August 2015

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

A publication of

access

accessnow.org

The authors of this report are Nader Ammari, Gustaf Björksten, Peter Micek, and Deji Olukotun.

They would like to thank the following individuals and organizations for their valuable feedback and input: Laura Moy, Jacob Hoffman-Andrews, and Kenn White.

Visual design by Anqi Li and Olivia Martin.

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.

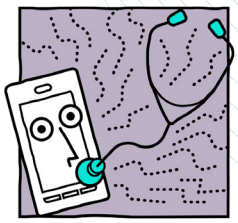
www.accessnow.org

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

Table of Contents

Executive Summary

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?



Amibeingtracked.com

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

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

Full Report

Mobile broadband serves as a crucial means of accessing the internet for hundreds of millions of people around the globe. Sixty-four percent of adults in the U.S. owned smartphones in 2015.[7] Many mobile phone users do not realize that when they access the internet through their devices they are sharing copious amounts of information with carriers or third parties. As a result, this kind of connectivity raises important concerns about privacy.

In October 2014, security researchers exposed a special code used by Verizon Wireless to track its users. Labeled by the media as "supercookies," the code was special tracking headers that Verizon injected into every single HTTP web request that users made through their mobile devices. It was not immediately clear how Verizon was using the tracking headers, and the revelations raised important questions about their structure and deployment.

Access is an international organization that defends and extends the digital rights of users at risk around the world, and our work with telecoms began during the Arab Spring uprisings in 2011. What happened during that tumultuous period exposed the integral role that these corporations and their regulators play in connecting us to the internet, a tool that is now essential to the exercise of human rights in the 21st Century.

Governments struggle to maintain sufficient regulatory oversight in the face of rapidly adopted and fast-changing technology. But carriers must recognize that people are increasingly aware of and concerned about privacy and security issues. The legal, financial, and public relations fallout from invading privacy is growing, and movements to hold corporations accountable for infringing human rights are gaining steam around the world. It is in the best interest of carriers, both in the short and long term, to stop tracking and exploiting people's information without their knowledge or consent, whether or not current regulations ban the practice. There are more ethical ways to gather information, such as giving customers a true opt-in after informed consent.

Using tracking headers also raises concerns related to data retention. When "honey pots" of sensitive information, such as data on browsing, location, and phone numbers, are collected and stored, they attract malicious hacking and government surveillance. This kind of collection and retention of user data is unsustainable and unwise, and creates unmanageable risks for businesses and customers alike.

In response to the revelations about the use of tracking headers by Verizon Wireless, Access developed an online tool called Amibeingtracked.com that lets people test whether their mobile carrier is using tracking headers to log their internet activity. We collected the results of nearly 180,000 tests over a six-month period from people around the world.

(7) Smith, A. (2015, April). U.S. Smartphone Use in 2015. Pew Research Center. Retrieved from http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/

What is a tracking header?

Tracking headers are *not* cookies

Although tracking headers are popularly called "supercookies," "zombie cookies," or "perma-cookies," these terms are inaccurate. Cookies are injected locally and can be manipulated by end users in a web browser. Tracking headers are in fact not cookies at all because they are injected at the network level, out of the reach of the user. A more accurate term would be Carrier-Injected HTTP Header. For the sake of simplicity, and to avoid creating yet another acronym, we will refer to "Carrier-Injected HTTP Headers" as simply "tracking headers" throughout this report.

How they work: users cannot block tracking headers because they are injected by carriers beyond their control

Headers are an essential part of internet communications. When you use the internet on a mobile device, you normally transmit one or more unique identifiers — including IMEI, [8] IMSI, [9] and ICCID[10] identities — that include information about who you are and where you are located. But tracking headers go beyond such normal data sharing. To explain how they function, we'll use the example of a hypothetical character named Kavita:

