



# Header Enrichment or ISP Enrichment?

## Emerging Privacy Threats in Mobile Networks

**Narseo Vallina-Rodriguez**, *ICSI*  
Srikanth Sundaresan, *ICSI*  
Christian Kreibich, *ICSI / LastLine*  
Vern Paxson, *ICSI / UC Berkeley*

“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”

–Colson Hillier, *VP of Verizon’s Precision Market Insight division.*



# HTTP Header Enrichment

(a.k.a Header Injection)

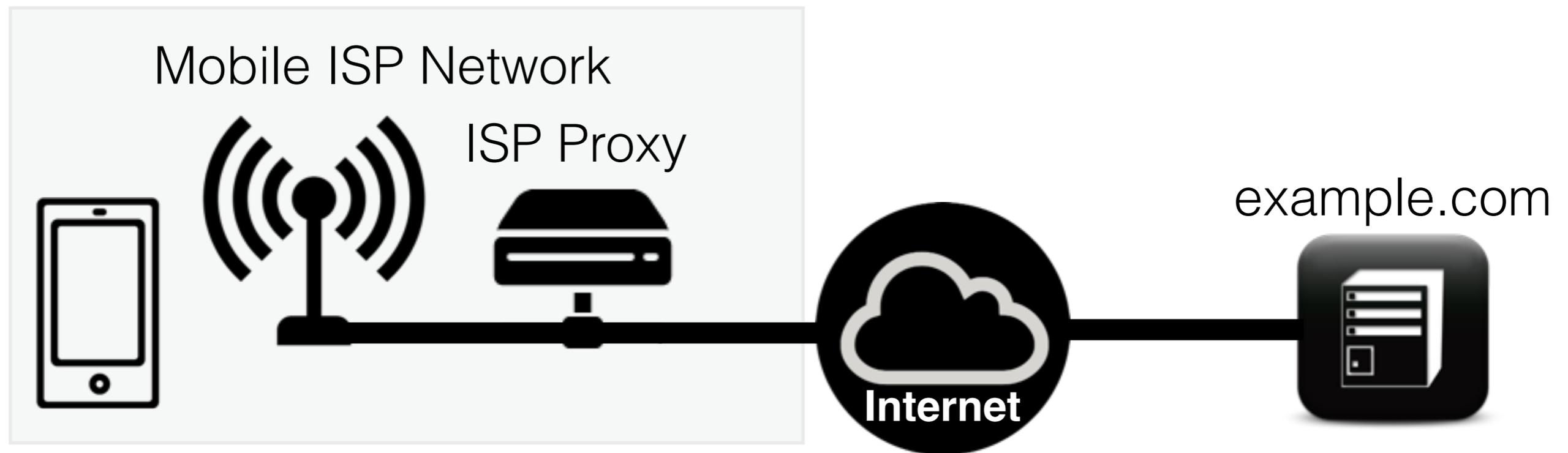
IETF Working Group **SFC**  
**S**ervice **F**unctioning **C**haining

