Header Enrichment or ISP Enrichment? Emerging Privacy Threats in Mobile Networks

Narseo Vallina-Rodriguez*, Srikanth Sundaresan*, Christian Kreibich*†,Vern Paxson*‡
*ICSI, †Lastline, ‡UC Berkeley
{narseo,srikanth}@icsi.berkeley.edu, {christian,vern}@icir.org

ABSTRACT

HTTP *header enrichment* allows mobile operators to annotate HTTP connections via the use of a wide range of request headers. Operators employ proxies to introduce such headers for operational purposes, and—as recently widely publicized—also to assist advertising programs in identifying the subscriber responsible for the originating traffic, with significant consequences for the user's privacy. In this paper, we use data collected by the Netalyzr network troubleshooting service over 16 months to identify and characterize HTTP header enrichment in modern mobile networks. We present a timeline of HTTP header usage for 299 mobile service providers from 112 countries, observing three main categories: (1) unique user and device identifiers (e.g., IMEI and IMSI), (2) headers related to advertising programs, and (3) headers associated with network operations.

CCS Concepts

•**Security and privacy** → **Mobile and wireless security; Mobile and wireless security;** •**Networks** → *Middle boxes / network appliances;* Application layer protocols;

Keywords

Mobile, Cookies, Privacy, HTTP, Proxies, Header Injection

1. INTRODUCTION

> *In the mobile space delivering the right ad to the right person is difficult because there is no common standard for identity and addressability. We think we're in a position to solve that. The second piece is the measurement of mobile; there are a lot of problems with getting good attribution data.* — C. Hillier, VP of Verizon's Precision Market Insights division [11]

This quote illustrates two important challenges mobile operators face today: how to ease network management and how to increase revenue by monetizing subscriber metadata and traffic.

HTTP *header enrichment* allows operators to kill two birds with one stone [6]: first, operators can append information into HTTP traffic to enable attribution (of network resources to specific users), performance enhancement, analytics, and content access control and customization [4, p. 62]; second, operators can monetize their network and user base through advertising programs by taking advantage of their position to inject unique tracking identifiers into every HTTP request, popularly known as "super-cookies" [8].

HTTP header enrichment can have serious consequences for millions of mobile subscribers all over the world. Standardization efforts and best practices suggest that providers ought to remove header enrichment at their network boundary to prevent privacy leaks [6]. However, as our analysis reveals, the egress point does not necessarily remove injected HTTP headers; thus, any web server visited from a mobile phone can use this information for purposes adverse to user interests like user discrimination and online tracking.

Users lack legal protections against these practices, which happen in a manner invisible to most of them. As we illustrated in a previous study [17], mobile operators enforce the use of HTTP proxies and gateways through preconfigured APN (Access Point Name) settings on a device. Typical users lack the mechanisms and knowledge to prevent operator-enforced proxies from performing header injection and to stop online services from collecting their information. Only select savvy users take advantage of VPN services to evade such practices.

This paper presents the first detailed characterization of HTTP header enrichment in modern mobile networks. We use our ICSI Netalyzr network troubleshooting service for Android, drawing upon measurements and accurate contextual data gathered from thousands of mobile users running our service to analyze how mobile operators alter HTTP requests. We analyze the HTTP request headers and values we see arriving at our server, inferring their likely purpose as well as security and privacy implications. Our study spans

HotMiddlebox'15, August 17-21 2015, London, United Kingdom

 ISBN 978-1-4503-3540-9/15/08…$15.00

DOI: http://dx.doi.org/10.1145/2785989.2786002

299 mobile operators (including both MNOs and MVNOs) in 112 countries over a 16-month period.

2. PREVIOUS WORK

Mulliner performed the most relevant study in the area of privacy leaks caused by early WAP proxies [14], analyzing HTTP headers collected by a web server hosting J2ME games he had developed. The analysis of the headers identified privacy leaks inflicted by WAP proxies in the form of IMSI, MSISDN and IMEI identifiers. Mulliner states that by default smartphones do not use HTTP proxies to reach the Internet. However, our analysis—in which we control both client and server, and incorporate contextual information about the network and mobile operator via Android's system APIs—in fact finds widespread proxy use in modern mobile networks. Moreover, we observe the onset of new types of tracking headers employed for advertising purposes.

