

Tracking and privacy

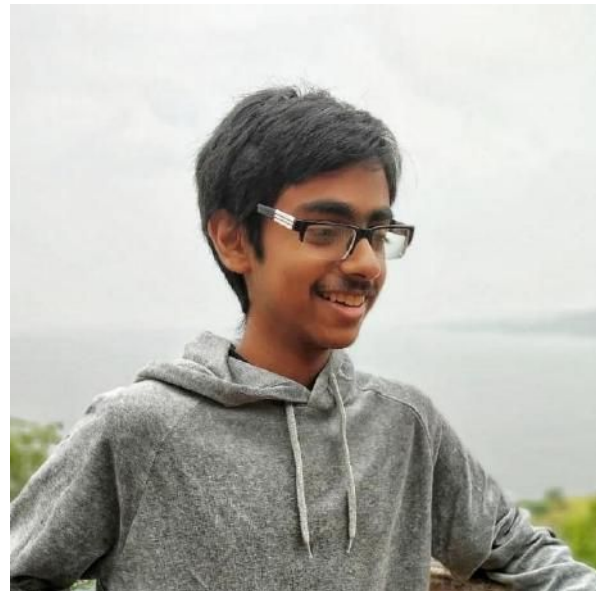
Sohom Datta

sdatta4@ncsu.edu

North Carolina State University

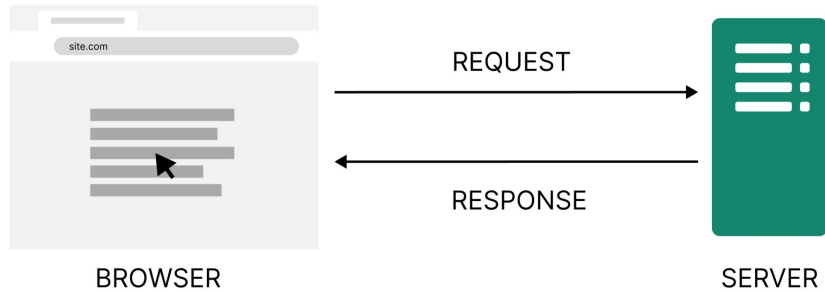
\$ whoami

- PhD student at NC State
- Interested in web-security and privacy



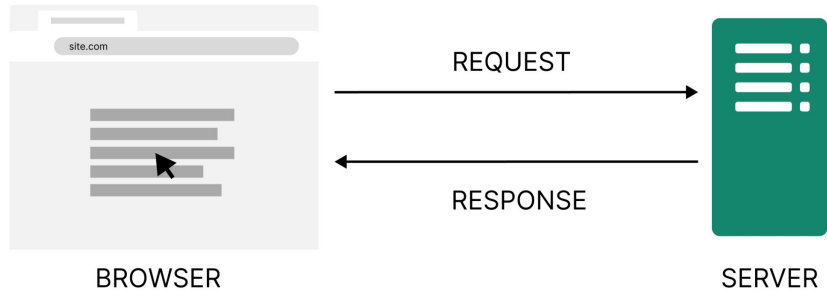
The Actual Web

Expectation

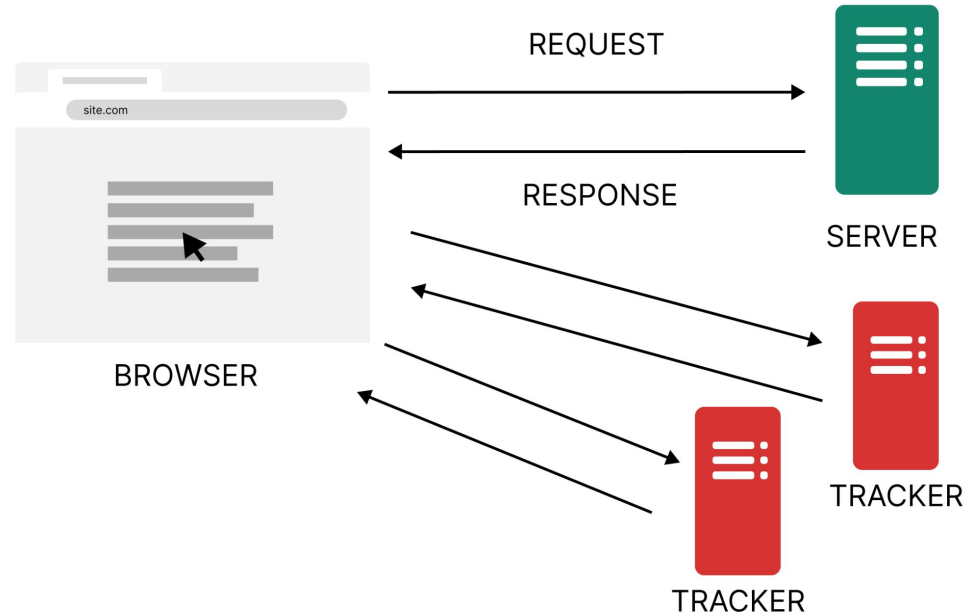


The Actual Web

Expectation

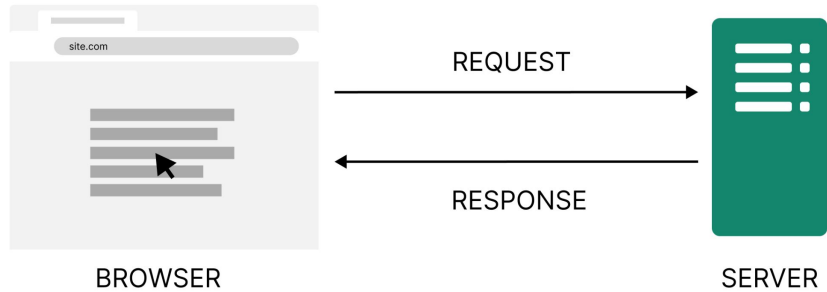


Reality

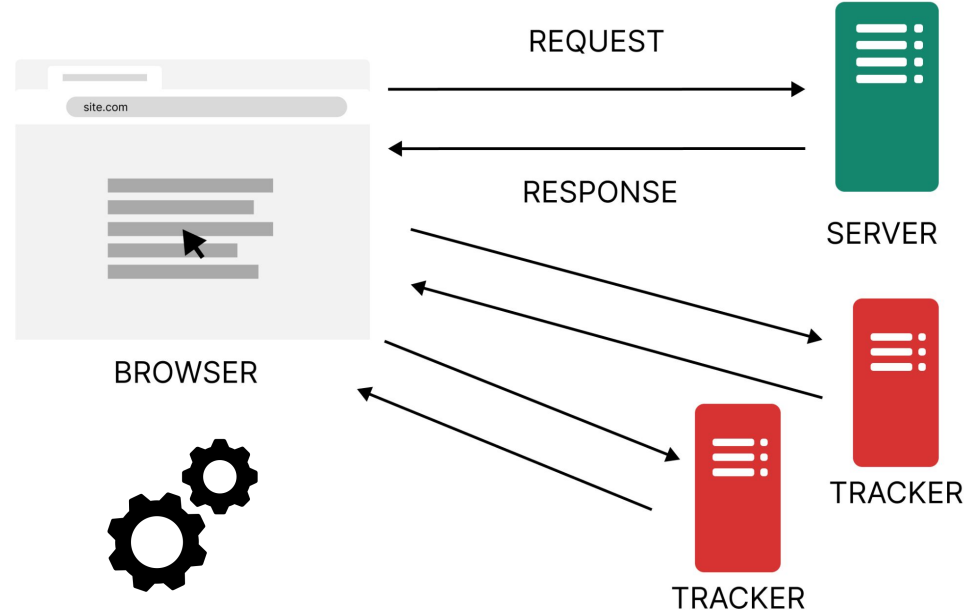


The Actual Web

Expectation



Reality



The anatomy of a tracker

The screenshot shows a browser's Network tab with a GET request to a tracking URL. The URL is highlighted in a red box and contains a long alphanumeric identifier. The response headers show a 42 status code and a Content-Type of 'image/gif'. A Set-Cookie header is present, containing a long alphanumeric string and a domain. The screenshot is annotated with red boxes and arrows pointing to these elements.

Name	Value