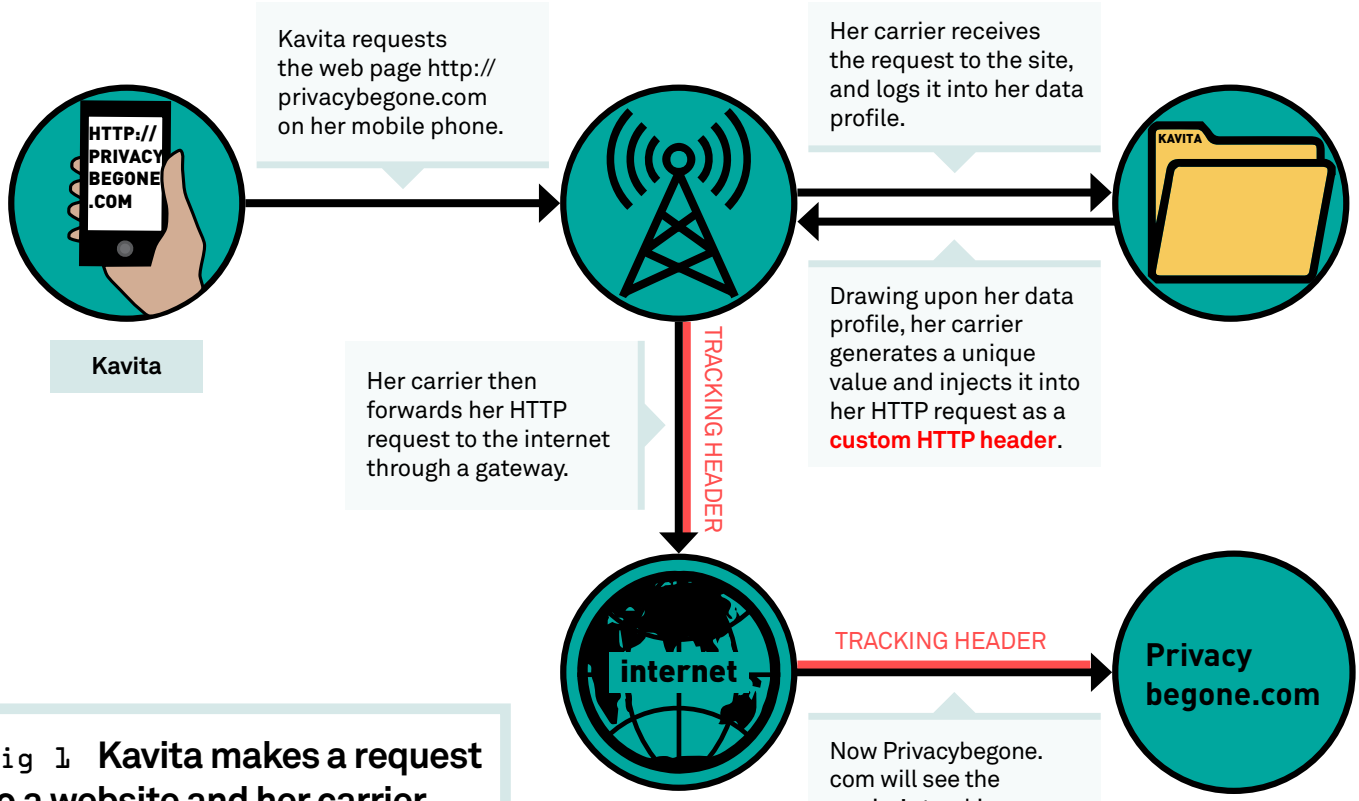


Fig 1 **Kavita makes a request to a website and her carrier injects an HTTP header.**

(8) International Mobile Station Equipment Identity.

(9) International Mobile Subscriber Identity.

(10) Integrated Circuit Card Identifier.

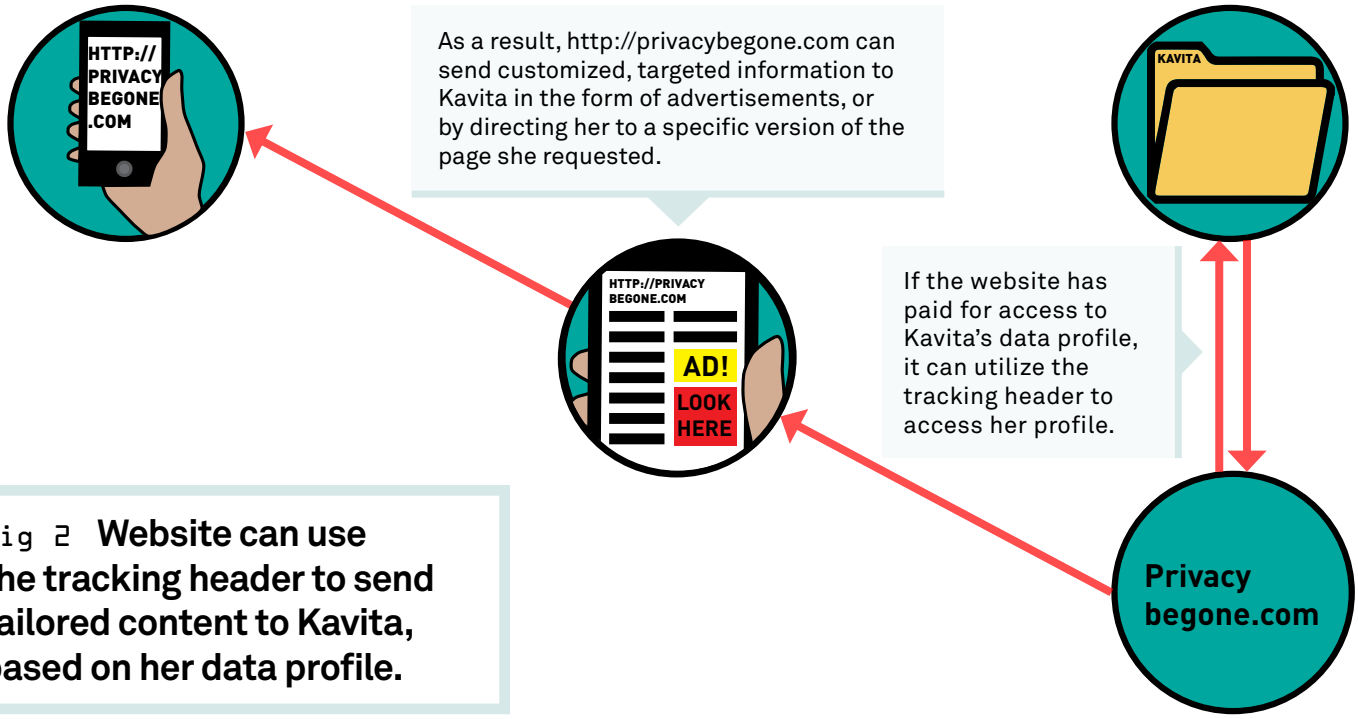


Fig 2 **Website can use the tracking header to send tailored content to Kavita, based on her data profile.**

