KU LEUVEN

Leaky Forms: A Study of Email and Password Exfiltration Before Form Submission

Asuman Senol
imec-COSIC, KU Leuven
asuman.senol@esat.kuleuven.be

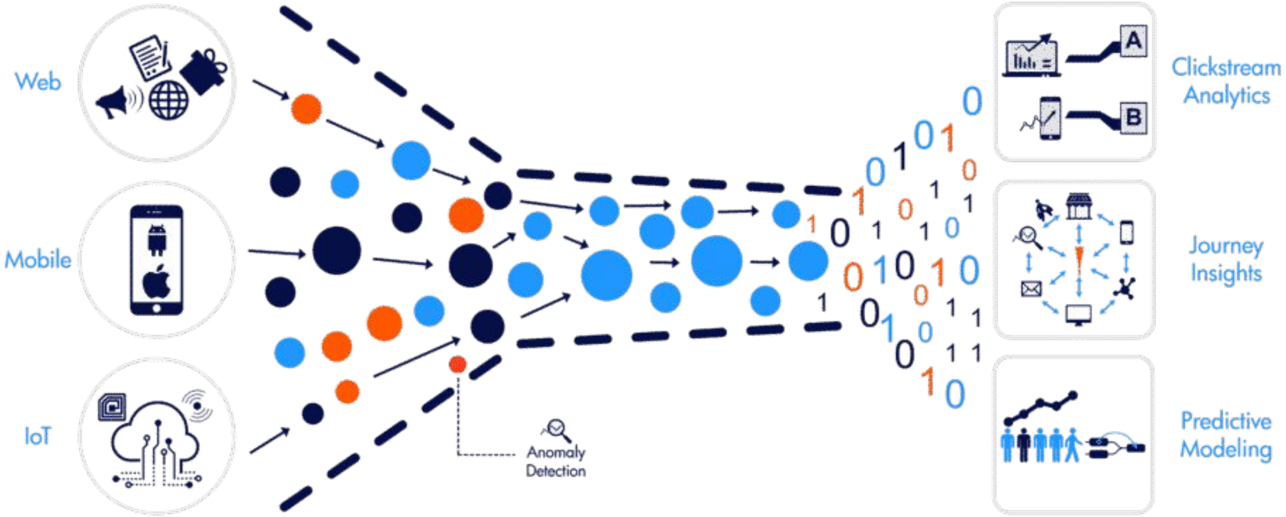
Gunes Acar
Radboud University
g.acar@cs.ru.nl

Mathias Humbert
University of Lausanne
mathias.humbert@unil.ch

Frederik Zuiderveen Borgesius
Radboud University
frederikzb@cs.ru.nl

Background

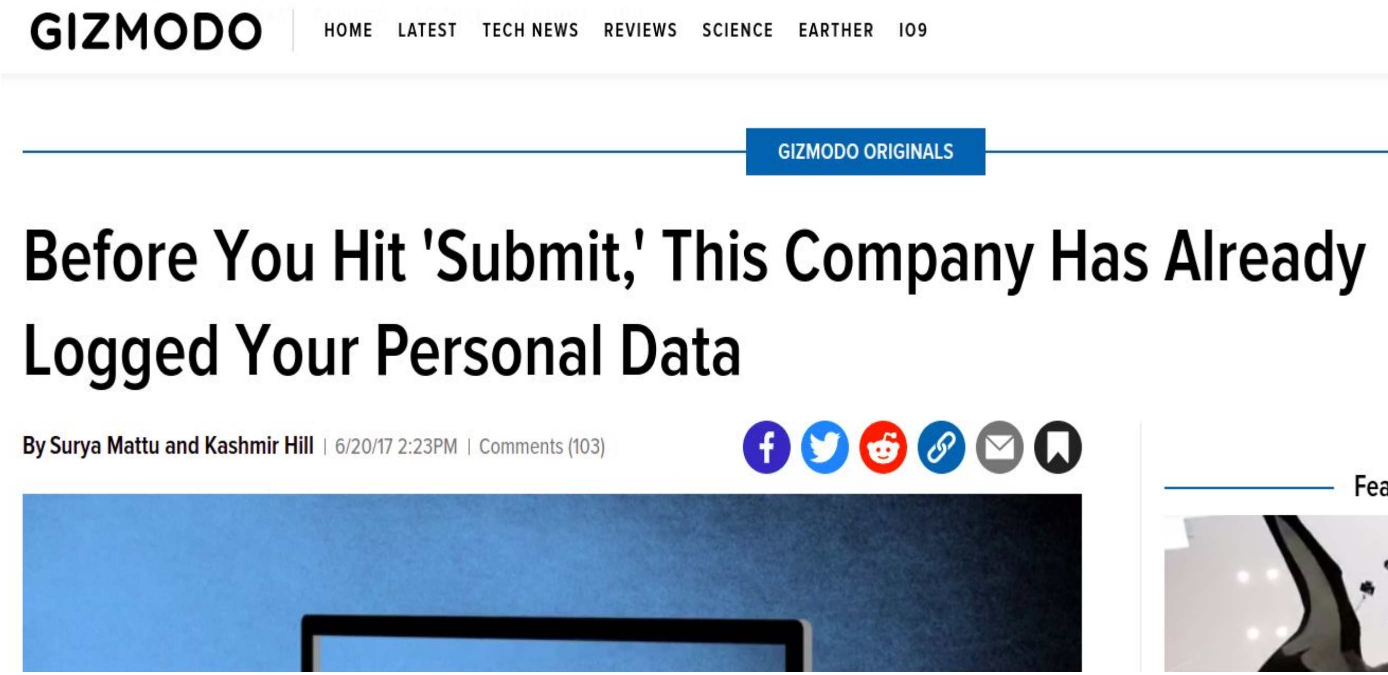
- Websites use advertising and marketing for monetization
  - built-in anti-tracking countermeasures
  - potential third-party cookie phase-out
- Tracking by email addresses
  - enables cross-site, cross-platform, persistent tracking



https://medium.com/@ugurekmekci/real-time-user-activity-tracking-w-divolte-collector-and-kafka-d8c106313400