The IETF Service Function Chaining (SFC) working group aims to standardize the use of header enrichment for operational purposes such as load balancing, performance enhancement, and charging [6]. The draft states that "service function chains typically reside in a LAN segment which links the mobile access network to the actual application platforms located in the carrier's datacenters or somewhere else in the Internet". Best practices and standardization efforts contemplate the possibility of inflicting privacy harm on mobile users if the egress point does not remove the injected headers. However, the current draft leaves the final decision to operators' discretion: "An operator may consider the SFC Metadata as sensitive. From a privacy perspective, a user may be concerned about the operator revealing data about (and not belonging to) the customer. Therefore, solutions should consider whether there is a risk of sensitive information slipping out of the operator's control" [7].

3. DATA COLLECTION

We use our in-house Netalyzr-for-Android tool for collecting data about HTTP header injection. Netalyzr is a free, user-driven network troubleshooting tool we have developed and maintained at ICSI since 2009 [10]. We launched Netalyzr for Android as a free app on Google Play in November 2013. Some 30,000 users in 130 countries have since installed the app. Netalyzr analyzes a broad spectrum of network properties as observed from the edge of the network; it interacts with a suite of custom-built test and measurement servers, looking for a range of performance and behavioral anomalies such as DNS manipulations and transport limitations, port filtering, HTTP proxy interference, and network path anomalies. Netalyzr for Android uses Android APIs to augment this data with local network information in mobile networks. In particular, the app collects Access Point Name (APN) settings, the SIM card provider, and the Mobile Country Code (MCC) / Mobile Network Code (MNC) tuple, allowing us to accurately attribute network features to operators without relying on misleading information such as the public IP address. We refer the reader to our prior work for a description of proxy identification tests [20], and for architectural and operational specifics of the platform [10].

3.1 Proxy-added header detection

Mobile operators deploy and enforce the use of in-path proxies in the network for performance enhancement [17] and, as we will characterize in the remainder of this paper, also for advertising purposes. While Netalyzr measures a wide spectrum of network properties, in this work we focus on the subset that pertains to HTTP header modification. At a high level, we detect the presence and properties of proxies and middleboxes by observing how they modify connections between the Netalyzr client and the server, both of which we control. Netalyzr employs Java APIs and a custom HTTP engine to characterize HTTP traffic modifications, proxies, artifacts, and limitations. The app fetches custom content from our servers using mixed-case request and response headers, in known order. If we see any changes in case or deviation from the known order, we know that the traffic has passed through an in-path proxy. This paper studies HTTP headers added by such in-path proxies to annotate connections, report on the information these headers provide, and focus particularly on headers causing privacy violations.

3.2 The Data

We collected data from the Netalyzr app between November 2013 and March 2015. Our dataset contains 8,264 sessions spanning 112 countries and 299 operators. We classify mobile operators into Mobile Network Operators (MNOs, owning spectrum) and Mobile Virtual Network Operators (MVNOs, leasing spectrum from MNOs), per our previous work [17]. MVNOs can operate as rebranded versions of MNOs ("light" MVNOs), or deploy their own IP core ("full" MVNOs). Our dataset covers both MNOs and MVNOs. We have made available part of the data used in this paper for the community via CRAWDAD [18].

3.3 Limitations and Data Sanitization

Netalyzr is a crowd-sourced tool that users run at their discretion. As a result, we cannot obtain data continuously or cover all operators. Header injection in HTTPS flows would require the ISP to perform TLS interception. To date, Netalyzr's TLS tests have not flagged this practice in any mobile provider [16]. Likewise, Netalyzr cannot identify operators performing HTTP header enrichment on traffic sent to selected partners only, due to its inability to access the HTTP headers received by the partners' servers. In addition, we cannot control the handset configuration of users running the tool (e.g., savvy users might employ VPN clients to avoid middlebox interference), handset peculiarities (e.g., inappropriate APN settings), or platform inconsistencies (e.g., operator names inaccurately reported by Android APIs). We refer the reader to our previous work for details about data sanitization mechanisms in mobile measurements [17]. Finally, this paper does not consider plausible alternative options for marking users' traffic uniquely, for example via device-specific allocation of routable IPv6 addresses.