Request URL	https://simage2.pubmatic.com/AdServer/Pug?vcode=bz0yJnR5cGU9MSZjb2RIPTI4NDkmdGw9MTISNjAw&piggybackCookie=51743de3-207f-4b0e-93b7-fb66c9ba28b2&gdpr=0&gdpr_consent=
Request Method	GET
Status Code	200 OK
Remote Address	8.28.7.83:443
Referrer Policy	strict-origin-when-cross-origin
Cache-Control	no-store, no-cache, private
Content-Length	42
Content-Type	image/gif; charset=utf-8
Date	Sun, 19 Apr 2026 16:44:02 GMT
P3p	CP="NOI DSP COR LAW CUR ADMo DEVo TALo PSAo PSDo IVAo IVDIo HISo OTPo OUR SAMo BUS UNI COM NAV INT DEM CNT STA PRE LOC"
Server	nginx
Set-Cookie	KRTBCOOKIE_377=6810-51743de3-207f-4b0e-93b7-fb66c9ba28b2&KRTB&22918-51743de3-207f-4b0e-93b7-fb66c9ba28b2&KRTB&22926-51743de3-207f-4b0e-93b7-fb66c9ba28b2&KRTB&23031-51743de3-207f-4b0e-93b7-fb66c9ba28b2; domain=pubmatic.com; SameSite=None; secure; expires=Sat, 18-Jul-2026 16:44:02 GMT; path=/
Set-Cookie	PugT=1776617042; domain=pubmatic.com; SameSite=None; secure; expires=Tue, 19-May-2026 16:44:02 GMT; path=/
Strict-Transport-Security	max-age=16070400; includeSubDomains