Evidence of tracking headers dates back to 2000

Our research conducted online confirms the existence and use of tracking headers as early as 2000. Our research shows that tracking headers were associated with Sprint[11] in February of 2000, and discussions[12] at the time indicate that they were also used by the carrier O2 in the United Kingdom. In 2006, there was discussion about x-up-subno, a particular type of tracking header that is used by Bell Canada. Four years later, in March 2010, the researcher Collin Mulliner discussed his research on tracking headers in a paper[13] announced at the CanSecWest conference in Vancouver, Canada. However, as we mentioned earlier, tracking headers began drawing widespread popular attention only after an article published in *Wired* in October 2014 revealed that Verizon Wireless had begun to use Unique Identifier Headers (UIDH).[14]

Access' response

After Verizon Wireless's use of tracking headers was revealed in 2014, Access mobilized its members, urging them to sign a petition asking both the U.S. Federal Communications Commission (FCC) and Federal Trade Commission (FTC) to investigate how tracking headers are being used. In February of 2015, we delivered nearly 3,000 signatures to both agencies, along with a formal letter detailing our concerns (see Appendix 1). In addition, our technology team built a tool that lets people quickly test to see if their carriers are tracking them (see Amibeingtracked.com). At the same time, public officials began to express their concerns. In February, U.S. Senators Bill Nelson, Edward Markey, and Richard Blumenthal sent a joint letter asking the FTC and FCC to investigate the practices.[15] In April 2015, the FCC confirmed that it has launched an investigation of Verizon's use of tracking headers.[16]

(11) Fu, K. (n.d.). Wireless Web Privacy - Test Your Phone. Retrieved from https://web.eecs.umich.edu/~kevinfu/news/hdmlprivacy.html

(12) X-up-subno uniqueness. (2006, April 6). Retrieved from http://developerboards.att.lithium.com/t5/Technical-Questions-Discussion/X-Up-Subno-uniqueness/td-p/23475

(13) Mulliner, C. (2010). Privacy Leaks in Mobile Phone Internet Access. Retrieved from https://www.mulliner.org/collin/academic/publications/mobile_web_privacy_icin10_mulliner.pdf

(14) 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/

(15) Gross, G. (2015, February 6). Senators call for investigation of Verizon's nearly unstoppable supercookies. *PC World*. Retrieved from http://www.pcworld.com/article/2881252/lawmakers-call-for-investigation-of-verizon-supercookies.html

(16) Max, M. (2015, April 15). FCC Investigating Verizon over 'supercookies'. *TechRaptor*. Retrieved from http://techraptor.net/content/fcc-investigating-verizon-over-supercookies

How Amibeingtracked.com works

The Am I Being Tracked website performs several simple tests to determine whether users are being tracked. The site first determines whether the device making the request is a mobile device operating on a 3G, 4G, or LTE carrier network. If the device is operating on a carrier network, the test extracts the user's IP address from the normal HTTP header (not the injected header) and looks up the IP address in an IP geolocation database,[17] matching the IP address with publicly available information about where the IP range is located. The system then looks for any unusual or custom headers in the HTTP request and, if found, it logs them. Finally, the site returns the results of the test to the user stating whether the user is being tracked or not. *We never disclose the personally identifying information of people who take our test.*