<https://datatracker.ietf.org/wg/sfc/documents/>

# HTTP Header Enrichment

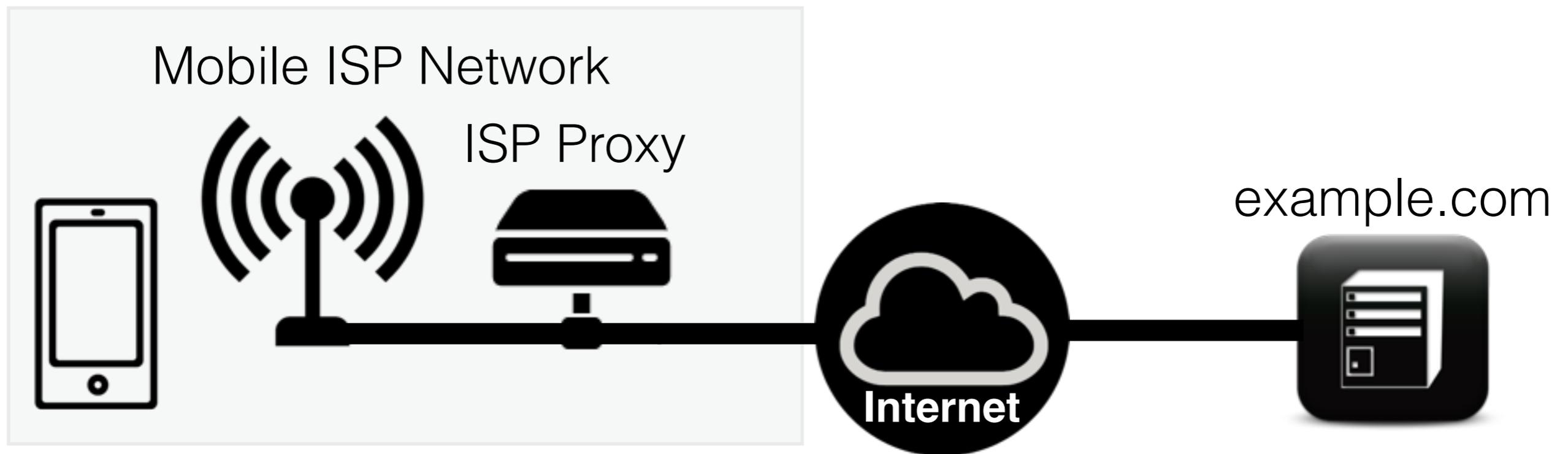
- Technique that allows ISP-enforced proxies to extend/inject HTTP headers for:
  - ▶ Performance Enhancement
  - ▶ Load Balancing
  - ▶ Access Control
  - ▶ Content Customization
  - ▶ Analytics
  - ▶ **Advertising and user-tracking**