Takes in identifier(s)

Imperceptible to humans

Generates third-party cookies

Too many third-party cookies :(

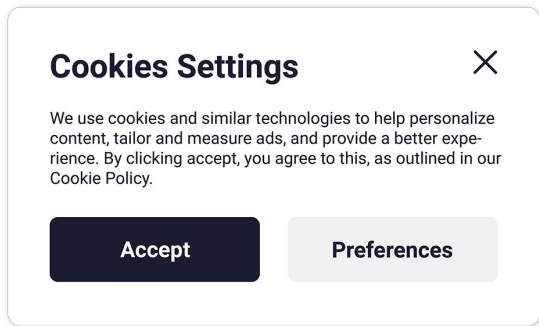
Application

Filter

Only show cookies with an issue

Name	Value	Domain	Path	Expires ...	Size	HttpOnly	Secure	SameSite	Partitio...	Cross Site	Priority
_ga	GA11.1.67995221.1776617121	.pubma...	/	2027-05...	28						Medium
_ga_7EY3MG987N	CS2.1s1776617120s01\$g0\$t1776617120s\$j60\$10\$0	.pubma...	/	2027-05...	59						Medium
_gcl_au	1.1.641055337.1776617121	.pubma...	/	2026-07...	31						Medium
_ketch_consent_v1	eyJhbmFseXRpY3MiOnsic3RhdHvzjoiz3JhbnRlZC1sm...	.pubma...	/	2027-05...	422		✓	None			Medium
_swb	a9330492-1edc-4f71-9404-07c5c699e147	.pubma...	/	2027-05...	40		✓	None			Medium
_swb_consent_	eyJjb2xsZWNOZWRBdCI6MTc3NjYxNzExNSwYy29udGV...	.pubma...	/	2026-04...	869		✓	None			Medium
_twpid	bw.1776617120820.465917206899261202	.pubma...	/	2027-05...	41		✓	Strict			Medium
ANON_ID_old	auntAZcwl6h7bQqwPBqU7vupZdkaZa3OdJmZbgnp...	.tribalfu...	/	2026-07...	116			○			Medium
chkChromeAb675ec	4	.pubma...	/	2026-07...	17		✓	None			Medium
DPSync4	1776643200%3A248%7C1777766400%3A197_226_21...	.pubma...	/	2026-07...	108		✓	None			Medium
KADUSERCOOKIE	29034C46-6C85-41BC-Bc43-3974EBD4360F	.pubma...	/	2027-04...	49		✓	None			Medium
KRTBCOOKIE_1101	23040-7630516134524680559&KRTB&23369-7630516...	.pubma...	/	2026-05...	102		✓	None			Medium
KRTBCOOKIE_1251	23269-dj_027df6b9c723701dcbfd0&KRTB&23571-dj_0...	.pubma...	/	2026-07...	153		✓	None			Medium
KRTBCOOKIE_1278	23329-74f1677a-e18b-4f0a-849f-6c3f110deba2&KRTB...	.pubma...	/	2026-07...	153		✓	None			Medium
KRTBCOOKIE_1323	23524-OPU8a1e8b65ec52491ebb47e56d6ee0da80&K...	.pubma...	/	2026-05...	197		✓	None			Medium
KRTBCOOKIE_1466	23578-b1206ee9-71fb-467b-1f4-3a50c7ea257d&KRTB...	.pubma...	/	2026-05...	105		✓	None			Medium
KRTBCOOKIE_148	19421-uid:357909DD1CDC44DA9B9895B2A284A184&...	.pubma...	/	2026-05...	200		✓	None			Medium
KRTBCOOKIE_153	19420-OHSdD5xPasjijFbPSYKX212MA8jDjgJpXDXioX...	.pubma...	/	2026-07...	216		✓	None			Medium
KRTBCOOKIE_18	22947-2809753649871299401&KRTB&23796-2809753...	.pubma...	/	2026-07...	69		✓	None			Medium
KRTBCOOKIE_188	3189-09e146bb-565c-4090-bff0-27c67819f90-69e506...	.pubma...	/	2026-07...	193		✓	None			Medium
KRTBCOOKIE_22	14911-8292830797813350638&KRTB&23150-8292830...	.pubma...	/	2026-05...	131		✓	None			Medium
KRTBCOOKIE_27	16735-uid:7fcb69e5-0652-4a00-9e3a-5e012e864ae	.pubma...	/	2026-07...	59		✓	None			Medium
KRTBCOOKIE_279	22890-5f689c63-facd-4d19-992a-fef9b21af5a9&KRTB&...	.pubma...	/	2026-05...	200		✓	None			Medium
KRTBCOOKIE_32	11175-AQAH-J7ZoBDEEWJFoUtaAQEBAQEBAQCcp6A...	.pubma...	/	2026-07...	247		✓	None			Medium
KRTBCOOKIE_377	6810-51743de3-207f-4b0e-93b7-fb66c9ba2bb2&KRTB...	.pubma...	/	2026-07...	199		✓	None			Medium
KRTBCOOKIE_391	22924-8866556683318959751&KRTB&23231-8866556...	.pubma...	/	2026-05...	132		✓	None			Medium
KRTBCOOKIE_452	23026-y-c4qeD7dE2oB4iyQVYFFakRzQYUcJtYl.WoZCF...	.pubma...	/	2026-05...	232		✓	None			Medium
KRTBCOOKIE_466	16530-d04330ab-9739-4b36-81a1-9b2fFe3abbaF&KRTB...	.pubma...	/	2026-07...	104		✓	None			Medium
KRTBCOOKIE_52	22772-R37AA4_139D286FD_10708E1C62&KRTB&2309...	.pubma...	/	2026-05...	124		✓	None			Medium
KRTBCOOKIE_57	22776-936472941663425602&KRTB&23339-93647294...	.pubma...	/	2026-07...	67		✓	None			Medium
KRTBCOOKIE_632	23041-UHszqFPPLojzJTH81sUvbHL-6ayKp2-QoqYMsxe...	.pubma...	/	2026-05...	228		✓	None			Medium
KRTBCOOKIE_80	16514-CAESE.JoaAa_cz1jwfbSM1XKlc&KRTB&22987...	.pubma...	/	2026-05...	163		✓	None			Medium
KRTBCOOKIE_860	16335-t8p3s6InUhfD25-1qjHVGsNxx&KRTB&23334-t...	.pubma...	/	2026-07...	164		✓	None			Medium
KRTBCOOKIE_945	19558-2b52a8a3-374f-4711-a2a0-5ed9037d4bc5	.pubma...	/	2026-07...	56		✓	None			Medium
KRTBCOOKIE_964	20918-cuid_f8ad9451-3c0e-11f1-bc59-42010ab2fff3&K...	.pubma...	/	2026-07...	220		✓	None			Medium
pi	163427:3	.pubma...	/	2026-04...	10		✓	None			Medium