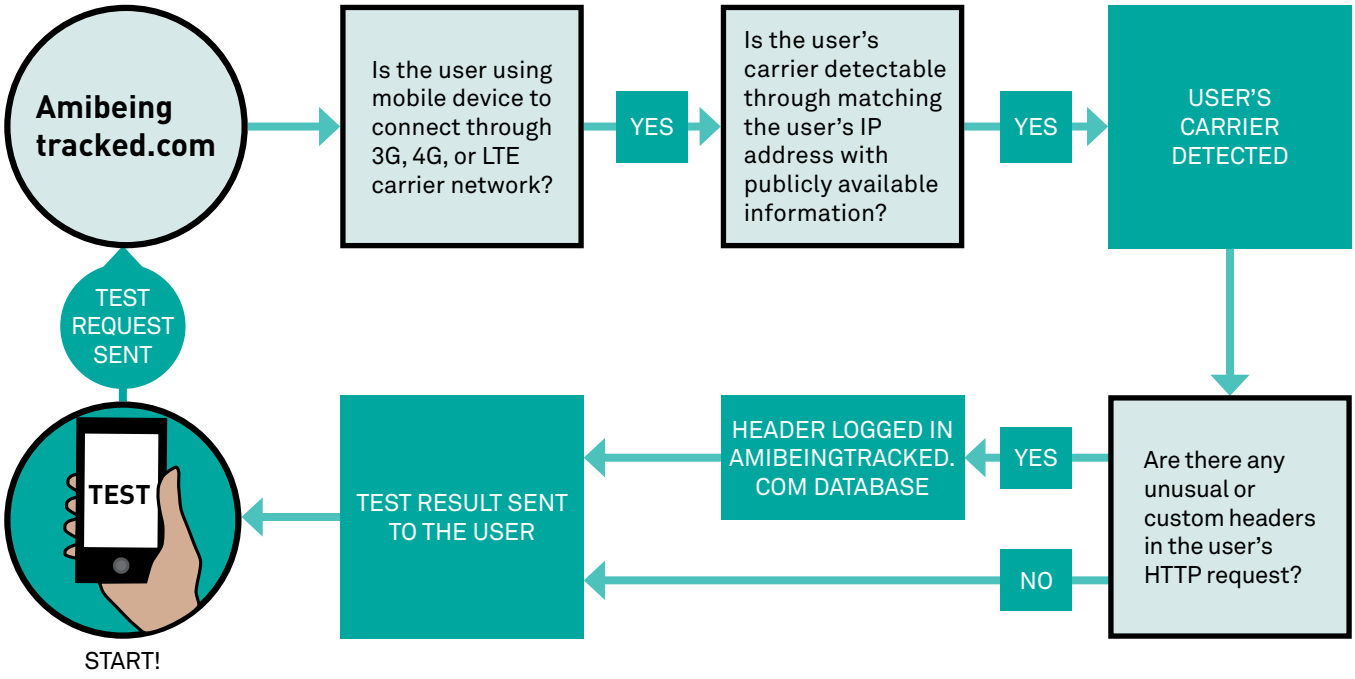


Fig 3 How Amibeingtracked.com works

The Amibeingtracked.com tool not only allows users to test for known tracking headers, but also allows us to learn from the results, specifically enabling us to identify new headers and make the test more robust. This has allowed us to improve the test's reporting accuracy over time. We have also improved accuracy by scrubbing inaccurate data, including tests run by malicious attackers (attackers typically have used Denial of Service attacks, attempted code injections, or automated scripts).

To encourage more people to take the test, we have shared links to Ambeingtracked.com in our newsletter, as well as in several email petitions. In addition, we have promoted the tool using our social media accounts. Media coverage and discussions in online fora such as Reddit.com have also generated attention and garnered further test results for analysis.

(17) Wikipedia. Geolocation software. Retrieved 2015 from https://en.wikipedia.org/wiki/Geolocation_software

Test Results

Research methodology

In the first six months, our Amibeingtracked.com tool returned nearly 180,000 results. This included 93,941 conclusive results and 80,156 inconclusive results. "Conclusive" means that our tool accurately identified the type of connection being used (3G, 4G, or LTE) and the carrier. "Inconclusive" means that our tool could not identify the carrier or the type of connection.[18] We separate the two types of results below for accuracy and transparency. Users who took the test have different demographic profiles and came through multiple referral sites, meaning that this is not a random statistical sample.

Evidence of widespread deployment

People from

164

different countries took the test with the tool at Amibeingtracked.com.

Among all the testers

26,726

received test results that showed the presence of tracking headers.

A further

67,215

did not have tracking headers present in their results.

Out of all test results

15.3%

showed the presence of tracking headers.

RESULTS BY COUNTRY

Tracked	Not Tracked	Inconclusive	Country
23123	46044	20443	USA
3344	12483	22222	SPAIN
125	434	980	NETHERLANDS
49	815	5616	CANADA
17	493	824	PERU
4	280	418	INDIA
3	93	256	CHINA

Among the people who took our test, the most tracking occurred in the USA, Spain, and the Netherlands. It is interesting to compare the Netherlands to Canada, because while more people in Canada tested their phones at Amibeingtracked.com, more people had tracking headers in the Netherlands. (We also detected tracking in Mexico, Venezuela, and Morocco. However, in each of these countries we had only one conclusive case of tracking.)

(18) This may have been because the user was accessing the test through WiFi, the test did not support a particular browser, the user was using a 2G connection, or the user had a new tracking header that had not previously been identified.

RESULTS BY CARRIER

Tracked	Not Tracked	Inconclusive	Carrier	Country
18868	8619	1282	Verizon	USA
5703	9854	1406	AT&T	USA
3335	4461	569	Telefonica de España	SPAIN
130	34	8	Vodafone NL	NETHERLANDS
48	264	779	Bell Canada	CANADA
17	0	322	Viettel Peru	PERU
11	5629	467	Vodafone Spain	SPAIN

Verizon had the most number of users with tracking headers amongst the people who took our test, followed by AT&T.[19] AT&T vowed to stop using heading trackers in November of 2014,[20] and we found that the number of users being tracked by AT&T dwindled to near zero after 17 weeks of running our test. Viettel Peru, which recently began operating in Peru, is also tracking users. The carrier is a subsidiary of Viettel, a Vietnamese carrier wholly owned by the government of Vietnam and operated by the Vietnamese military. We do not have tests from Vietnamese users to determine whether Viettel uses tracking headers in Vietnam, but it is worth further investigation to understand why a military operator would wish to use tracking headers. Results from two Vodafone subsidiaries varied greatly. A high percentage of Vodafone NL users were tracked, while Vodafone Spain tracked very few users overall, despite a higher number of tests. This demonstrates the need for more testing and investigation on a country-by-country basis, and for greater oversight and governance by senior-level corporate directors over national-level entities.