# How does HTTP Header Enrichment work?



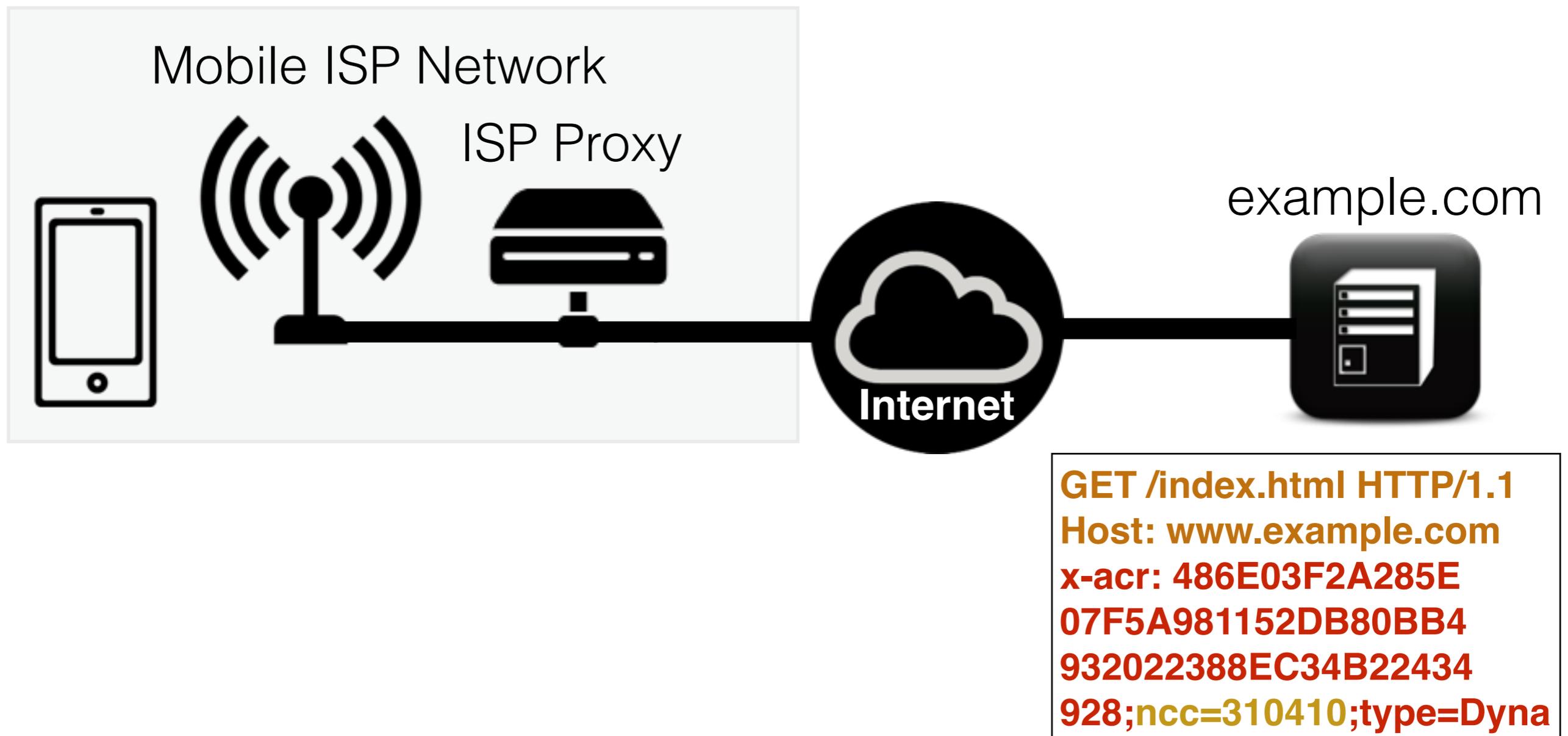
GET /index.html HTTP/1.1	GET /index.html HTTP/1.1
Host: www.example.com	Host: www.example.com
	x-acr: 486E03F2A285E 07F5A981152DB80BB4 932022388EC34B22434 928;ncc=310410;type=Dyna

# How does HTTP Header Enrichment work?



```
GET /index.html HTTP/1.1  
Host: www.example.com  
x-acr: 486E03F2A285E  
07F5A981152DB80BB4  
932022388EC34B22434  
928;ncc=310410;type=Dyna
```

# How does HTTP Header Enrichment work?



# User Implications

- HTTP Header Enrichment may become a privacy threat for mobile users:
  - ▶ ISPs may **leak** sensitive user and device data
  - ▶ ISPs may enable **user-tracking** (unique IDs)

# Why does it matter?

- User sensitive data may be **collected** and **combined** with other metadata by **any** online service if not removed by the egress point
- IETF GW SFC leaves this decision up to the ISP