This caused regulator action



- Ask for consent before tracking
- Identifier data should be kept private
- If you want to sell the data, consumer should know who you sell the data to
- Consumer should be able to opt out

Enter stateless tracking

Slide credit @Junhua



JavaScript (Browser APIs)



Enter stateless tracking

```
function generateCanvasFingerprint() {
  const canvas = document.createElement("canvas");
  const ctx = canvas.getContext("2d");
  document.body.appendChild(canvas);
  canvas.width = 240;
  canvas.height = 60;
  ctx.textBaseline = "alphabetic";
  ctx.fillStyle = "#f60";
  ctx.fillRect(100, 1, 62, 20);
  ctx.fillStyle = "#069";
  ctx.font = '11pt "Times New Roman"';
  const text = "Cwm fjordbank gly " + String.fromCharCode(55357, 56835);
  ctx.fillText(text, 2, 15);
  ctx.fillStyle = "rgba(102, 204, 0, 0.2)";
  ctx.font = "18pt Arial";
  ctx.fillText(text, 4, 45);
  return canvas.toDataURL();
}
generateCanvasFingerprint();
```



Cwm fjordbank gly 😊
Cwm fjordbank gly 😊

`"data:image/png;base64,iVBORw0KGgoAAAANSUhEU...."`

How do we detect it?



- Short answer: You scan the web!
- Measure “entropy” of JS code
- If it collects too much entropy + sends the data to a server 🤔

```
$89:.....fetch("https://a.g.co/tracking", {...})
!89
...
g78:{Window:7439837}:"fetch"
c78:{Window:7439837}:%fetch:"https://a.g.co/tracking":{Object:788080:...}
...
...
```

Automatic Discovery of Emerging Browser Fingerprinting Techniques, Su et al.

Another project: github.com/duckduck-go/tracker-radar

How do I avoid it? (layman)

uBlock Origin Lite

[Remove from Chrome](#)

Featured 4.5★ (2.9K ratings) ⓘ ↵ Share

Extension

Privacy & Security

16,000,000 users

www.bloomberg.com

filtering mode
optimal

Ads, trackers, miners, and more
Block Outsider Intrusion into LAN
AdGuard URL Tracking Protection

More ^ Less

Settings About

Default filtering mode

The default filtering mode will be overridden by per-website filtering modes. You can adjust the filtering mode on any given website according to whichever mode works best on that website. Each mode has its advantages and disadvantages.