HTTP Header	Operators	Notes
x-up-calling-line-id x-up-nai x-up-vodacomgw-subid	Vodacom (ZA)	Phone #
msisdn x-nokia-msisdn	Orange (JO) Smart (PH)	MSISDN
tm_user-id x-up-subno	Movistar (ES)	Subscriber ID
x-up-3gpp-imeisv	Vodacom (ZA)	IMEI
lbs-eventtime	Smartone (HK)	Timestamp
lbs-zoneid	Smartone (HK)	Location

Table 1: Privacy-sensitive HTTP header added by different operators.

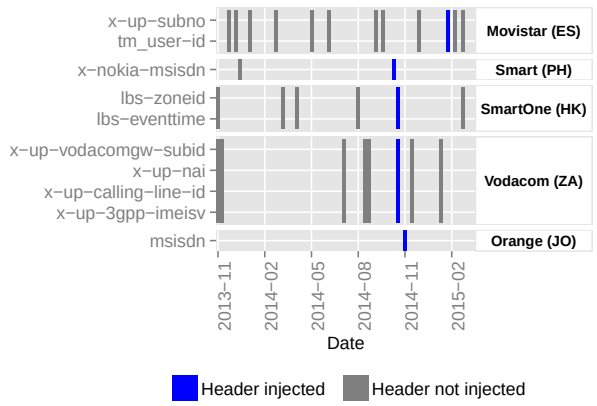

Figure 1: Privacy-sensitive HTTP Headers observed per MNO. We show sessions that indicate presence of the respective header in blue, while sessions from the same provider but without the particular header appear in gray.

4. ANALYSIS

Our analysis reveals a range of HTTP headers injected into mobile user traffic by 13% of the 299 mobile operators in our dataset (including both MNOs and MVNOs). We classify the headers in our dataset into three categories, based on their likely purpose:

- **Privacy-compromising headers (5 operators):** HTTP headers leaking sensitive information that can uniquely identify the device (IMEI), the subscriber (MSISDN or phone number), or the subscriber's location.
- **Tracking headers (6 operators):** operator-generated UIDs (subscriber-unique identifiers) that enable user tracking for advertising purposes [12]. They are also known as super-cookies. Tracking headers do not directly reveal sensitive information about users but can lead to loss of privacy for mobile subscribers.
- **Operational headers (24 operators):** information related to network operations and network infrastructure, such as internal IP addresses of subscribers (i.e., the local IP address assigned by the provider), and subscriber gateway locations and versions. Some of these headers can assist with tracking users (e.g., internal IP addresses as reported in RFC7239 [15]).

In § 4.4 we discuss 5 headers for which we could not identify an apparent purpose. Finally, as MVNOs are generally just rebranded versions of MNOs, they inherit HTTP header injection practices from the parent MNO [17]. We analyze MVNOs separately in § 4.5.

4.1 Privacy-compromising headers

Headers in this category not only uniquely tag users but also reveal their identity, raising major concerns about user privacy. Table 1 lists the headers we observed in this category and the sensitive information they leak. Figure 1 shows a per-operator timeline of the occurrence of these headers in our dataset.

Vodacom South Africa is the most egregious information leaker in our dataset, revealing the subscriber's phone number, device IMEI, and an email-like string that contains their phone number (`subscriber_phone_number@lte.vodacom.za`), though we only have one session from this ISP that leaks these headers. As of late October 2014, Vodacom South Africa no longer leaks sensitive information about their subscribers [19]. Our subsequent sessions from the provider confirm this.

We also observed header injection by a SmartOne gateway in Hong Kong that includes `lbs` in two header keys, which likely stands for Location-Based Services. Analyzing the header value `LBS-ZoneID: MTR;O`, we speculate that the header indicates a specific zone of the Hong Kong Metro (MTR) system. The second header, `lbs-eventtime`, reports a timestamp. We only have six sessions from this ISP, only one of which exhibits this behavior. A gateway serving subscribers of the mobile network infrastructure deployed in Hong Kong's metro system may inject such headers.

Orange in Jordan and Smart in the Philippines directly append the MSISDN (i.e., the phone number stored in the SIM card) to each HTTP request. We also observed unique user identifiers in one session from Movistar (Spain).