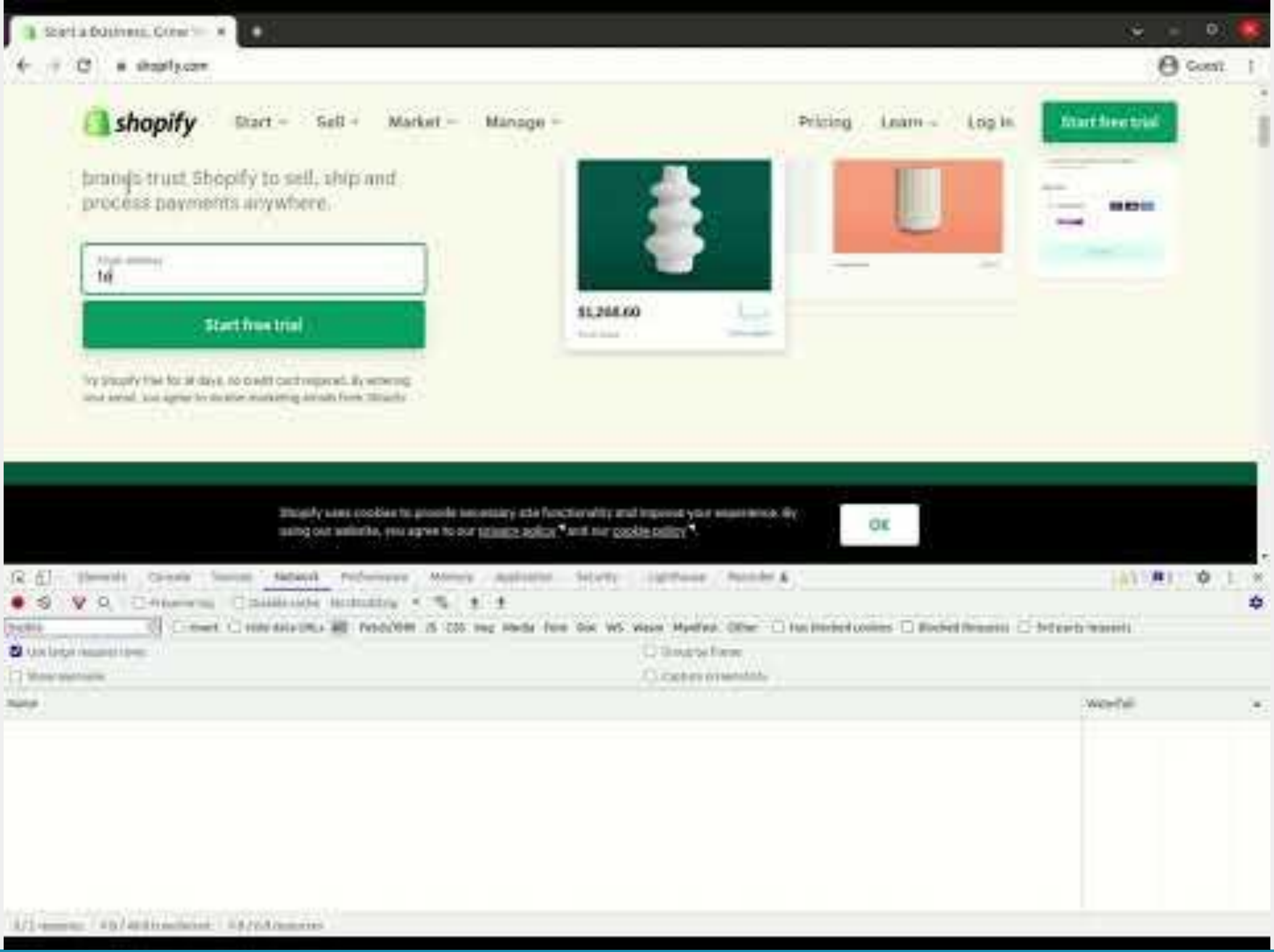
Motivation

- PII collection before form submission on a mortgage calculator website (Gizmodo, 2017)
- A 2018 survey (n=502):
    - 81% abandoned forms at least once
    - 59% abandoned a form in the last month [6].



Before You Hit 'Submit,' This Company Has Already Logged Your Personal Data

By Surya Mattu and Kashmir Hill | 6/20/17 2:23PM | Comments (103)



brands trust Shopify to sell, ship and process payments anywhere.

Email address: te

Start free trial

Try Shopify free for 14 days, no credit card required. By entering your email, you agree to receive marketing emails from Shopify.

Shopify uses cookies to provide necessary site functionality and improve your experience. By using our website, you agree to our privacy policy and our cookie policy.

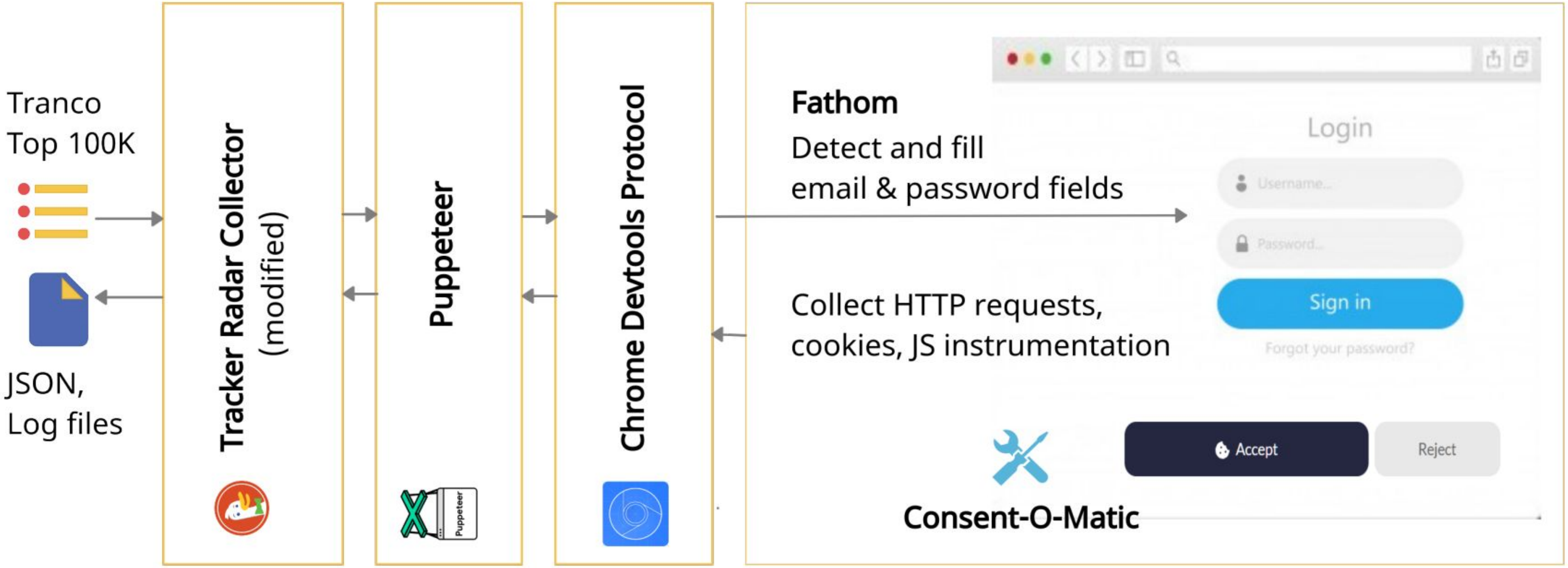
OK

Objectives

- Measure email and password collection prior to form submission
  - effect of location: EU vs. US
  - effect of consent
  - mobile vs. desktop

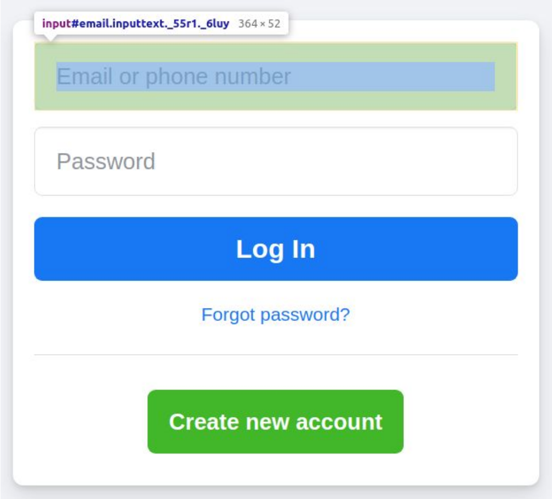
Method – Web Crawler

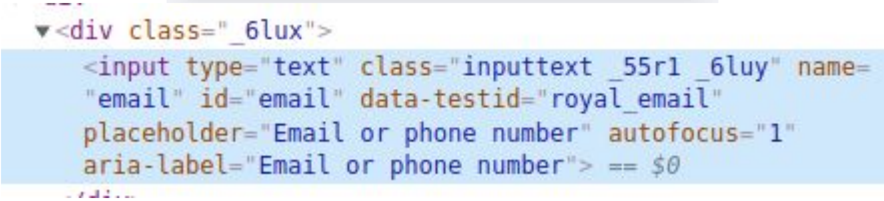
- Built on Tracker Radar Collector (developed by DuckDuckGo)



Method – Email field detection

- **Fathom**: A supervised learning framework specialized to detect webpage parts [8]

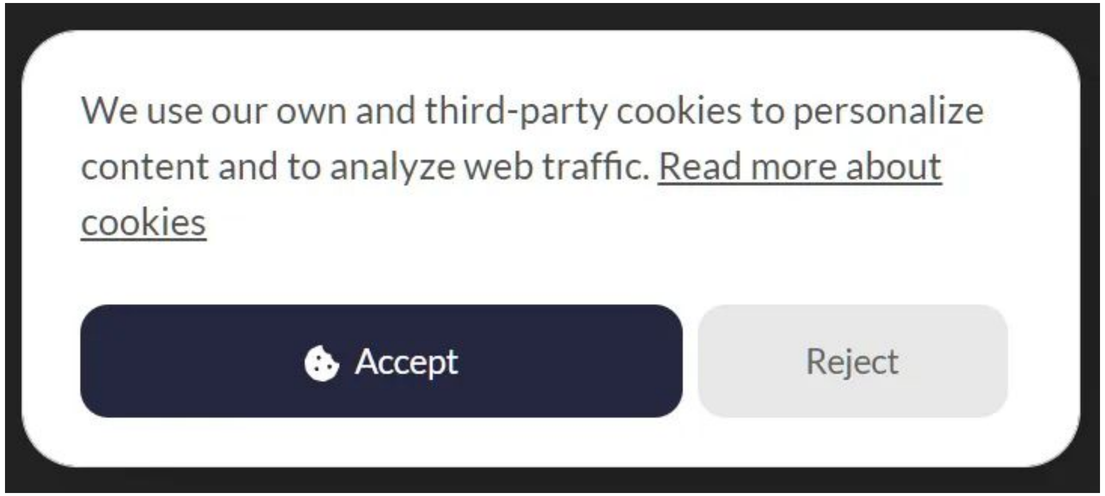




```
▼<div class="_6lux">
   <input type="text" class="inputtext _55r1 _6luy" name=
   "email" id="email" data-testid="royal_email"
   placeholder="Email or phone number" autofocus="1"
   aria-label="Email or phone number"> == $0
```