<input checked="" type="radio"/> Basic	<input type="radio"/> Optimal	<input type="radio"/> Complete
<p>Basic network filtering from selected filter lists.</p> <p>Does not require permission to read and change data on websites.</p>	<p>Advanced network filtering plus specific extended filtering from selected filter lists.</p> <p>Requires broad permission to read and change data on all websites.</p>	<p>Advanced network filtering plus specific and generic extended filtering from selected filter lists.</p> <p>Requires broad permission to read and change data on all websites.</p> <p>Generic extended filtering may cause higher webpage resources usage.</p>

How do I avoid it? (mobile)



How bad is it? (mobile)

Cross-Boundary Mobile Tracking: Exploring Java-to-JavaScript Information Diffusion in WebViews



Sohom Datta[†], Michalis Diamantaris[‡], Ahsan Zafar[†], Junhua Su[†],
Anupam Das[†], Jason Polakis^{*}, and Alexandros Kapravelos[†]

[†]North Carolina State University, USA
{sdatta4, azafar2, jus6, anupam.das, akprav}@ncsu.edu
[‡]Technical University of Crete, Greece
mdiamantaris@tuc.gr
^{*}University of Illinois Chicago, USA
polakis@uic.edu

Same Script, Different Behavior: Characterizing Divergent JavaScript Execution Across Different Device Platforms

Ahsan Zafar
azafar2@ncsu.edu
North Carolina State University
Raleigh, North Carolina, USA

Junhua Su
jsu6@ncsu.edu
North Carolina State University
Raleigh, North Carolina, USA

Sohom Datta
sdatta4@ncsu.edu
North Carolina State University
Raleigh, North Carolina, USA

Alexandros Kapravelos
akprav@ncsu.edu
North Carolina State University
Raleigh, North Carolina, USA

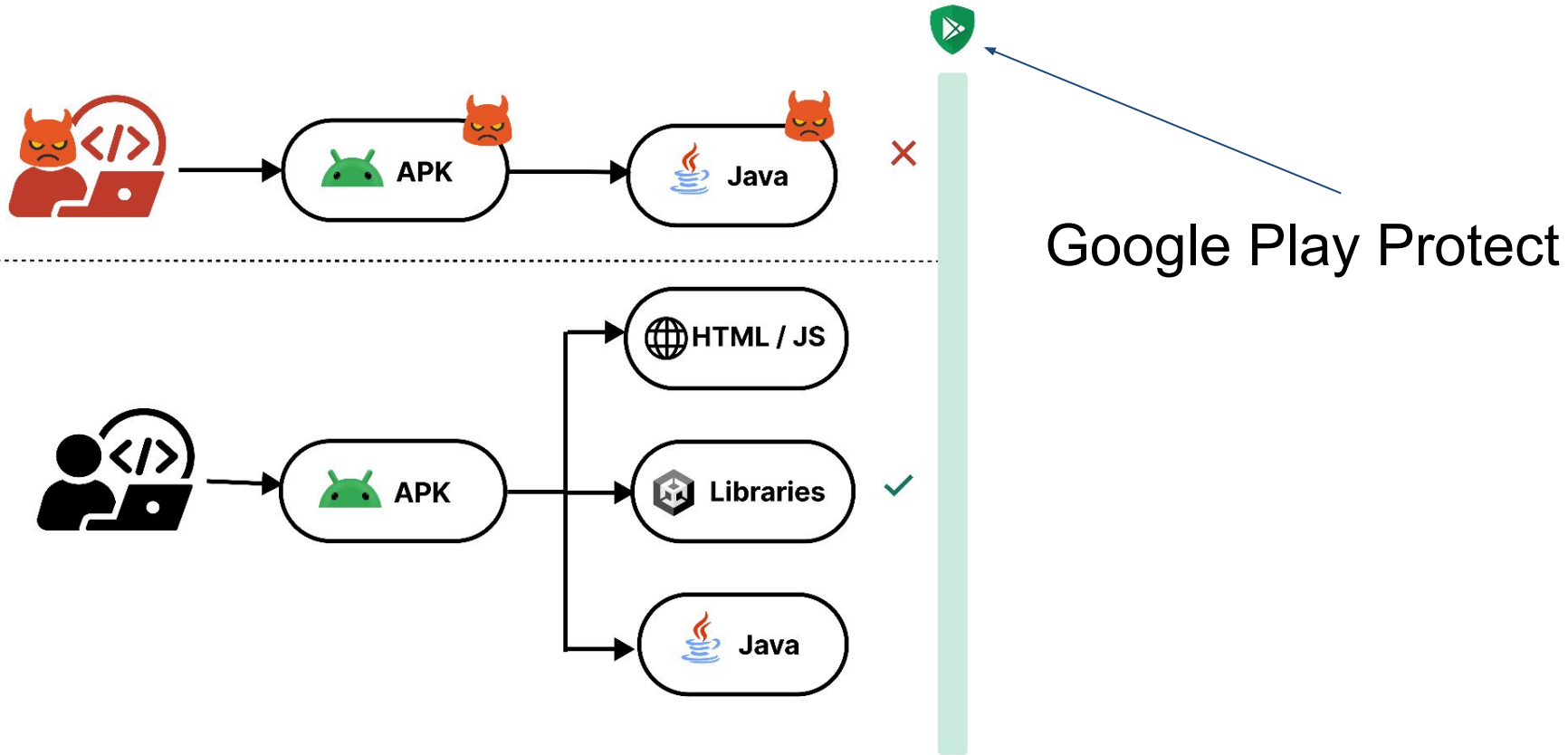
Anupam Das
anupam.das@ncsu.edu
North Carolina State University
Raleigh, North Carolina, USA