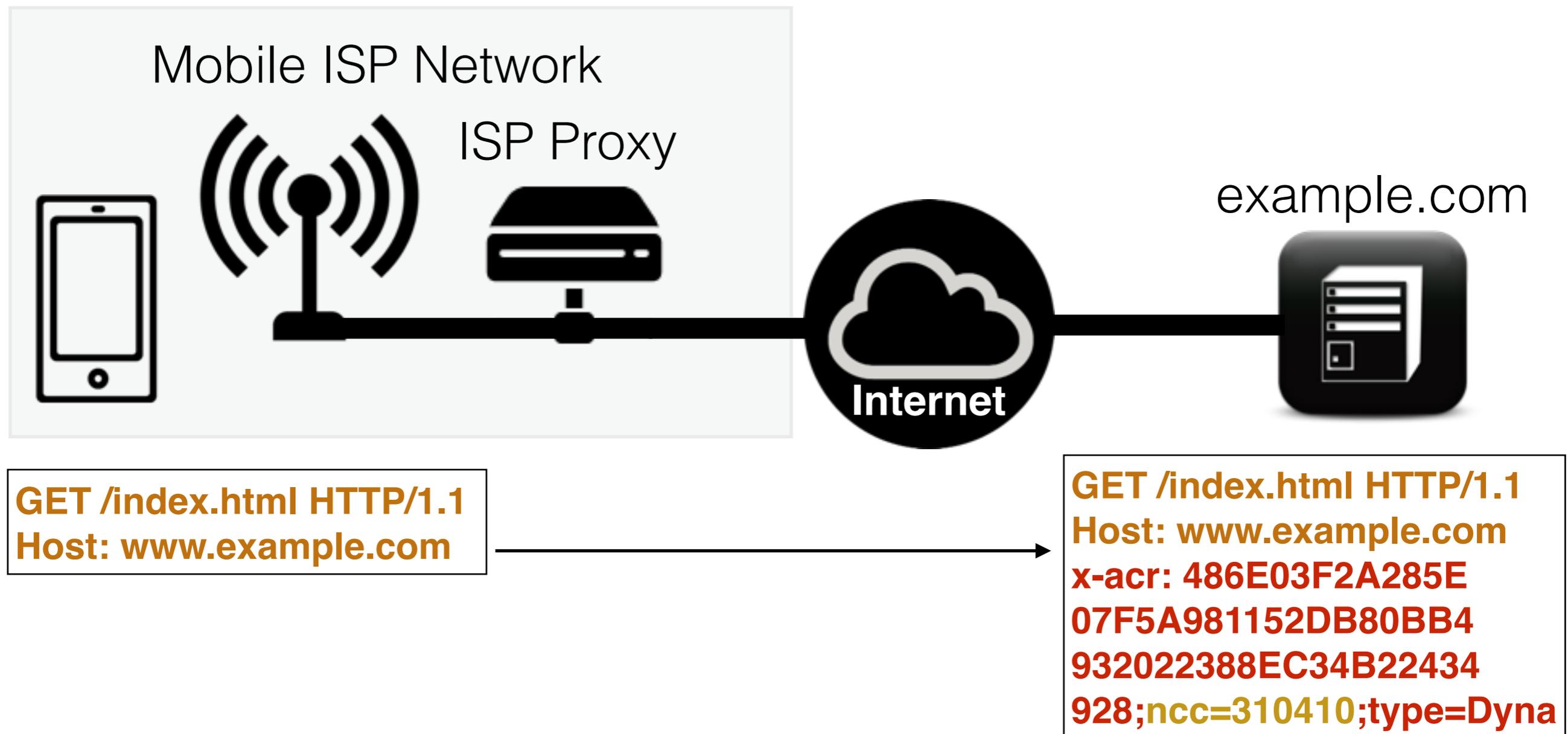
Inappropriate use of HTTP Header Enrichment  
affects millions of mobile subscribers  
all over the world