Method – CMP detection

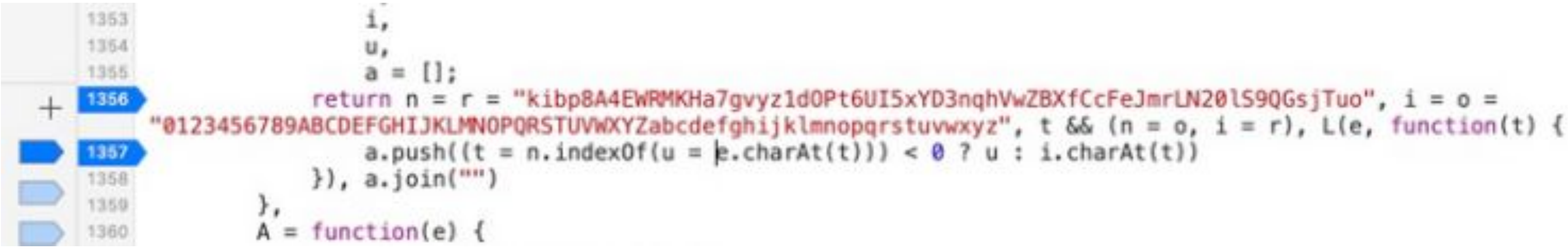
- **Consent-O-Matic**: browser extension that can recognize and interact with Consent Management Provider (CMP) pop-ups [7]
- Consent modes:
  - No-action
  - Accept-all
  - Reject-all
- ≈7,700/100K



We use our own and third-party cookies to personalize content and to analyze web traffic. Read more about cookies

Method – Leak Detection

- Based on Englehardt et al.’s method [3]
    - search for different encodings and hashes of search terms
- Identified two new encodings and a hashing method
    - LZString, custom mapping, hashing with a fixed salt



```
                i,
                u,
                a = [];
            return n = r = "kibp8A4EWRMKHa7gvyz1dOPt6UI5xYD3nqhVwZBXfCcFeJmrLN20lS9QGsjTuo", i = o =
"0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz", t && (n = o, i = r), L(e, function(t) {
                a.push((t = n.indexOf(u = e.charAt(t))) < 0 ? u : i.charAt(t))
            }), a.join("")
        },
        A = function(e) {
```

Method – Tracker Labeling

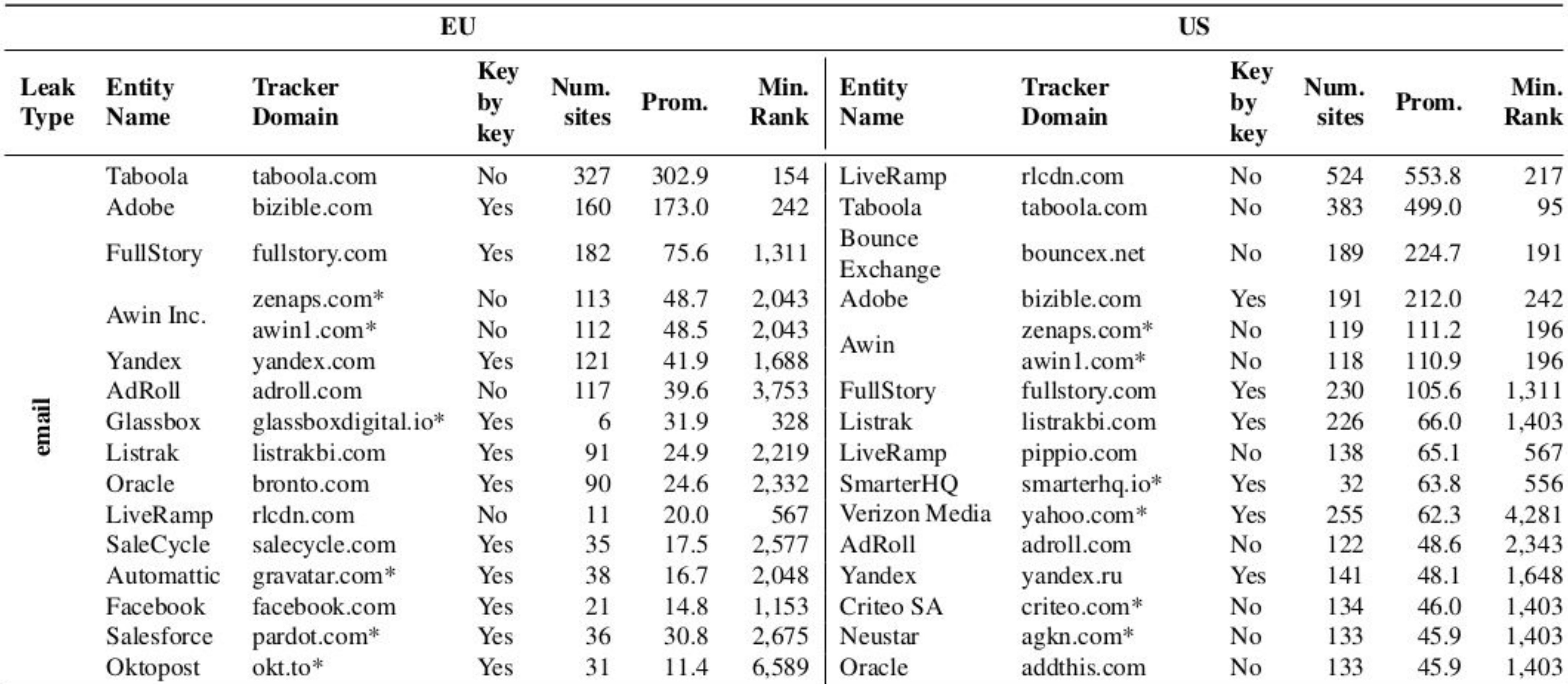
- Only considered leaks to tracker domains
- Block-lists we used:
    - Disconnect
    - Whotracks.me
    - DuckDuckGo (tds.json)
    - uBlock Origin
    - + Manual labeling

Dataset & Results (No interaction with the consent dialogs)

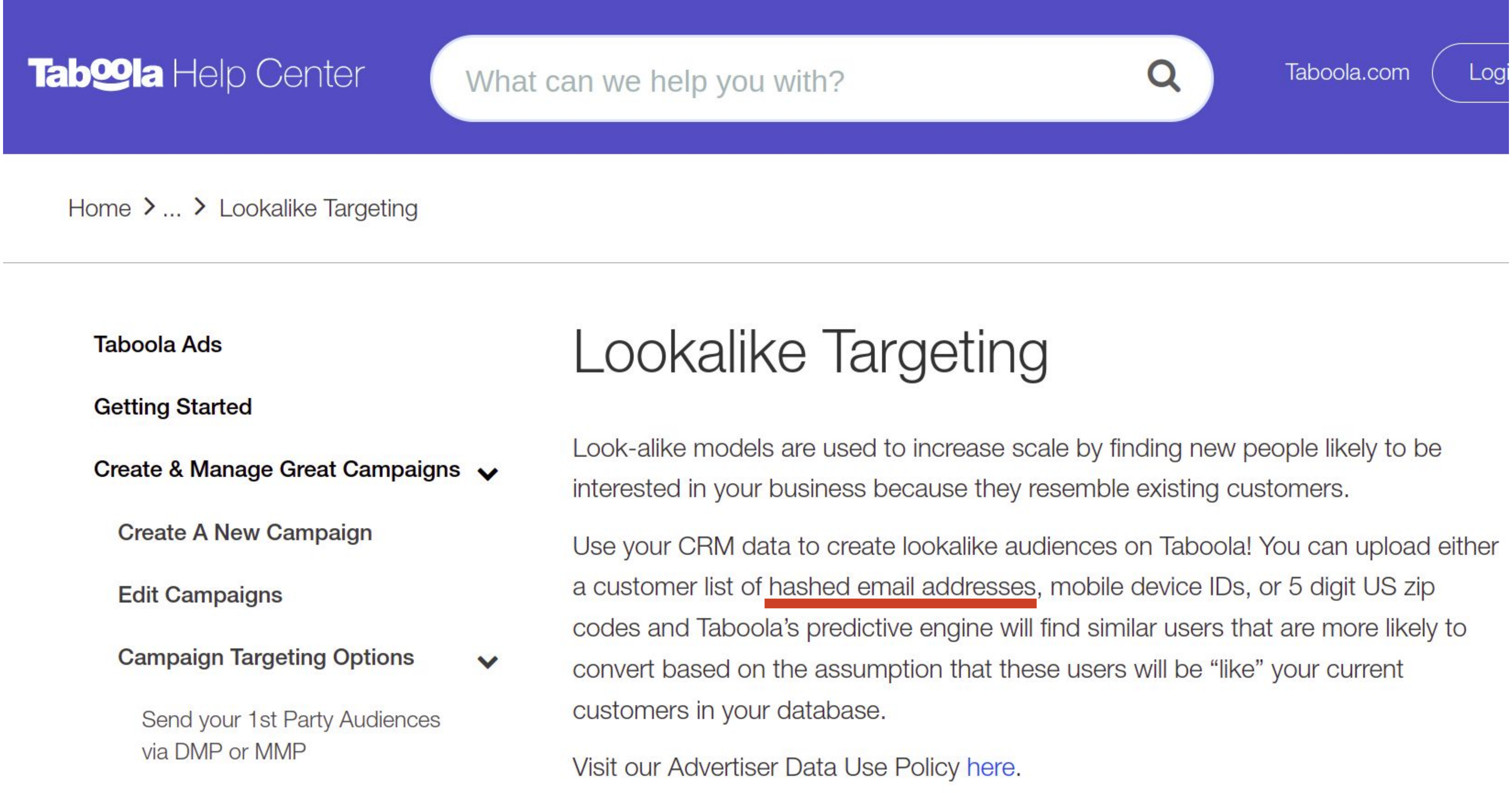
	Email		Password	
	EU	**US**	**EU**	**US**
Visited websites	99,380	99,437	99,380	99,437
Websites where we filled	52,055	53,038	31,002	31,324
Leaks to 1st party	4,395	5,518	89	92
Leaks to 3rd party	2,633	3,790	87	87
Leaks to trackers	**1,844**	**2,950**	**48**	**49**