Short answer: Very very bad

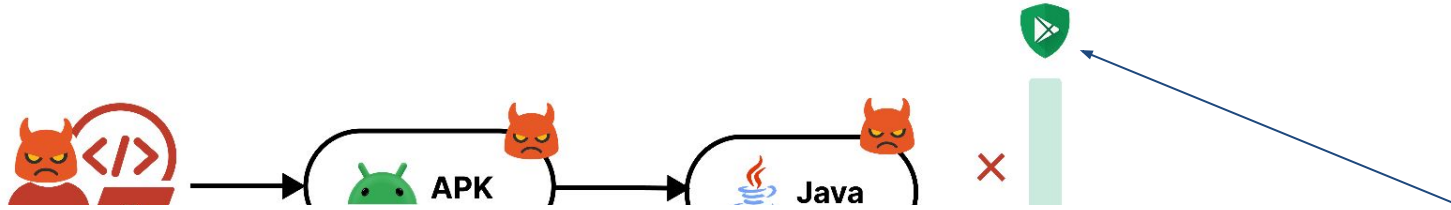
How bad is it? (mobile)

```
1  hasTouch: function() {
2      return !!navigator.maxTouchPoints || !!navigator.msMaxTouchPoints ||
      ↪ (l.matchMedia ? l.matchMedia("(any-pointer: coarse)").matches :
      ↪ "ontouchstart" in l)
3  }, isMobile: function() {
4      var e = navigator.userAgent;
5      return /Android|webOS|iPhone|iPad|iPod|Windows Phone|IEMobile|Opera
      ↪ Mini|Mobile|mobile|Tablet [^PC]|CriOS/i.test(e)
6  }
```