We temper our findings with respect to the sparseness of our dataset for these ISPs. For each, we only observe the injected headers in one session as shown in Figure 1. This suggests that the leaks resulted from short-lived injection policies, temporal misconfigurations on gateways, specific APN configurations, or even from injection occurring on the user's device. Malware running on rooted handsets (the Movistar device was rooted according to our data) or operator modifications on the Android phones subsidized to their customers could result in the latter option. We require more extensive data to pinpoint the root cause of such injections.

4.2 Tracking headers

Tracking headers identify mobile users uniquely and persistently. Cookies offer a similar function in the browser context, though not as pervasively for a given user. In addition, modern mobile applications tend to bypass browsers entirely, making user tracking harder, and thus rendering mobile advertisements less effective.

HTTP Header	Operator
x-acr	AT&T (US)
x-amobee-1	Airtel (IN)
x-amobee-2	Singtel (SG)
x-uidh	Verizon (US)
x-vf-acr	Vodacom (ZA), Vodafone (NL)

Table 2: Tracking headers identified in different operators.

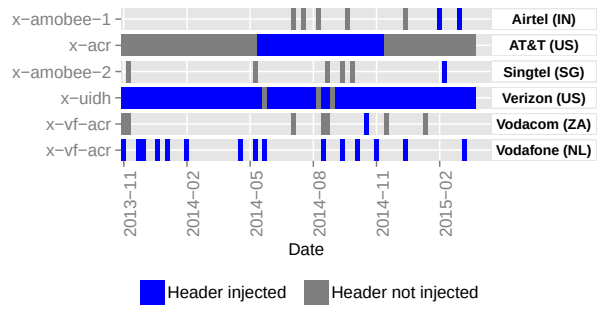

Figure 2: Tracking headers observed per MNO.

Tracking headers solve this problem by injecting identifiers into every HTTP request passing through the operator's gateways. Since the ISP knows which user originated the traffic, they can add identifiers unique to the user without compromising their identity. ISPs claim that this significantly improves ad-delivery on mobile networks [11]. As opposed to browser cookies, mobile users typically remain oblivious to the addition of tracking headers and have no control over them.

Table 2 lists the operators injecting tracking headers seen by Netalyzr, while Figure 2 shows the time-span over which we observed them. We have evidence of tracking headers in Vodafone, Vodacom (co-occurring with the privacy-compromising headers listed in Table 1), Verizon and AT&T. Interestingly, AT&T users with legacy APN settings for GPRS do not suffer from header injection. According to an EFF article Verizon's header injection does not affect government and corporate subscribers [8]. This may explain the time windows in Figure 2 for which we have no evidence of super-cookies among Verizon's subscribers. Since Feb. 2015, we have evidence of a new type of tracking header on Airtel (India) and Singtel (Singapore) that map to the Israeli mobile advertising company Amobee [1]. According to their website, Amobee provide such services to some of the largest mobile operators in the world. We contacted Amobee to corroborate our findings, but have not received a response.

Since user tracking happens unbeknownst to most mobile subscribers, it can undermine the trust relationship between users and their mobile operators. Tracking headers recently received significant press coverage when Verizon's and AT&T's practices came to light. While the largely negative media coverage led to AT&T disabling its program in Nov. 2014 [9], Verizon continues this practice. Until Apr. 2015 Verizon injected tracking headers into user traffic even when they opted out of the advertising program [5].

4.3 Operational headers

The third class of headers consists of those added for operational purposes, to aid ISPs in managing their network and users subscribed to different plans or services. We group these headers into four sub-categories: headers that identify (1) the type of network coverage at the handset so servers can adapt content to poor network conditions (e.g., the 3GPP standard on the `x-nokia-bearer` header), (2) the mobile operator and roaming state (e.g., `x-operator-domain` header), (3) the 3GPP gateway serving the client (e.g., `x-nokia-gid` header), and (4) the private IP address of a client connecting to a web server through a gateway. We list this category's headers in Table 3.