Overview of crawl statistics based on servers located in EU and the USA

Results - Email Leaks



	EU						US					
Leak Type	**Entity Name**	**Tracker Domain**	**Key by key**	**Num. sites**	**Prom.**	**Min. Rank**	**Entity Name**	**Tracker Domain**	**Key by key**	**Num. sites**	**Prom.**	**Min. Rank**
email	Taboola	taboola.com	No	327	302.9	154	LiveRamp	rlcdn.com	No	524	553.8	217
	Adobe	bizible.com	Yes	160	173.0	242	Taboola	taboola.com	No	383	499.0	95
	FullStory	fullstory.com	Yes	182	75.6	1,311	Bounce Exchange	bouncex.net	No	189	224.7	191
	Awin Inc.	zenaps.com*	No	113	48.7	2,043	Adobe	bizible.com	Yes	191	212.0	242
		awin1.com*	No	112	48.5	2,043	Awin	zenaps.com*	No	119	111.2	196
	Yandex	yandex.com	Yes	121	41.9	1,688		awin1.com*	No	118	110.9	196
	AdRoll	adroll.com	No	117	39.6	3,753	FullStory	fullstory.com	Yes	230	105.6	1,311
	Glassbox	glassboxdigital.io*	Yes	6	31.9	328	Listrak	listrakbi.com	Yes	226	66.0	1,403
	Listrak	listrakbi.com	Yes	91	24.9	2,219	LiveRamp	pippio.com	No	138	65.1	567
	Oracle	bronto.com	Yes	90	24.6	2,332	SmarterHQ	smarterhq.io*	Yes	32	63.8	556
	LiveRamp	rlcdn.com	No	11	20.0	567	Verizon Media	yahoo.com*	Yes	255	62.3	4,281
	SaleCycle	salecycle.com	Yes	35	17.5	2,577	AdRoll	adroll.com	No	122	48.6	2,343
	Automattic	gravatar.com*	Yes	38	16.7	2,048	Yandex	yandex.ru	Yes	141	48.1	1,648
	Facebook	facebook.com	Yes	21	14.8	1,153	Criteo SA	criteo.com*	No	134	46.0	1,403
	Salesforce	pardot.com*	Yes	36	30.8	2,675	Neustar	agkn.com*	No	133	45.9	1,403
	Oktopost	okt.to*	Yes	31	11.4	6,589	Oracle	addthis.com	No	133	45.9	1,403

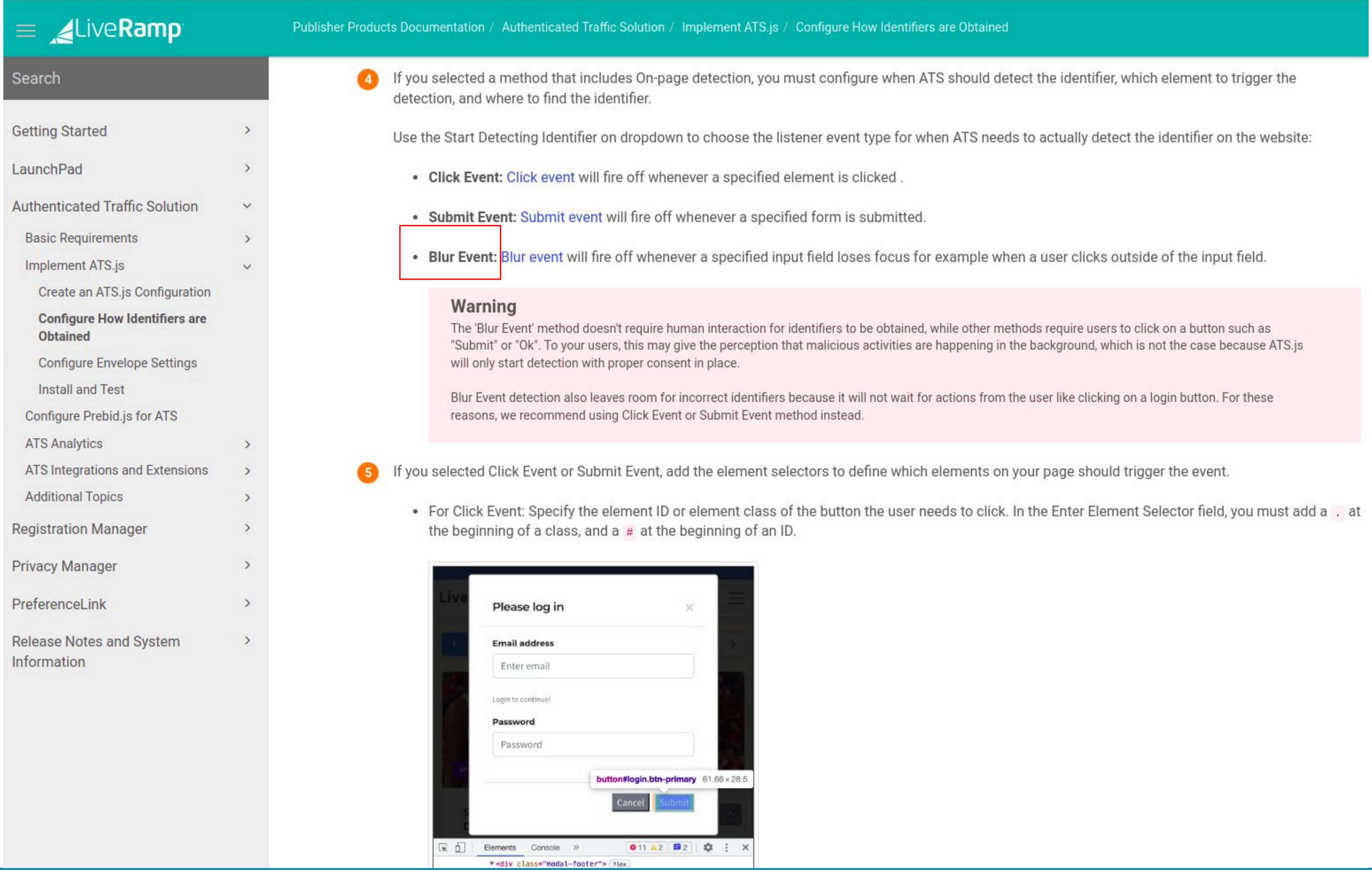

Taboola Help Center
What can we help you with?
Taboola.com
Logi
Home > ... > Lookalike Targeting
Taboola Ads
Getting Started
Create & Manage Great Campaigns
Create A New Campaign
Edit Campaigns
Campaign Targeting Options
Send your 1st Party Audiences via DMP or MMP

Lookalike Targeting

Look-alike models are used to increase scale by finding new people likely to be interested in your business because they resemble existing customers.

Use your CRM data to create lookalike audiences on Taboola! You can upload either a customer list of hashed email addresses, mobile device IDs, or 5 digit US zip codes and Taboola's predictive engine will find similar users that are more likely to convert based on the assumption that these users will be "like" your current customers in your database.

Visit our Advertiser Data Use Policy here.