Android privacy was already bad



Android privacy was already bad

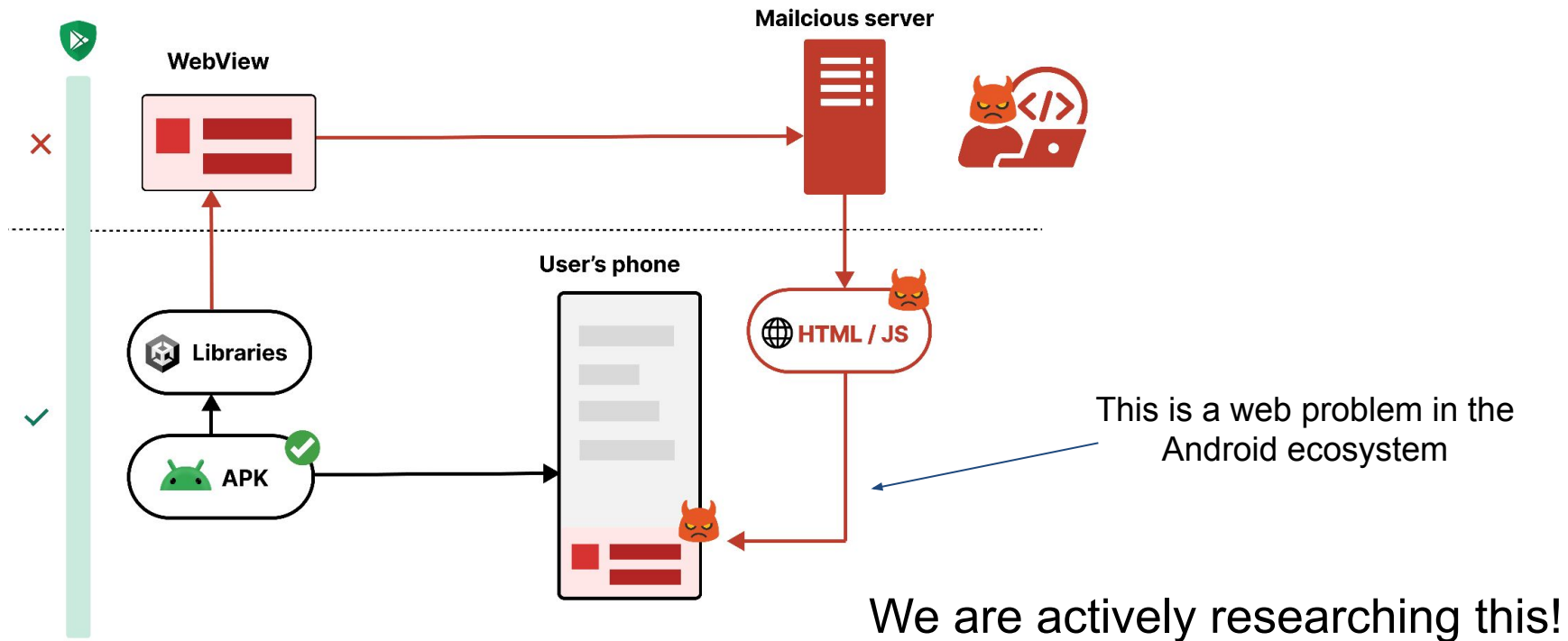


For Release

FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites



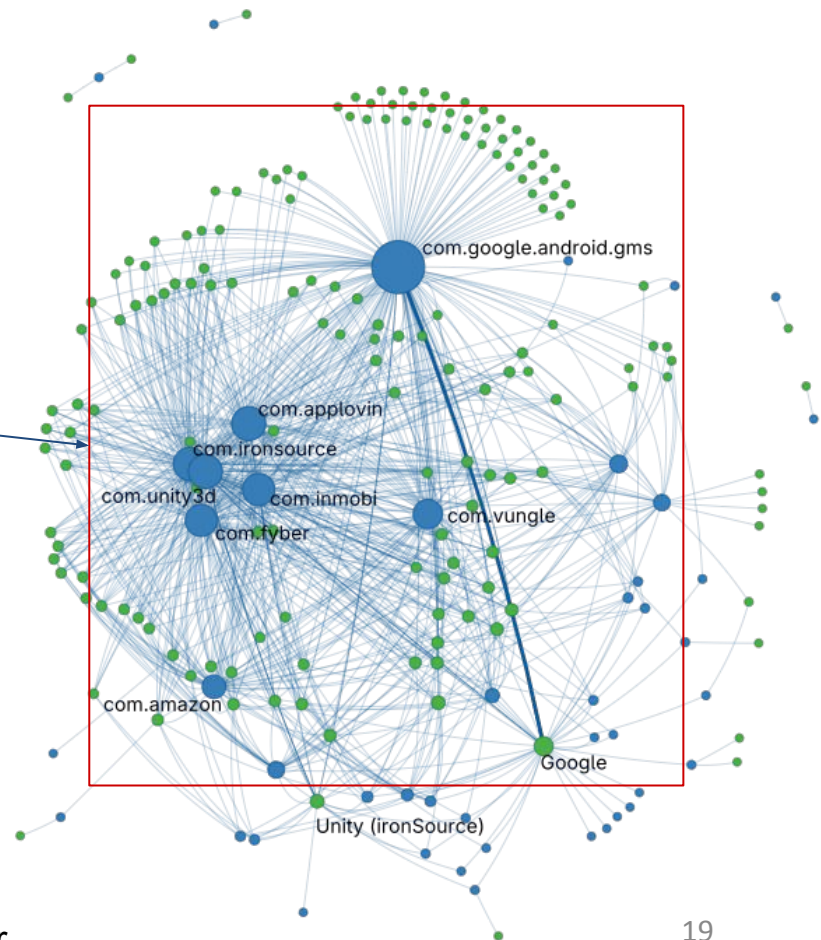
But WebViews enable evasive attacks



Entities involved in info leakage

Reality

! A small number of third-parties libraries exfiltrate to a large number of companies