Mobile operators use header enrichment for load balancing, debugging, statistics, and detection and prevention of abusive access [4, 6, 7]. For example, operators can use `x-forwarded-for` to tag the internal IP address of users for managing traffic. However, such headers also disclose client-related information typically hidden by NATs or proxies. Petersson and Nilsson point out the potential privacy risks as `x-forwarded-for` headers de-anonymize clients [15]. The device's IP address, the mobile operator, and the approximate geographic location of the user (as revealed e.g. by the `x-gateway` header) all contribute information potentially usable in lieu of HTTP cookies, and remaining beyond the visibility or control of users. This problem will grow more critical with the adoption of IPv6 addressing, which will encourage unique addressing per device, though our data does not provide evidence of this occurring in IPv6 deployments at this point.

Many operators leak their gateway vendor to the external world. We identified Blue Coat proxies (via `x-bluecoat-via` header) used by Vodafone in Qatar, SFR, and 3 in Ireland.[1] EE in the UK and SFR in France not only reveal the hardware vendor but also the model and build version via headers such as `x-nokia-gateway-id`, potentially informing attackers of equipment vulnerabilities.

Because such headers pertain to the inner workings of the ISP, some of them also have interesting quirks. We identified mismatches in the internal IP addresses reported by the HTTP headers and the actual internal IP address of the client (as separately identified by Netalyzr) in sessions coming from Singtel Singapore and T-Mobile Germany subscribers. Singtel proxies replace the private IP address of the terminal by a routable address registered by Singtel. Regarding the latter, despite the fact that 97% of T-Mobile Germany sessions contain the `x-forwarded-for` header, only 3% of them accurately report the actual internal IP address of the device. Upon closer inspection, we noticed that T-Mobile proxies replace the first octet of the private IP address with an integer value ranging from 11 to 17.[2] For example, the

[1] We note that Reporters Without Borders and the University of Toronto's Citizen Lab deem Blue Coat an enemy-of-the-Internet due to their censorship and surveillance equipment [2].

[2] These are the values that we have records of. T-mobile could use more values.

HTTP Header	Operator	Notes
x-nokia-bearer	3 (ID), EE (GB), SFR (FR)	3GPP standard
x-orange-rat	EE (GB)	
x-up-3gpp-rat-type	Vodacom (ZA)	
x-up-bear-type	Movistar (MX)	
x-up-bearer-type	Vodacom (ZA)	
x-operator-domain	EE (GB)	Operator name
x-vfprovider	SFR (FR)	
x-vodafone-roamingind	Vodafone (IE)	MCC, MNC
x-up-3gpp-sgsn-mcc-mnc	Vodacom (ZA)	Operator name
x-orange-roaming	EE (GB)	Roaming state
x-sdp-roaming	Vodafone (TR)	
vf-za-trust	Vodacom (ZA)	Private IP address
x-ee-client-ip	EE (GB)	
x-forwarded-for	AIS (TH), AT&T (US), Bouygues (FR), Etisalat (AE), LMT (LV), Movistar (MX), O2 (GB), Orange (CH), SaskTel (CA), SFR (FR), Singtel (SG), T-Mobile (DE), TOT (TH), Vodacom (ZA), Vodafone (DE)	
x-nokia-ipaddress	EE (GB), SFR (FR)	
x-up-forwarded-for	TIM (IT)	
o2gw-id	O2 (GB)	Gateway ID & location
x-gateway	O2 (GB)	
x-bluecoat-via	3 (IE), Vodafone (QA)	Bluecoat-specific
x-nokia-gateway-id	SFR (FR)	Gateway model
x-nokia-gid	SFR (FR)	
x-proxy-id	LMT (LV)	Proxy unique ID
x-up-sgsn-ip	Vodacom (ZA)	SGSN IP address
proxy-connection	TIM (IT)	Persistent connections
wap-connection	Airtel (IN)	Layer-7 protocol
x-nokia-connection_mode	SFR (FR)	Layer-4 protocol
x-vodafone-3gpdpcontext	Vodafone (IE)	PDP context
wisp-a	Orange (FR)	Wireless provider
x-wisp	Orange (FR)	

Table 3: HTTP headers leaking network-related information added by different operators.