LiveRamp

Publisher Products Documentation / Authenticated Traffic Solution / Implement ATS.js / Configure How Identifiers are Obtained

Search

- Getting Started
- LaunchPad
- Authenticated Traffic Solution
  - Basic Requirements
  - Implement ATS.js
    - Create an ATS.js Configuration
    - **Configure How Identifiers are Obtained**
    - Configure Envelope Settings
    - Install and Test
  - Configure Prebid.js for ATS
  - ATS Analytics
  - ATS Integrations and Extensions
  - Additional Topics
- Registration Manager
- Privacy Manager
- PreferenceLink
- Release Notes and System Information

4 If you selected a method that includes On-page detection, you must configure when ATS should detect the identifier, which element to trigger the detection, and where to find the identifier.

Use the Start Detecting Identifier on dropdown to choose the listener event type for when ATS needs to actually detect the identifier on the website:

- **Click Event:** Click event will fire off whenever a specified element is clicked .
- **Submit Event:** Submit event will fire off whenever a specified form is submitted.
- **Blur Event:** Blur event will fire off whenever a specified input field loses focus for example when a user clicks outside of the input field.

Warning

The 'Blur Event' method doesn't require human interaction for identifiers to be obtained, while other methods require users to click on a button such as "Submit" or "Ok". To your users, this may give the perception that malicious activities are happening in the background, which is not the case because ATS.js will only start detection with proper consent in place.

Blur Event detection also leaves room for incorrect identifiers because it will not wait for actions from the user like clicking on a login button. For these reasons, we recommend using Click Event or Submit Event method instead.

5 If you selected Click Event or Submit Event, add the element selectors to define which elements on your page should trigger the event.

- For Click Event: Specify the element ID or element class of the button the user needs to click. In the Enter Element Selector field, you must add a `.` at the beginning of a class, and a `#` at the beginning of an ID.

Please log in

Email address

Enter email

Login to continue!

Password

Password

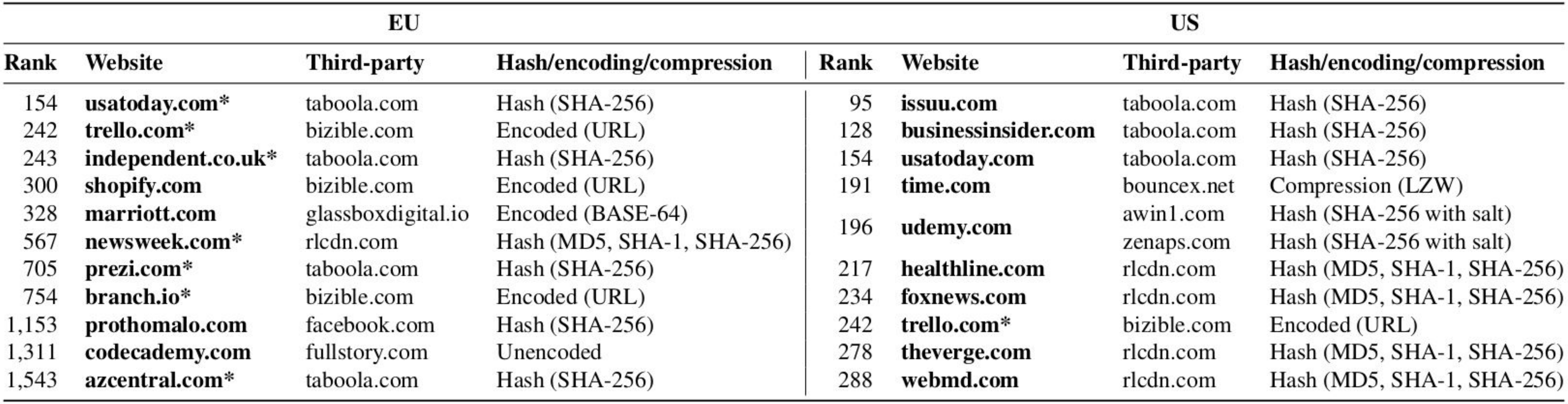
button#login.btn-primary 61.66 × 28.5

Cancel Submit

Elements Console

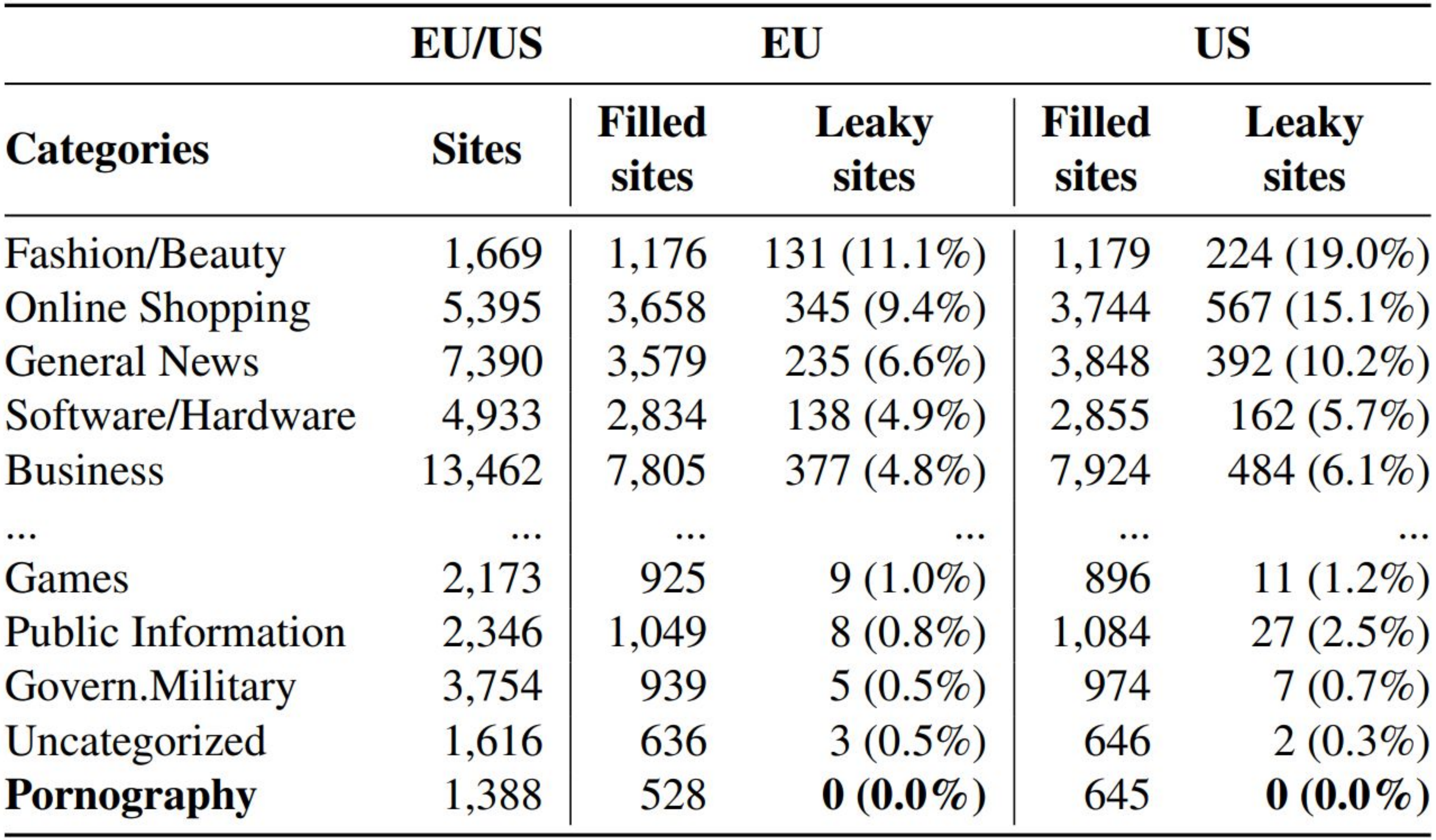
```
▾<div class="modal-footer"> flex
```

Results - Top ten websites



		EU				US	
Rank	**Website**	**Third-party**	**Hash/encoding/compression**	**Rank**	**Website**	**Third-party**	**Hash/encoding/compression**
154	**usatoday.com***	taboola.com	Hash (SHA-256)	95	**issuu.com**	taboola.com	Hash (SHA-256)
242	**trello.com***	bizible.com	Encoded (URL)	128	**businessinsider.com**	taboola.com	Hash (SHA-256)
243	**independent.co.uk***	taboola.com	Hash (SHA-256)	154	**usatoday.com**	taboola.com	Hash (SHA-256)
300	**shopify.com**	bizible.com	Encoded (URL)	191	**time.com**	bouncex.net	Compression (LZW)
328	**marriott.com**	glassboxdigital.io	Encoded (BASE-64)	196	**udemy.com**	awin1.com	Hash (SHA-256 with salt)
567	**newsweek.com***	rlcdn.com	Hash (MD5, SHA-1, SHA-256)			zenaps.com	Hash (SHA-256 with salt)
705	**prezi.com***	taboola.com	Hash (SHA-256)	217	**healthline.com**	rlcdn.com	Hash (MD5, SHA-1, SHA-256)
754	**branch.io***	bizible.com	Encoded (URL)	234	**foxnews.com**	rlcdn.com	Hash (MD5, SHA-1, SHA-256)
1,153	**prothomalo.com**	facebook.com	Hash (SHA-256)	242	**trello.com***	bizible.com	Encoded (URL)
1,311	**codecademy.com**	fullstory.com	Unencoded	278	**theverge.com**	rlcdn.com	Hash (MD5, SHA-1, SHA-256)
1,543	**azcentral.com***	taboola.com	Hash (SHA-256)	288	**webmd.com**	rlcdn.com	Hash (MD5, SHA-1, SHA-256)