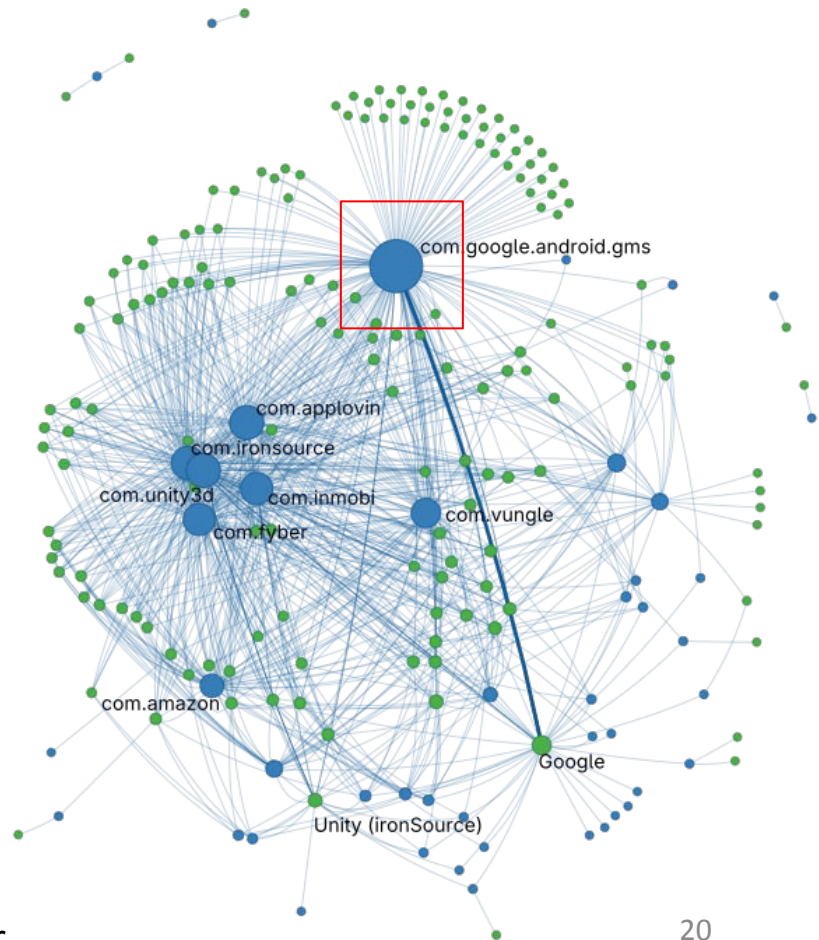
* Blue are third-party libraries

Green is companies based on DuckDuckGo Tracker Radar

Entities involved in info leakage

! `com.google.android.gms` is the largest player in our abuse ecosystem

! Google Play SDK has a degree of over 147 distinct companies

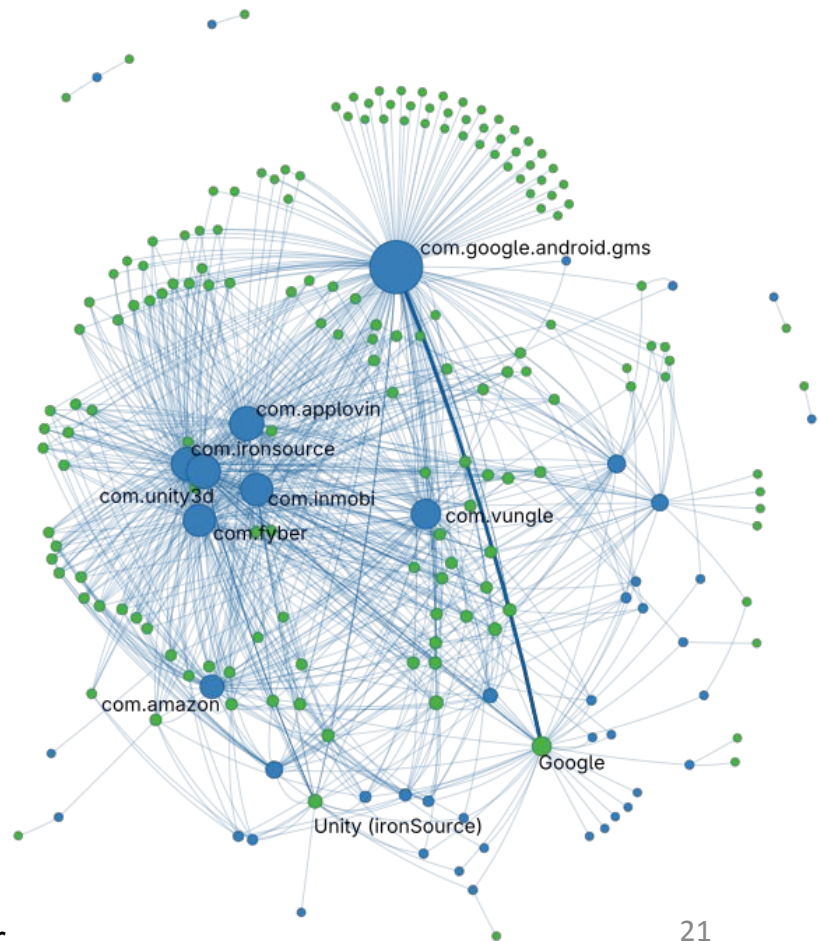


* Blue are third-party libraries

Green is companies based on DuckDuckGo Tracker Radar

Entities involved in info leakage

- ! 25 companies have a tracking-score of 0 on DuckDuckGo Tracker Radar
- ! Some trackers in our ecosystem are not being seen by traditional web tracking detectors



* Blue are third-party libraries
Green is companies based on DuckDuckGo Tracker Radar