IP address reported for a user with the private IP address 10.42.41.97 could become 17.42.41.97, a routable IP address not registered by T-Mobile Germany. The remaining 3% of T-Mobile sessions accurately report the private IP address of the handset; they all have private IP address in the range 100.64.0.0/10 (used for Carrier-Grade NAT). This suggests that T-Mobile uses specific gateways or addressing policies to tag users depending on aspects such as their data plans or services. We performed active tests by crafting HTTP headers on requests from a device subscribed to T-Mobile, confirming that the proxy rewrites the values sent by the client in the `x-forwarded-for` header.

4.4 Unclassified Headers

While most of the headers we saw fit neatly in one of our categories, we saw 5 headers to which we could not assign a purpose, per Table 4. We have a single AT&T session with an `x-content-opt` header, which occurs only in the Voice-over-LTE APN `nxtgenphone`. Similarly, we saw two headers in EE that exist solely in the APN `orangeinternet`. In fact, EE is a joint venture between T-Mobile and Orange in the UK. As a result we have evidence of several APN settings including legacy APNs inherited from the parent companies [17].

Interestingly, we also identified two users enabling the "Do Not Track" browsing option in their devices (a strikingly low number). When this option is enabled, the system adds a `dnt` header into each HTTP request. As the name suggests, this header expresses the user's preference to not be tracked by online services, but services are not legally obliged to honor this request, rendering its efficacy questionable, and indeed the Digital Advertising Alliance does not require its members to honor it [3]. Moreover, given the proliferation of proxies in mobile networks [17] and how they intercept and modify HTTP headers, no guarantee exists that a client-generated headers will even reach the server.

HTTP Header	Operator	Example
x-content-opt	AT&T (US)	X-Content-Opt: Turbo/4.35.6119
x-ee-brand-id	EE (GB)	X-EE-Brand-ID: 2
x-ee-mig	EE (GB)	X-EE-MIG: 1
x-tmv-type	True (TH)	X-TMV-TYPE: NA
x-vfstatus	SFR (FR)	X-vfstatus: 10

Table 4: Unrecognized HTTP headers.

4.5 MVNO propagation

Our previous work shows that the majority of MVNOs operate as "light" MVNOs, and generally consist of rebranded versions on top of well established MNOs [17]. As a result, light MVNO subscribers become exposed to infrastructure inefficiencies, security vulnerabilities, and privacy risks

present in the host MNO. Our dataset reveals records of MNO header additions propagating to light MVNOs operating in their networks. For example, SFR France's headers propagate to Prixtel, T-Mobile Germany's headers to Congstar, and Orange France headers to Virgin.

5. CONCLUSIONS

As mobile operators fight for a larger share of the mobile advertising market—a sphere largely dominated by online services and smartphone vendors—they appear to have increasingly turned to new techniques for tracking users. A direct consequence of these steps for increasing revenues is HTTP "header enrichment".

In this paper, we used data collected by the Netalyzr-for-Android app to identify the presence of HTTP header injection performed by mobile operators all over the world. We classify the techniques in three categories, two of which directly affect user anonymity and privacy, and the third reflecting headers injected ostensibly for operational reasons, but potentially affecting user privacy and security.

While HTTP header enrichment can prove useful for improving the efficacy of mobile advertisement and network management, if mobile operators do not remove the injected information before user traffic leaves its network premises, it can leak information for millions of mobile subscribers all over the world. Unfortunately, HTTP header enrichment typically occurs in a manner transparent to mobile users. Recent news suggest that mobile operators may also inject JavaScript code into web traffic, for advertising purposes [13]. Even when aware of such practices, users have limited options to turn them off in order to protect their privacy. We note that media exposure led to AT&T abandoning its practice [9], and Verizon very recently decided to allow its users to opt-out.

Absent such protections, users cannot control which parties collect this information about their activity nor how such parties use (or misuse) their metadata for tracking, surveillance, and content discrimination. Only savvy users can avoid header injection by taking advantage of VPNs and enabling the "Do Not Track" option in their web browser, if supported (and honored). This leads us to advocate that mobile operators, proxy vendors, regulatory bodies, and members of relevant IETF working groups such as SFC (Service Function Chaining) should thoroughly consider how HTTP header enrichment affects mobile users and how to deploy it in a privacy-safe manner, giving users informed control over their own traffic.