# Paper Contributions

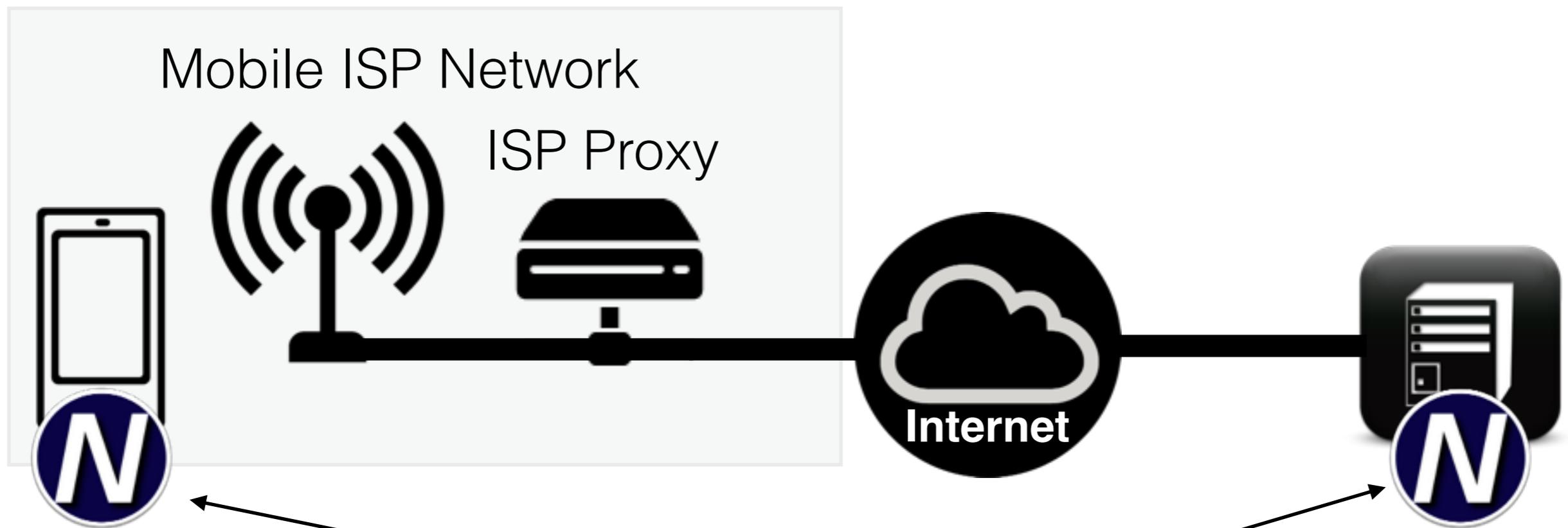
- Identification, analysis and characterization of HTTP Header Enrichment:
  - ▶ 299 Mobile ISPs from 112 countries
  - ▶ 16-month period
- Data collection: **Netalyzr** for **Android** traces
- Discussion of user implications and solutions

# Method and Data Collection

# How does HTTP Header Enrichment work?



# Netalyzr: Proxy Artifacts Detection



We control both end-points and generated traffic:  
**we can identify modifications!**

# Method Limitations

- We cannot identify when HTTP Header Injection occurs to selected destinations (e.g., ISP partners)
- Crowd-sourcing data collection: discrete sampling

# Results

# HTTP Header Analysis

We defined 3 categories:

✓ Privacy-compromising headers

✓ Tracking headers

● Operational headers

## **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

# 1 Privacy-compromising headers

**Definition:** HTTP headers leaking sensitive information that identify uniquely:

- ▶ the device (e.g., **IMEI**)
- ▶ the user (e.g., **IMSI/MSISDN**)

Identified in **5 mobile operators**

# 1 Privacy-compromising headers

<b>x-up-calling-line-id</b>	Vodacom (ZA)	Phone #
<b>msisdn</b>	Orange (JO)	MSISDN
<b>x-nokia-msisdn</b>	Smart (PH)	
<b>x-up-3gpp-imeisv</b>	Vodacom (ZA)	IMEI

**x-up-3gpp-imeisv: 35858805517XXXXX**

## 2 Tracking headers

**Definition:** Operator-generated unique identifier for **advertising** purposes

- ▶ They are immutable
- ▶ They do not directly reveal sensitive information about users but enable user-tracking