Results - Website Categories



	EU/US	EU		US	
Categories	**Sites**	**Filled sites**	**Leaky sites**	**Filled sites**	**Leaky sites**
Fashion/Beauty	1,669	1,176	131 (11.1%)	1,179	224 (19.0%)
Online Shopping	5,395	3,658	345 (9.4%)	3,744	567 (15.1%)
General News	7,390	3,579	235 (6.6%)	3,848	392 (10.2%)
Software/Hardware	4,933	2,834	138 (4.9%)	2,855	162 (5.7%)
Business	13,462	7,805	377 (4.8%)	7,924	484 (6.1%)
...	...	...	...	...	...
Games	2,173	925	9 (1.0%)	896	11 (1.2%)
Public Information	2,346	1,049	8 (0.8%)	1,084	27 (2.5%)
Govern.Military	3,754	939	5 (0.5%)	974	7 (0.7%)
Uncategorized	1,616	636	3 (0.5%)	646	2 (0.3%)
Pornography	1,388	528	**0 (0.0%)**	645	**0 (0.0%)**

Results - EU vs US

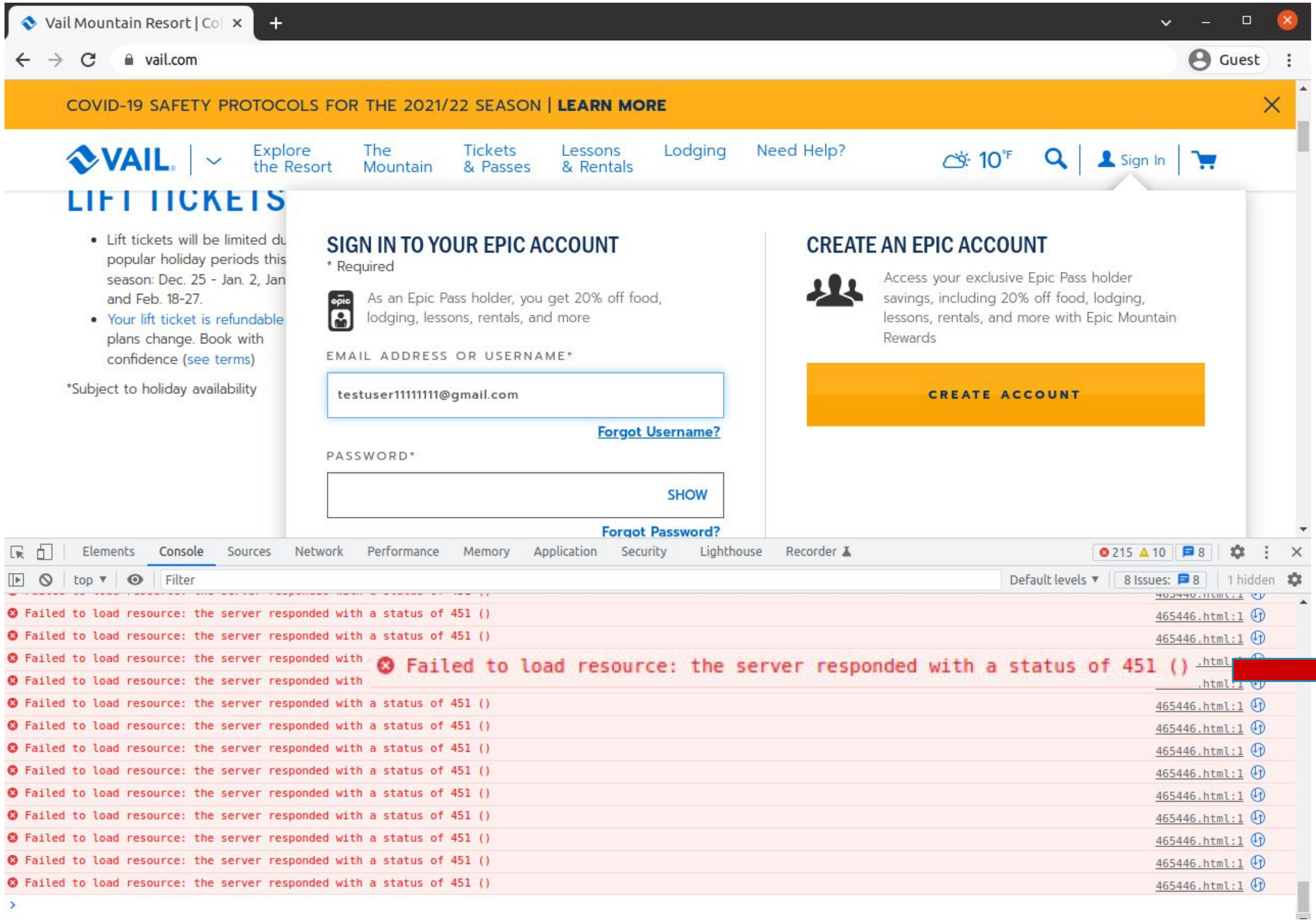
	EU	US
Visited websites	99,380	99,437
Websites where we filed	52,055	53,038
Emails sent to 1st party	4,395	5,518
Emails sent to 3rd party	**2,633**	**3,790**
Emails sent to trackers	**1,844**	**2,950**

60% difference

addthis.com, yahoo.com, doubleclick.net and criteo.com

Only appear in the US crawl

Results - EU vs US



COVID-19 SAFETY PROTOCOLS FOR THE 2021/22 SEASON | **LEARN MORE**

VAIL | Explore the Resort | The Mountain | Tickets & Passes | Lessons & Rentals | Lodging | Need Help? | 10°F | Sign In

LIFT TICKETS

- Lift tickets will be limited du popular holiday periods this season: Dec. 25 - Jan. 2, Jan and Feb. 18-27.
- Your lift ticket is refundable plans change. Book with confidence (see terms)

*Subject to holiday availability

SIGN IN TO YOUR EPIC ACCOUNT

* Required

As an Epic Pass holder, you get 20% off food, lodging, lessons, rentals, and more

EMAIL ADDRESS OR USERNAME*

testuser11111111@gmail.com

Forgot Username?

PASSWORD*

SHOW

Forgot Password?

CREATE AN EPIC ACCOUNT

Access your exclusive Epic Pass holder savings, including 20% off food, lodging, lessons, rentals, and more with Epic Mountain Rewards