We also found conclusive results of tracking headers by people using Chinanet (China),[21] Bharti Airtel (India), Cricket (USA), Iusacell (Mexico), Rogers (Canada), and Telcel (Venezuela). However, we had less than ten conclusive results of tracking for each of these carriers.

HIGHEST PERCENTAGE OF TRACKING BY CARRIER*

Users tracked (%)	Carrier	Country
75.6	Vodafone NL	NETHERLANDS
65.6	Verizon	USA
39.9	Telefonica de España	SPAIN
33.6	AT&T	USA
5.0	Viettel Peru	PERU
4.4	Bell Canada	CANADA

* The percentage was calculated by dividing the number of users tracked by the total of conclusive results plus inconclusive results. This provides the most conservative estimate of the percentage of tracking. It is possible that the real figure is higher.

(19) Each of these companies used to be part of AT&T, as Verizon was created out of Bell Atlantic, a former company in the Bell system. See Wu, T. (2011). *The Master Switch: the Rise and Fall of Information Empires.* Vintage.

(20) Albanesius, C. (2014, November 16). AT&T drops 'supercookie' mobile tracking. *PC Mag*. Retrieved from http://www.pcmag.com/article2/0,2817,2472230,00.asp

(21) We are investigating this result, because Chinanet is not one of the three major mobile carriers in China. The result may have occurred because of the unique nature of mobile WiFi hotspots. A mobile carrier owns a list of IP addresses that it can allocate to users when they connect to the internet, typically by a 3G or 4G connection. Occasionally, the carrier does not allocate the IP address to a mobile connection and instead allocates it to a WiFi hotspot. The reverse also occurs, when an IP address allocated for a WiFi hotspot is instead allocated to a 3G or 4G connection. In our results, Chinanet may have received WiFi hotspot allocations from carriers that had injected tracking headers. The reverse may have also occurred, so Chinanet may have allocated an IP address to a mobile carrier, and injected the header.

DIFFERENT TYPES OF HEADERS

They leak private information about users and make them vulnerable to criminal attacks or government surveillance

Tracking header		Carrier	Characteristics
Encrypted	TM_user-id	Telefonica	Always paired with the header x-up-subno. It is possible the two headers are used for two different purposes.
	x-acr	AT&T	Remains active even when "do not track" option is turned on in a web browser. Can remain with the user even when roaming on other carriers in other countries.
	x-amobee-1	Bharti Airtel	Remains active even when "do not track" option is turned on in a web browser.
	x-uidh	Verizon, AT&T	Base64 encrypted. Binary data combines with null-terminated nine-digit number.
	x-vf-acr	Vodafone	Contains two parts: a constant string and base64 binary string. Remains active even when "do not track" option is turned on in a web browser.
New version: encrypted Old version: clear text	x-up-subno	Vodafone España, Telefonica de España, Bell Canada, Sprint, AT&T, Iusacell PCS, Jazz Telecom	Dates back to 2000. Different versions used by different carriers.
Not encrypted	x-msisdn	Bharti Airtel	Contains phone number in clear text.
	x-nokia-msisdn	Iusacell PCS de Mexico	Contains phone number in clear text.
	x-piper-id	Verizon, Chinanet	Contains random 10-digit number affixed to another header.

The various tracking headers raise several interrelated issues. First, encrypted headers make it impossible to know what types of data are being collected or how the data are being used. Conversely, headers sent in clear text raise privacy concerns. Such headers compromise user security and make users vulnerable to exploitation by criminals, who can take advantage of an individual user based on the header (although we found no evidence of this occurring to date). Governments could, in theory, surveil users by following individual headers or by requesting data from carriers that use the headers to assemble profiles.[22]

(22) We did not uncover evidence that government authorities are using these headers to monitor communications, but leaks about the NSA's Operation Auroragold and the British and Canadian BADASS program, which infiltrate mobile phone usage through sophisticated methods, suggest that the NSA, GCHQ, and other intelligence agencies may be capable of using tracking headers to monitor users. See more at Gallagher, Ryan. (2014, December 4). Operation Auroragold: How the NSA Hacks Cellphone Networks Worldwide. *The Intercept*. Retrieved from https://firstlook.org/theintercept/2014/12/04/nsa-auroragold-hack-cellphones/ See also Marquis-Boire, M. et al. (2015, July 1). XKEYSCORE: NSA's Google for the World's Private Communications. *The Intercept*. Retrieved from https://firstlook.org/theintercept/2015/07/01/nsas-google-worlds-private-communications/ For more BADASS information, see document hosted by *Der Spiegel* at http://www.spiegel.de/media/media-35670.pdf.

ENCRYPTED CONNECTIONS THWART TRACKING HEADERS

Websites with Secure Socket Layer (SSL) and Transport Layer Security (TLS) encryption prevent carriers from being able to insert tracking headers into users web browsing. Such sites are identifiable because the web address contains "HTTPS" instead of "HTTP." HTTPS stops carriers from identifying the exact resource requested by the user from a website. Although the carrier can view the base domain, such as Amibeingtracked.com, the carrier cannot identify the path to a particular page or resource on the site. Encrypted connections therefore improve privacy.