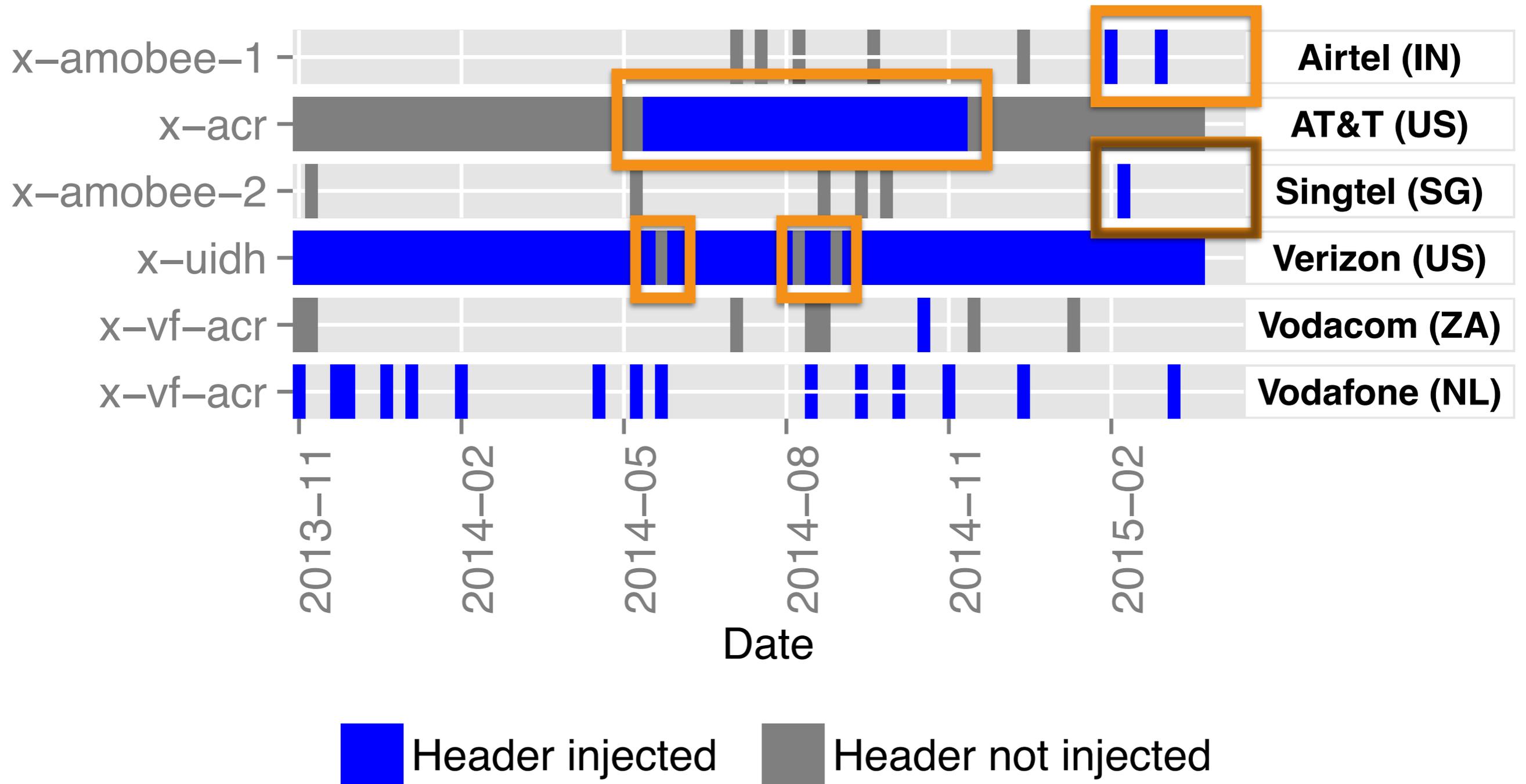
Identified in **6 mobile operators**

## 2 Tracking headers

<b>x-acr</b>	AT&T (US)
<b>x-amobee</b>	Airtel (IN), Singtel (SG)
<b>x-uidh</b>	Verizon (US)
<b>x-vf-acr</b>	Vodacom (ZA), Vodafone (NL)

```
x-acr: 486E03D [...]D359D;ncc=310410;type=Dyna
```

# 2 Tracking headers



# 3 Operational headers

**Definition:** HTTP headers for operational purposes. They contain information such as:

- ▶ Mobile operator (**MCC/MNC** codes) and 3GPP technology
- ▶ 3GPP Gateway, manufacturer (**Nokia/BlueCoat**), software version and even its location
- ▶ Handset's private IP address

Identified in **24 operators**

# 3 Operational headers

Use-case: **x-forwarded-for** header [RFC 7239]

- ▶ Reports the internal IP address of proxied traffic
- ▶ Used for load-balancing and abusive access

Flip-side:

- ▶ **De-anonymizes** traffic
- ▶ It may not tell the truth!