CREATE ACCOUNT

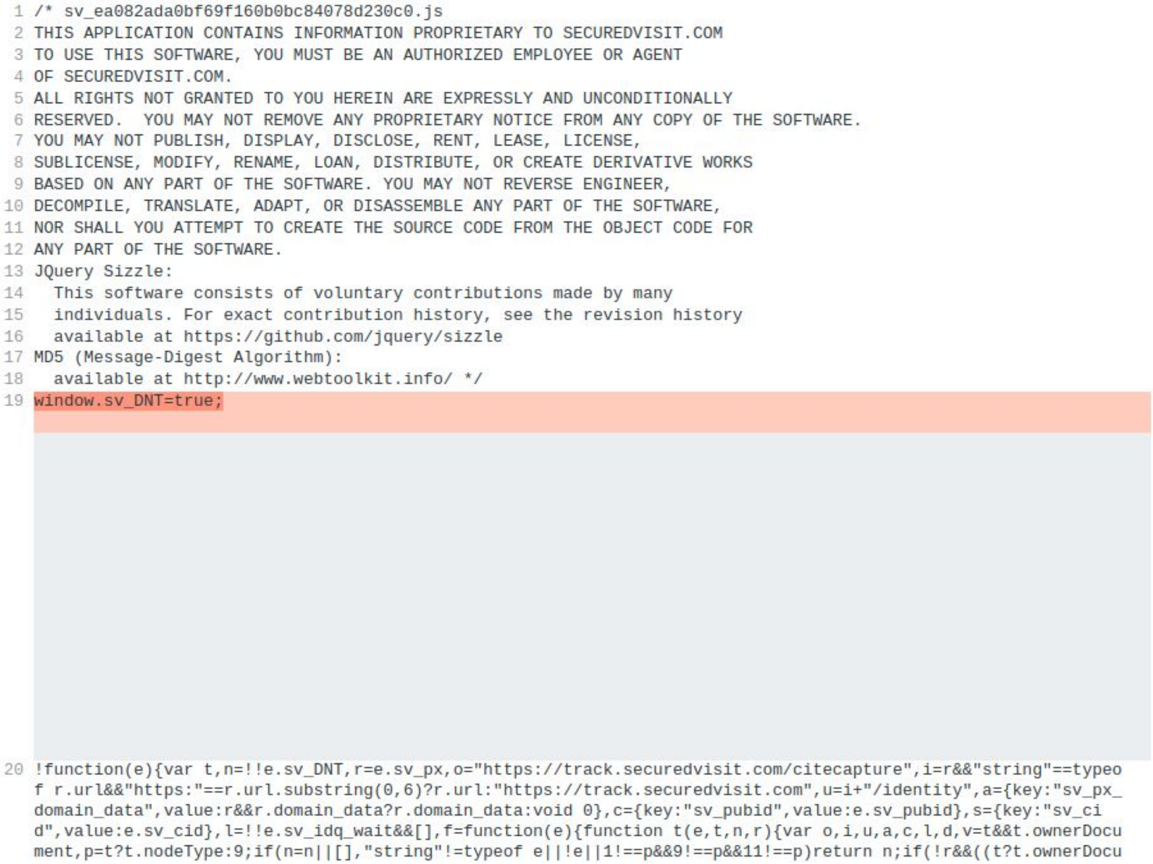
```
Failed to load resource: the server responded with a status of 451 ()    465446.html:1
Failed to load resource: the server responded with a status of 451 ()    465446.html:1
Failed to load resource: the server responded with                         .html:1
Failed to load resource: the server responded with                         .html:1
Failed to load resource: the server responded with a status of 451 ()    465446.html:1
Failed to load resource: the server responded with a status of 451 ()    465446.html:1
Failed to load resource: the server responded with a status of 451 ()    465446.html:1
Failed to load resource: the server responded with a status of 451 ()    465446.html:1
Failed to load resource: the server responded with a status of 451 ()    465446.html:1
Failed to load resource: the server responded with a status of 451 ()    465446.html:1
Failed to load resource: the server responded with a status of 451 ()    465446.html:1
Failed to load resource: the server responded with a status of 451 ()    465446.html:1
Failed to load resource: the server responded with a status of 451 ()    465446.html:1
```

```
Failed to load resource: the server responded with a status of 451 ()
```

rlcdn.com sends HTTP 451 error: Unavailable For Legal Reasons

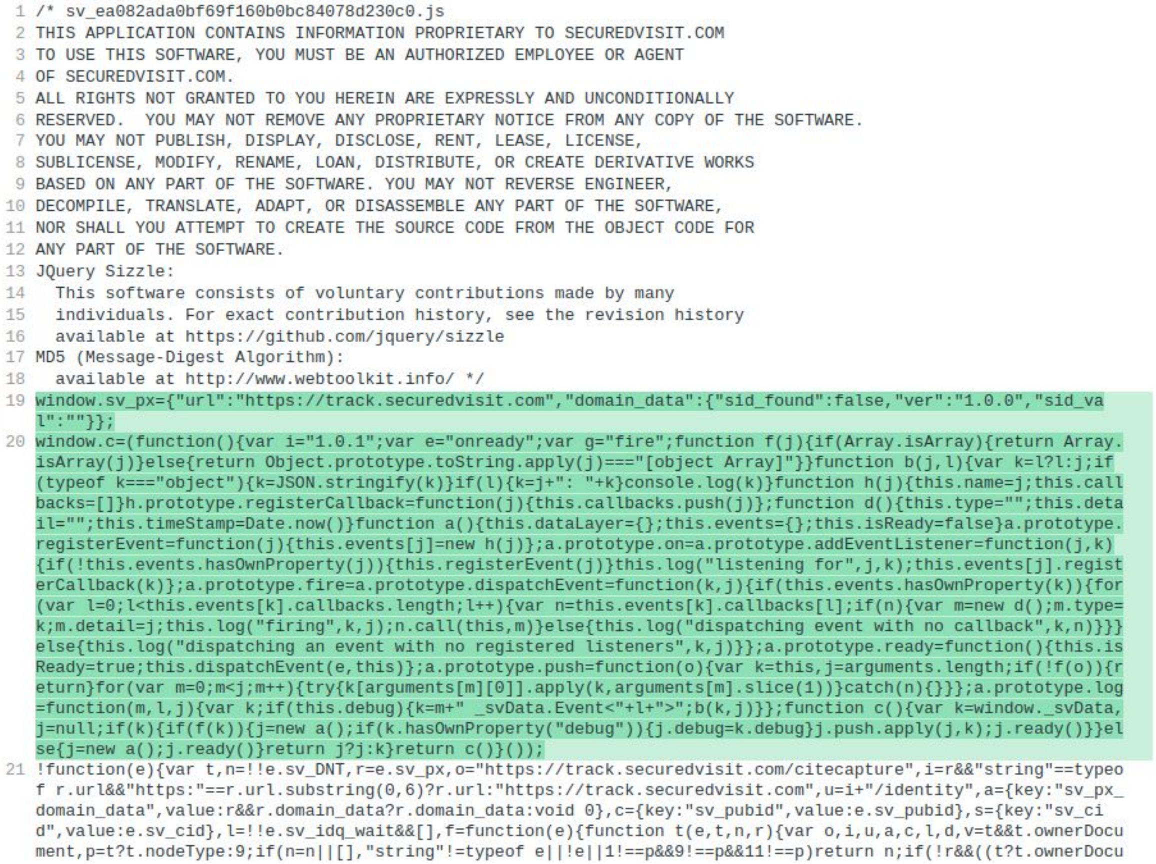
Results - EU vs US

Same script (from securedvisit.com) served with different content



```
/* sv_ea082ada0bf69f160b0bc84078d230c0.js
THIS APPLICATION CONTAINS INFORMATION PROPRIETARY TO SECUREDVISIT.COM
TO USE THIS SOFTWARE, YOU MUST BE AN AUTHORIZED EMPLOYEE OR AGENT
OF SECUREDVISIT.COM.
ALL RIGHTS NOT GRANTED TO YOU HEREIN ARE EXPRESSLY AND UNCONDITIONALLY
RESERVED.  YOU MAY NOT REMOVE ANY PROPRIETARY NOTICE FROM ANY COPY OF THE SOFTWARE.
YOU MAY NOT PUBLISH, DISPLAY, DISCLOSE, RENT, LEASE, LICENSE,
SUBLICENSE, MODIFY, RENAME, LOAN, DISTRIBUTE, OR CREATE DERIVATIVE WORKS
BASED ON ANY PART OF THE SOFTWARE. YOU MAY NOT REVERSE ENGINEER,
DECOMPILE, TRANSLATE, ADAPT, OR DISASSEMBLE ANY PART OF THE SOFTWARE,
NOR SHALL YOU ATTEMPT TO CREATE THE SOURCE CODE FROM THE OBJECT CODE FOR
ANY PART OF THE SOFTWARE.
JQuery Sizzle:
  This software consists of voluntary contributions made by many
  individuals. For exact contribution history, see the revision history
  available at https://github.com/jquery/sizzle
MD5 (Message-Digest Algorithm):
  available at http://www.webtoolkit.info/ */
window.sv_DNT=true;
!function(e){var t,n=!!e.sv_DNT,r=e.sv_px,o="https://track.securedvisit.com/citecapture",i=r&&"string"==typeo
f r.url&&"https:"==r.url.substring(0,6)?r.url:"https://track.securedvisit.com",u=i+"/identity",a={key:"sv_px_
domain_data",value:r&&r.domain_data?r.domain_data:void 0},c={key:"sv_pubid",value:e.sv_pubid},s={key:"sv_ci
d",value:e.sv_cid},l=!!e.sv_idq_wait&&[],f=function(e){function t(e,t,n,r){var o,i,u,a,c,l,d,v=t&&t.ownerDocu
ment,p=t?t.nodeType:9;if(n=n||[],"string"!=typeof e||!e||1!==p&&9!==p&&11!==p)return n;if(!r&&((t?t.ownerDocu
```