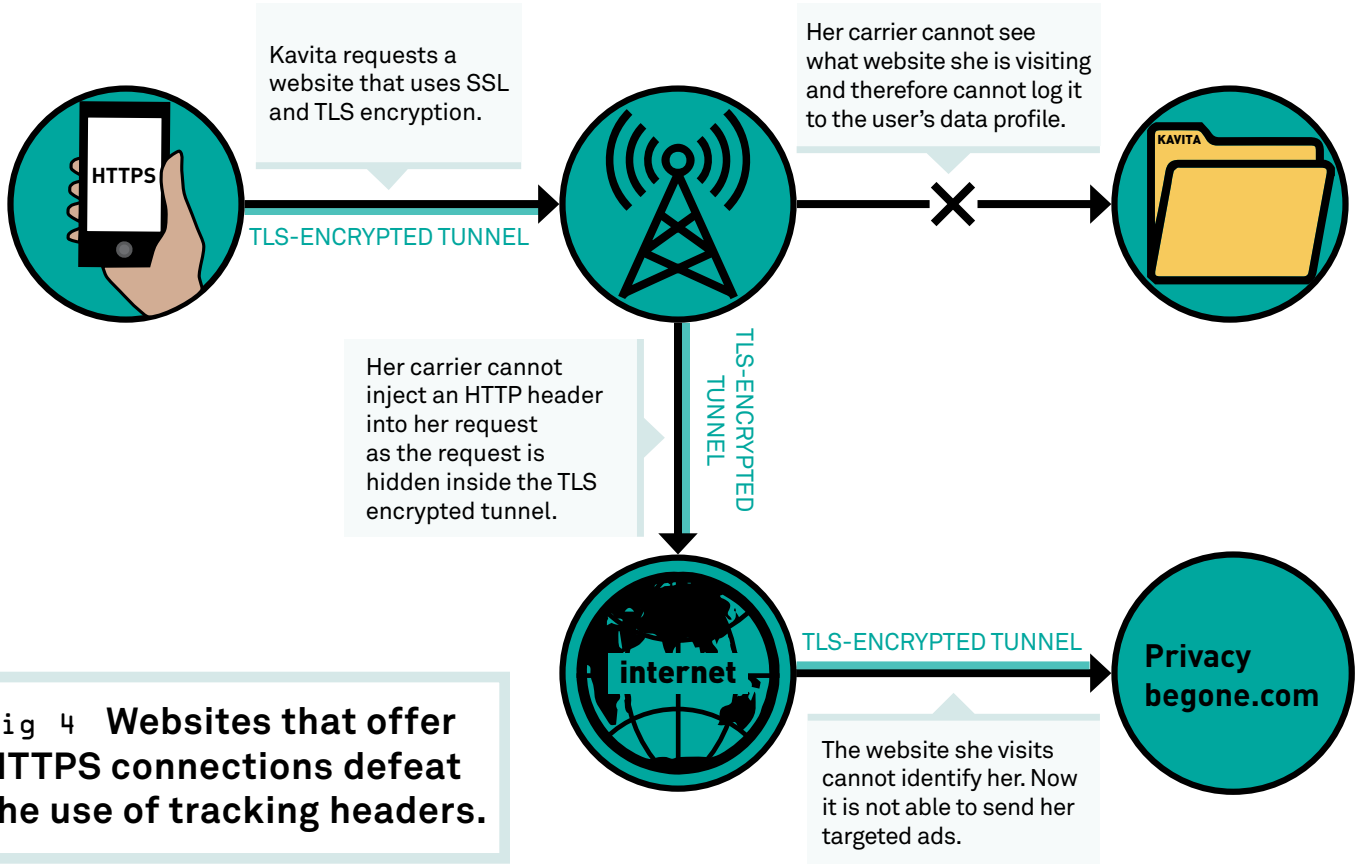


Fig 4 Websites that offer HTTPS connections defeat the use of tracking headers.

Unfortunately, the ability of HTTPS to block tracking headers may discourage websites from offering HTTPS connections. Carriers make money by selling user profiles, and websites make money from ad sales targeted at users.[23] It may be worth further investigation to see whether apps or services on a carrier tend to favor one type of connection over another. There are competing incentives for websites that could drive them to make different choices. Suffice it to say, a secure HTTPS website could not use a carrier's profiling service if it relies upon tracking headers.

TROUBLING QUESTIONS ABOUT PRIVACY AND NEW TECHNOLOGY

Since various groups began applying public pressure to carriers utilizing tracking headers, two have changed their practices: AT&T and Verizon. AT&T pledged to end its use of tracking headers in November 2014, and our tests suggest that the tracking has indeed stopped. Verizon Wireless allowed a user to opt out of its Relevant Advertising prior to press coverage in October 2014, and opting out meant that Verizon would stop populating

(23) We do not take issue with carriers as to their relationships with websites on advertising. Our concern here is that a lack of HTTPS can negatively impact user security.

profiles about the user's web browsing.[24] But opting out did not seem to stop Verizon Wireless from injecting the tracking headers — they just weren't used by Verizon for advertising. Third parties could still track the headers and use them for their own purposes. Indeed, the advertiser Turn appears to have accomplished this very feat, using Verizon's tracking header to create local cookies stored in users' web browsers.[25] In March of 2015, Verizon Wireless promised to allow a true-opt out for users so that Verizon would stop injecting tracking headers entirely.[26] In response to media coverage, Turn stated that it would suspend the use of Verizon's specific tracking headers to sell advertisements, pending further review.[27] Both Turn and Verizon Wireless are embroiled in litigation related to tracking headers at the time of this writing.[28][29]

Thus far, carriers have in general not been transparent or demonstrated accountability with regard to their use of tracking headers. In addition, government investigation of the practice has been inadequate to date.