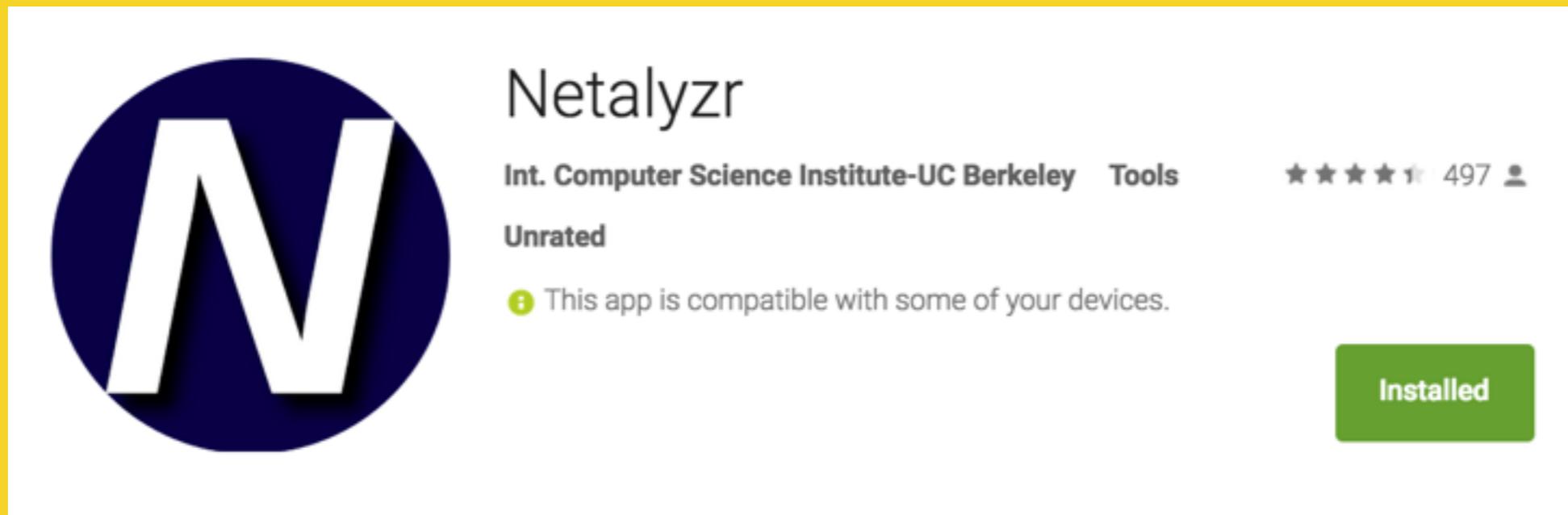
**T-Mobile (DE):** Private IP **10.92.13.12**->**17.92.13.12**

# Final Remarks

# What can users do?

- ▶ Tech-savvy users may use **VPNs**
- ▶ “**Do-Not-Track**” header is useless

# Be aware and complain



<http://amibeingtracked.com>

**This problem also requires  
non-technical solutions**

# This is an increasing concern!

- Evidence of **JavaScript injection** for advertising
- New **3rd party services** providing advertising services for ISPs
- No evidence of header injection in **HTTPS** traffic (**yet**)

narseo@icsi.berkeley.edu  
netalyzr-help@icsi.berkeley.edu