[4] Despite these small victories, tracking headers are still being used around the world, and important questions remain. How extensive is the use of these tracking headers? What kind of information have carriers been collecting with them? Does their use violate users' privacy? And what should be done about them, if anything?

To call attention to the practice and to better understand tracking headers, Access built a tool at **Amibeingtracked.com** that allows users to test their devices to see if they are being tracked. Since its launch in October 2014, more than 200,000 people from around the world have used the tool, and the results are startling. This report presents results of nearly 180,000 tests conducted in the first six months, along with our major findings about the use of tracking headers worldwide, and it provides our recommendations for governments, carriers, websites, intergovernmental bodies, and researchers.

(1) McMillan, R. (2014, October 27). Verizon's Perma-cookie is a 'privacy killing' machine. *Wired*. Retrieved from http://www.wired.com/2014/10/verizons-perma-cookie/

(2) Goldstein, P. (2015, April 15). FCC is probing Verizon's 'super cookie' used to track mobile browsing. *Fierce Wireless*. Retrieved from http://www.fiercewireless.com/story/fcc-probing-verizons-super-cookie-used-track-mobile-browsing/2015-04-10

(3) Hojek, H. (2015, February 6). Senators urge FCC to investigate Verizon Wireless 'super cookies'. *NBC 2*. Retrieved from http://www.fiercewireless.com/story/fcc-probing-verizons-super-cookie-used-track-mobile-browsing/2015-04-10

(4) Davis, W. (2015, June 8). Verizon Should Stay Out Of 'Supercookie' Lawsuit, Consumers Say. *MediaPost*. Retrieved from http://www.mediapost.com/publications/article/251503/verizon-should-stay-out-of-supercookie-lawsuit.html

Download the full report at https://www.accessnow.org/trackingreport

Key Findings

Evidence of widespread deployment	Carriers in 10 countries around the world, including Canada, China, India, Mexico, Morocco, Peru, the Netherlands, Spain, the United States, and Venezuela, are using tracking headers
	The following mobile carriers are using tracking headers: AT&T, Bell Canada, Bharti Airtel, Cricket, Telefonica de España, Verizon, Viettel Peru S.a.c., Vodafone NL, and Vodafone Spain
	15.3% of those who used our tool were being tracked by tracking headers
	Carriers around the world are using multiple types of tracking headers, all of which have distinct structures
Correlative evidence exists that tracking headers may have been used by carriers for more than a decade	We found information indicating the use of tracking headers dating back 15 years
Users cannot block tracking headers because they are injected by carriers beyond their control	Users cannot block tracking headers, because they are injected by carriers out of reach at the network level
	"Do not track" tools in web browsers do not block the tracking headers
	Tracking headers can attach to the user even when roaming across international borders
	Even if tracking headers are not used by the carrier itself to sell advertising, other firms can independently identify and use the tracking headers for advertising purposes
Encrypted connections to websites stop tracking headers from functioning	Tracking headers do not work when users visit websites that encrypt connections using Secure Socket Layer (SSL) or Transport Layer Security (TLS) (demarcated by "HTTPS" in a web address)
	Tracking headers depend upon an HTTP, or unencrypted connection, to function, and may lead to fewer websites offering HTTPS
Tracking headers leak private information about users and make them vulnerable to criminal attacks or even government surveillance	Certain tracking headers leak important private information about the user in clear text, including phone numbers
	Although we do not have evidence that criminal attacks have occurred, clear text leaks of phone numbers and other identifying information make tracking headers ripe for exploitation by criminals
	Although we do not have evidence that government surveillance has taken place, the rich data profiles about users that tracking headers create make them prime targets for government legal requests or surveillance
Tracking headers raise troubling questions about privacy as new technologies are developed	Carriers have changed their behavior because of public pressure or because of changes in technology
	Current trends suggest that tracking headers will grow in use or will be replaced by a new tracking technology

Recommendations

Government authorities	Appropriate authorities, including data protection and consumer rights regulators, should investigate the use of tracking headers in every country
	Authorities should hold carriers accountable for false or misleading statements or practices regarding tracking headers
	Authorities should require carriers to provide affected users with an adequate remedy, and to make guarantees of non-repetition
Carriers	All carriers should publicly disclose their use of tracking headers and not enroll users by default for any reason, such as advertising
	Any use of tracking headers or similar tracking technology should require users to clearly, specifically, and explicitly opt-in, after being fully informed of the potential risks
	Carriers must provide a clear, easy-to-use opt out mechanism for users, regardless of whether they previously opted in.
	Carriers that commit to stopping the use of tracking headers in one country or region should commit to stop using them in other countries or regions where they have operations
	Industry associations like the GSM Association should study the harms that tracking headers present, and advise members to strictly circumscribe their use
	Carriers should utilize Access' **Telco Action Plan** for further guidance on how to respect the privacy of users[5]
	Carriers should consider joining multistakeholder groups, such as the Global Network Initiative, that assess progress in meeting privacy and freedom of expression benchmarks based on international human rights laws and standards
Websites and Apps	Websites and apps should use encrypted HTTPS connections by default
	Companies should sign on to Access' **Digital Security Action Plan** to support basic steps to protect users against unauthorized access[6]
Intergovernmental bodies	United Nations experts, including special procedures mandate holders, should investigate the use of tracking headers as a threat to user rights
	Governments in the Freedom Online Coalition should take steps to ensure that carriers in their countries do not inject tracking headers
	Technical standards bodies should ensure that existing and future standards do not enable tracking headers or similar technologies that may threaten user privacy
Researchers	To identify more carriers using tracking headers, larger data samples are needed from around the world
	Researchers should consider means of collecting data other than a standalone site, such as developing code for individual website owners to install, with appropriate privacy and anonymity protections built in
	Researchers should seek to uncover the form and structure of new tracking mechanisms that may replace tracking headers

(5) Access. Telco Action Plan. (2012, March). Retrieved from https://s3.amazonaws.com/access.3cdn.net/1f9ab2891a86f3f081_uom6iil1w.pdf

(6) Access. Digital Security Action Plan. (2015). Retrieved from https://encryptallthethings.net/docs/EATT.pdf