Acknowledgments

As always, we are deeply grateful to our Netalyzr users for using our tool and enabling this study. This work was partially supported by NSF grants CNS-1213157, CNS-1237265, and CNS-1111672, and by the DHS Directorate of Science and Technology under grant N66001-12-C-0128. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors or originators and do not necessarily reflect the views of the NSF or of the DHS. The authors would like to thank the anonymous reviewers for constructive feedback on preparation of the final version of this paper and Florian Wohlfart (TU Munich) for his valuable help. We also wish to thank Amazon, Comcast, and Google for their generous support.

6. REFERENCES

[1] Amobee. Operator Solutions. http://amobee.com/operators/.

[2] Blue Coat Portfolio. Reporters Without Borders. http://surveillance.rsf.org/en/blue-coat-2/, 2012.

[3] Digital Advertising Alliance. Guidance to Marketers for Microsoft IE10 "Do Not Track" Default Setting. 2012.

[4] Cisco. Cisco ASR 5000 Series Packet Data Network Gateway Administration Guide. http://www.cisco.com/c/dam/en/us/td/docs/wireless/asr_5000/12_2/OL-25557_PGW_Admin.pdf.

[5] K. Cox. You Can Now Finally, Really Truly, Opt Out Of Verizon Wireless Tracking "Supercookies". Consumerist, http://consumerist.com/2015/04/01/you-can-now-finally-really-truly-opt-out-of-verizon-wireless-tracking-supercookies/, 2015.

[6] W. Haeffner, J. Napper, M. Stiemerling, D. Lopez, and J. Uttaro. Service function chaining use cases in mobile networks. *IETF Work in Progress*, 2015.

[7] J. Halpern and C. Pignataro. Service Function Chaining (SFC) Architecture. *IETF Work in Progress*, 2015.

[8] J. Hoffman-Andrews. Verizon injecting perma-cookies to track mobile customers, bypassing privacy controls, 2014.

[9] M. Kassner. AT&T ends controversial use of perma-cookies to track users. Tech Republic, http://www.techrepublic.com/article/att-ends-controversial-use-of-perma-cookies-to-track-users/, 2015.

[10] C. Kreibich, N. Weaver, B. Nechaev, and V. Paxson. Netalyzr: Illuminating The Edge Network . In *Proc. ACM IMC* , 2010.

[11] J. Marshall. How Verizon Plans to Fix Mobile Advertising. Wall Street Journal, http://blogs.wsj.com/cmo/2014/05/23/how-verizon-plans-to-fix-mobile-advertising/, 2014.

[12] R. McMillan. Verizon and AT&T are the only wireless carriers using Perma-cookies. Wired, http://http://www.wired.com/2014/11/permacookie-free/.

[13] V. Mukunth. Israeli Firm Strong-Arms Indian Techie for Exposing Suspicious Code. The Wire, http://thewire.in/2015/06/09/israeli-firm-strong-arms-indian-techie-for-exposing-suspicious-code/, 2015.

[14] C. Mulliner. Privacy leaks in mobile phone internet access. In *Proc. IEEE ICIN*, 2010.

[15] A Petersson and M Nilsson. Forwarded http extension. *IETF. Work in Progress*, 2012.

[16] N. Vallina-Rodriguez, J. Amann, C. Kreibich, N. Weaver, and V. Paxson. A tangled mass: The android root certificate stores. In *Proc. ACM CoNEXT*, 2014.

[17] N. Vallina-Rodriguez, S. Sundaresan, C. Kreibich, N. Weaver, and V. Paxson. Beyond the radio: Illuminating the higher layers of mobile networks. In *Proc. ACM MobiSys*, 2015.

[18] N. Vallina-Rodriguez, S. Sundaresan, C. Kreibich, N. Weaver, and V. Paxson. CRAWDAD data set *icsi/netalyzr-android* (v. 2015-03-24). http://crawdad.org/icsi/netalyzr-android/, 2015.

[19] Jan Vermeulen. Vodacom number leak fix: all the details. http://mybroadband.co.za/news/security/113149-vodacom-number-leak-fix-all-the-details.html.

[20] N. Weaver, C. Kreibich, M. Dam, and V. Paxson. Here Be Web Proxies. In *Proc. PAM*, 2014.