The public policy implications of this practice demand greater attention. The tracking activity revealed in this report takes place within a context of massively increased government surveillance capabilities that span the globe. International human rights experts have extolled anonymity as an important facilitator of the rights to freedom of expression and privacy online,[30] yet users who wish to express themselves and receive and impart information without revealing their identity can face extreme difficulty. Intelligence agencies, malicious users, and other actors can exploit this power imbalance to unlawfully collect personal data, build profiles, and monitor marginalized communities. Far from hypothetical, recent reports about a secret British and Canadian surveillance program show that it "mines as much valuable information from leaky smartphone apps as possible," including unique tracking identifiers.[31]

TRACKING HEADERS MAY BE JUST THE BEGINNING

The promised changes by AT&T and Verizon Wireless around the use of tracking headers are positive steps, but this does not mean that all tracking will stop. Carriers may simply have more effective tracking mechanisms waiting in the wings. AT&T has already demonstrated that it intends to use advertising programs in its roll-out of new broadband fiber in the U.S. The company charges a premium for people who do not wish to be tracked.[32] When Verizon announced[33] its purchase of AOL in May of 2015, tech journalists trumpeted AOL's ability to deliver new forms of mobile advertising to Verizon customers.[34] These advertising mechanisms may utilize new tracking technologies instead of tracking headers.

(24) 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/

(25) Angwin, J. and Tiga, M. (2015, January 14). Zombie Cookie: the tracking cookie that you can't kill. *ProPublica*. Retrieved from http://www.propublica.org/article/zombie-cookie-the-tracking-cookie-that-you-cant-kill

(26) Graziano, D. (2015, March 31). How to opt out of Verizon's 'supercookie program'. *CNET*. Retrieved from http://www.cnet.com/how-to/how-to-opt-out-of-verizon-supercookie-tracking-program/#!

(27) In a January 2015 blog post, Turn said that it would stop using tracking headers "pending revaluation." The post specifically refers to the use of UIDH headers by Verizon and there is no mention of whether Turn uses other headers or would suspend their use. There have been no further announcements about Turn's review, and no indication of whether it has resumed using Verizon's tracking headers. See more at Ochoa, M. (2015, January 17). 'Zombie' Cookie ID to be suspended pending re-evaluation [blog post]. Retrieved from http://www.turn.com/blog/zombie-cookie-id-to-be-suspended-pending-re-evaluation

(28) Davis, W. (2015, April 9). Turn hit with new lawsuit over 'zombie' cookies. *Media Post*. Retrieved from http://www.mediapost.com/publications/article/247463/turn-hit-with-new-lawsuit-over-zombie-cookies.html

(29) Coren, C. (2015, February 12). Verizon hit with privacy class action over 'supercookies'. *Top Class Actions*. Retrieved from http://topclassactions.com/lawsuit-settlements/lawsuit-news/49503-verizon-hit-privacy-class-action-supercookies/

(30) Kaye, D. (2015, May 22). Report on encryption, anonymity, and the human rights framework. *United Nations Office of the High Commissioner for Human Right*s. Retrieved from http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

(31) Marquis-Boire, et al. (2015, July 1).

(32) Brodkin, J. (2015, February 16). AT&T charges $29 more for gigabit fiber that doesn't watch your web browsing. *ArsTechnica*. Retrieved from http://arstechnica.com/business/2015/02/att-charges-29-more-for-gigabit-fiber-that-doesnt-watch-your-web-browsing/

(33) Shields, M. and Gryta, T. (2015, May 12). Verizon to Buy AOL for $4.4 billion. *The Wall Street Journal*. Retrieved from https://secure.marketwatch.com/story/verizon-to-buy-aol-for-44-billion-2015-05-12-81032958

(34) Manjoo, F. For Verizon and AOL, Mobile is a Magic Word. *The New York Times*. Retrieved from http://www.nytimes.com/2015/05/13/technology/verizons-data-trove-could-help-aol-score-with-ads.html?ref=technology&_r=0

CONCLUSION

Tracking headers are a global phenomenon — we have determined that they are being used in numerous countries in various formats among a variety of carriers. But not all carriers track their users, and those that respect user privacy deserve our support. Telecommunications companies occupy a central role in providing access to the internet, enhancing the communications capabilities of billions of people. By delivering open access, networks, and services, telcos can serve not just as internet service providers, but also as "freedom providers." Our Telco Action Plan offers proactive steps for any carrier to better respect human rights in policy and practice, and provides guidelines for safeguarding users' right to privacy.[35]

Injecting tracking headers out of the control of users, without their informed consent, may abuse the privileged position that telcos occupy. End User License Agreements are typically complex and most people do not read them when purchasing a mobile internet plan.[36] The use of tracking headers dates back to at least 2000, which means that it took 15 years for U.S. regulatory agencies to investigate how they are being used. And it is entirely possible that new, undiscovered tracking mechanisms are already being deployed.

In many ways, our research raises more questions about the use of tracking headers than it answers. We believe that further research is necessary to uncover what is happening so that we can develop policy and practices to address the privacy issues that are implicated by this form of tracking.

We offer the following recommendations to address the use of tracking headers and take action to respect user privacy. Although we present specific responses, any regulatory action should address the problem as we know it today while also considering the privacy-invading technologies of the future. *See next page for recommendations.*

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

(36) Masnick, Mike. (2012, April 23). To Read All Of The Privacy Policies You Encounter, You'd Need To Take A Month Off From Work Each Year. *Techdirt*. Retrieved from https://www.techdirt.com/articles/20120420/10560418585/to-read-all-privacy-policies-you-encounter-youd-need-to-take-month-off-work-each-year.shtml

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

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

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

APPENDIX 1

Letter to Federal Communications Commission and Federal Trade Commission Urging Agencies to Investigate Use of Tracking Headers

February 17, 2015

Dear FCC Commissioners,

We respectfully urge you to investigate the use of persistent cookies that were recently found to be injected by U.S. cellular network operators into the HTTP requests of mobile users.

More users access the internet on mobile networks, and unknowingly reveal sensitive data, including real-time location information, to operators, apps, and third parties. Their trust in the companies that enable their internet access and services must be matched by vigilant regulation to prevent abuse.

Today, we are delivering an Access petition that drew 3,000 signatures calling for the FCC and FTC to investigate the use of UIDH and to take immediate action to protect user rights. The fact that AT&T and Verizon both deployed a pernicious form of persistent cookie — a UIDH or "Unique Identifier Header" — led to public outcry and spurred our community into action. While both companies have now responded to our voices and suspended the UIDH injection, all action by the companies has been voluntary, and recent revelations about the use of the service operated by Turn suggest that companies will continue to utilize such tracking mechanisms whenever they can get away with it.

Spoofing and surveillance

In addition to consumer-related privacy problems, we believe that these cookies can make users vulnerable to spoofing by criminals. They could also potentially enable authorities to surveil users without their knowledge. Even without this type of third-party abuse, though, the very existence of these cookies violates our privacy rights if users cannot truly opt out.

FCC Authority

The FCC is empowered to investigate and set clear rules banning the use of persistent cookies in mobile internet traffic. The FCC already established precedent in the matter of Terracom, Inc. and YourTel America, Inc. in 2014. In that important proceeding, your agency found that the companies had collected data about their customers, willfully misled the customers about how that data was stored and used, and failed to provide reasonable security measures.

The cookie technology at issue here also thrives on the web traffic of unsecured http communications that do not use SSL or TLS security to encrypt their connection. Exploiting the mobile browsing of users to track them for advertising purposes is misleading and may expose the users to security risks. Furthermore, Verizon and other carriers have been shown to track users over time and across websites, even when they opt out.

The FCC should investigate and end this unfair practice that exploits the trust of mobile internet users.

Global precedent for privacy

Your actions will not only protect users in the U.S., but set a precedent around the world: Access has already found mobile operators in several countries injecting these pernicious cookies and enabling tracking of their users. By striking out against UIDH and its use, U.S. regulators will begin building an international norm banning this insidious tracking technology.

In holding Verizon and others accountable for their actions, the FCC can set an important precedent that opting in should be the new normal, and not opting out.

Best regards,
Access

APPENDIX 2

Glossary of Terms

Cookie
- A small piece of data sent from a website and stored in a user's web browser that is designed to track web browsing sessions.

Encryption
- Encryption is the process of encoding messages or information in such a way that only authorized parties can read it.

FCC
- Federal Communications Commission

FTC
- Federal Trade Commission

HTTP
- Hypertext Transfer Protocol, a foundational protocol for the World Wide Web.

HTTPS
- A communications protocol for secure communication over a computer network.

Header
- Introductory lines of text at the beginning of a web request that negotiate how a web browser and web server communicate.

IMEI
- International Mobile Station Equipment Identity. Transmitted to a carrier when placing a call or browsing the web.

IMSI
- International Mobile Subscriber Identity. Transmitted to a carrier when placing a call or browsing the web.

ICCID
- Integrated Circuit Card Identifier. Transmitted to a carrier when placing a call or browsing the web.

IP
- Internet Protocol

IP geolocation database
- A database that matches an IP address with publicly available information about the location where the associated IP range is located.

Perma-cookie
- Popularly used to refer to tracking headers. However, a cookie is stored within a users' web browser, and tracking headers are injected by the carrier out of the control of the user, making this term inaccurate.

Supercookie
- Popularly used to refer to tracking headers. However, a cookie is stored within a users' web browser, and tracking headers are injected by the carrier out of the control of the user, making this term inaccurate.

Tracking header
- A header injected by a carrier out of the control of the user.

Zombie cookie
- Popularly used to refer to tracking headers. However, a cookie is stored within a users' web browser, and tracking headers are injected by the carrier out of the control of the user, making this term inaccurate.