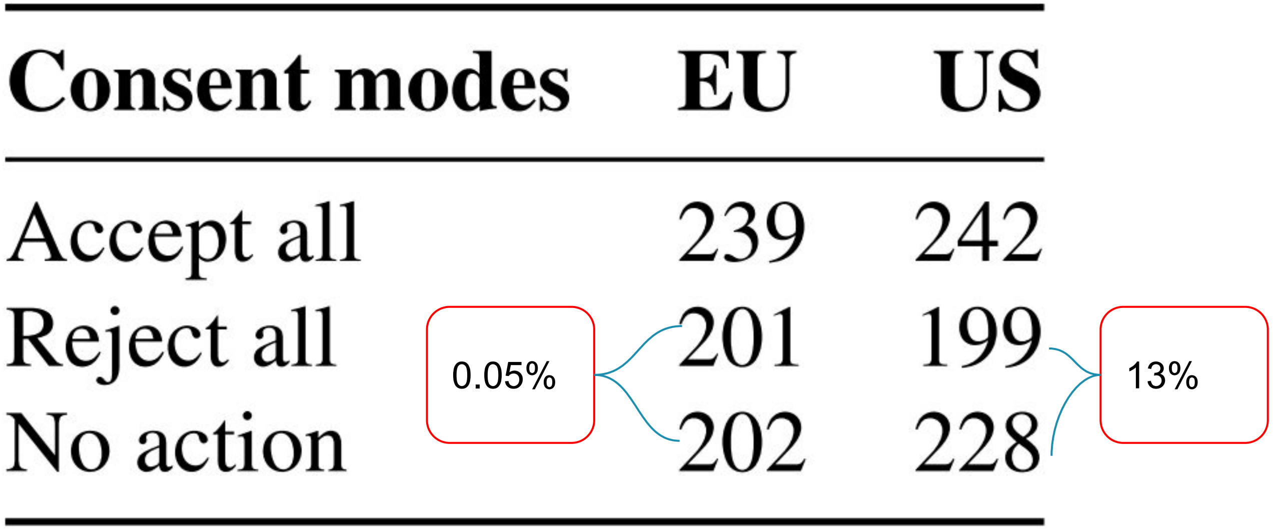
in the EU



```
/* sv_ea082ada0bf69f160b0bc84078d230c0.js
THIS APPLICATION CONTAINS INFORMATION PROPRIETARY TO SECUREDVISIT.COM
TO USE THIS SOFTWARE, YOU MUST BE AN AUTHORIZED EMPLOYEE OR AGENT
OF SECUREDVISIT.COM.
ALL RIGHTS NOT GRANTED TO YOU HEREIN ARE EXPRESSLY AND UNCONDITIONALLY
RESERVED.  YOU MAY NOT REMOVE ANY PROPRIETARY NOTICE FROM ANY COPY OF THE SOFTWARE.
YOU MAY NOT PUBLISH, DISPLAY, DISCLOSE, RENT, LEASE, LICENSE,
SUBLICENSE, MODIFY, RENAME, LOAN, DISTRIBUTE, OR CREATE DERIVATIVE WORKS
BASED ON ANY PART OF THE SOFTWARE. YOU MAY NOT REVERSE ENGINEER,
DECOMPILE, TRANSLATE, ADAPT, OR DISASSEMBLE ANY PART OF THE SOFTWARE,
NOR SHALL YOU ATTEMPT TO CREATE THE SOURCE CODE FROM THE OBJECT CODE FOR
ANY PART OF THE SOFTWARE.
JQuery Sizzle:
  This software consists of voluntary contributions made by many
  individuals. For exact contribution history, see the revision history
  available at https://github.com/jquery/sizzle
MD5 (Message-Digest Algorithm):
  available at http://www.webtoolkit.info/ */
window.sv_px={"url":"https://track.securedvisit.com","domain_data":{"sid_found":false,"ver":"1.0.0","sid_va
l":""}};
window.c=(function(){var i="1.0.1";var e="onready";var g="fire";function f(j){if(Array.isArray){return Array.
isArray(j)}else{return Object.prototype.toString.apply(j)==="[object Array]"}}function b(j,l){var k=l?l:j;if
(typeof k==="object"){k=JSON.stringify(k)}if(l){k=j+": "+k}console.log(k)}function h(j){this.name=j;this.call
backs=[]}h.prototype.registerCallback=function(j){this.callbacks.push(j)};function d(){this.type="";this.deta
il="";this.timeStamp=Date.now()}function a(){this.dataLayer={};this.events={};this.isReady=false}a.prototype.
registerEvent=function(j){this.events[j]=new h(j)};a.prototype.on=a.prototype.addEventListener=function(j,k)
{if(!this.events.hasOwnProperty(j)){this.registerEvent(j)}this.log("listening for",j,k);this.events[j].regist
erCallback(k)};a.prototype.fire=a.prototype.dispatchEvent=function(k,j){if(this.events.hasOwnProperty(k)){for
(var l=0;l<this.events[k].callbacks.length;l++){var n=this.events[k].callbacks[l];if(n){var m=new d();m.type=
k;m.detail=j;this.log("firing",k,j);n.call(this,m)}else{this.log("dispatching event with no callback",k,n)}}}
else{this.log("dispatching an event with no registered listeners",k,j)}};a.prototype.ready=function(){this.is
Ready=true;this.dispatchEvent(e,this)};a.prototype.push=function(o){var k=this,j=arguments.length;if(!f(o)){r
eturn}for(var m=0;m<j;m++){try{k[arguments[m][0]].apply(k,arguments[m].slice(1))}catch(n){}}};a.prototype.log
=function(m,l,j){var k;if(this.debug){k=m+" _svData.Event<"+l+">";b(k,j)}};function c(){var k=window._svData,
j=null;if(k){if(f(k)){j=new a();if(k.hasOwnProperty("debug")){j.debug=k.debug}j.push.apply(j,k);j.ready()}}el
se{j=new a();j.ready()}return j?j:k}return c()}());
!function(e){var t,n=!!e.sv_DNT,r=e.sv_px,o="https://track.securedvisit.com/citecapture",i=r&&"string"==typeo
f r.url&&"https:"==r.url.substring(0,6)?r.url:"https://track.securedvisit.com",u=i+"/identity",a={key:"sv_px_
domain_data",value:r&&r.domain_data?r.domain_data:void 0},c={key:"sv_pubid",value:e.sv_pubid},s={key:"sv_ci
d",value:e.sv_cid},l=!!e.sv_idq_wait&&[],f=function(e){function t(e,t,n,r){var o,i,u,a,c,l,d,v=t&&t.ownerDocu
ment,p=t?t.nodeType:9;if(n=n||[],"string"!=typeof e||!e||1!==p&&9!==p&&11!==p)return n;if(!r&&((t?t.ownerDocu
```

in the US

Results - The Effect of Consent

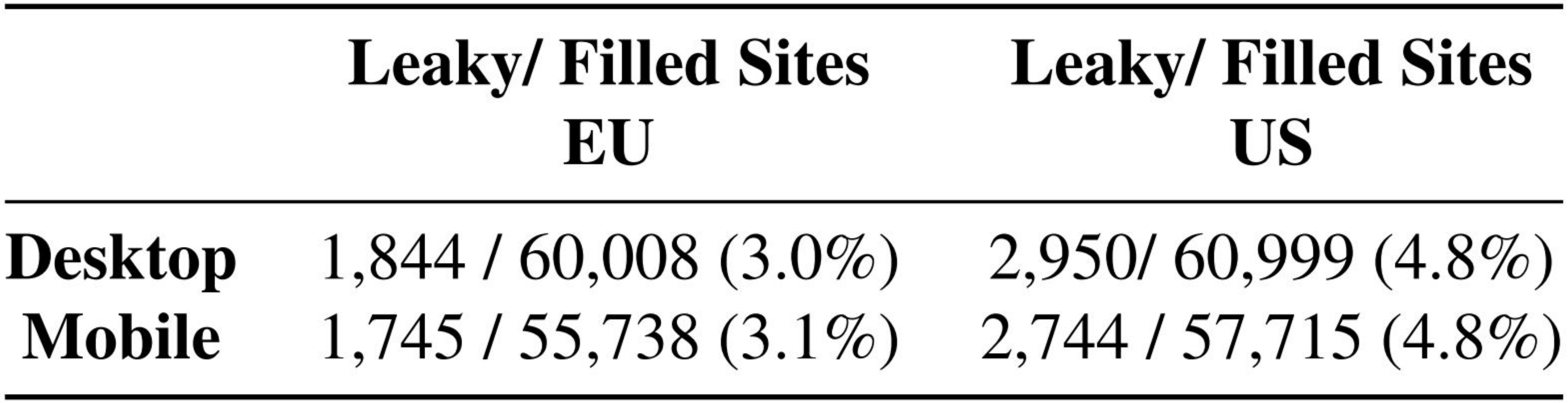


Consent modes	EU	US
Accept all	239	242
Reject all	201	199
No action	202	228

0.05%

13%

Results - Mobile

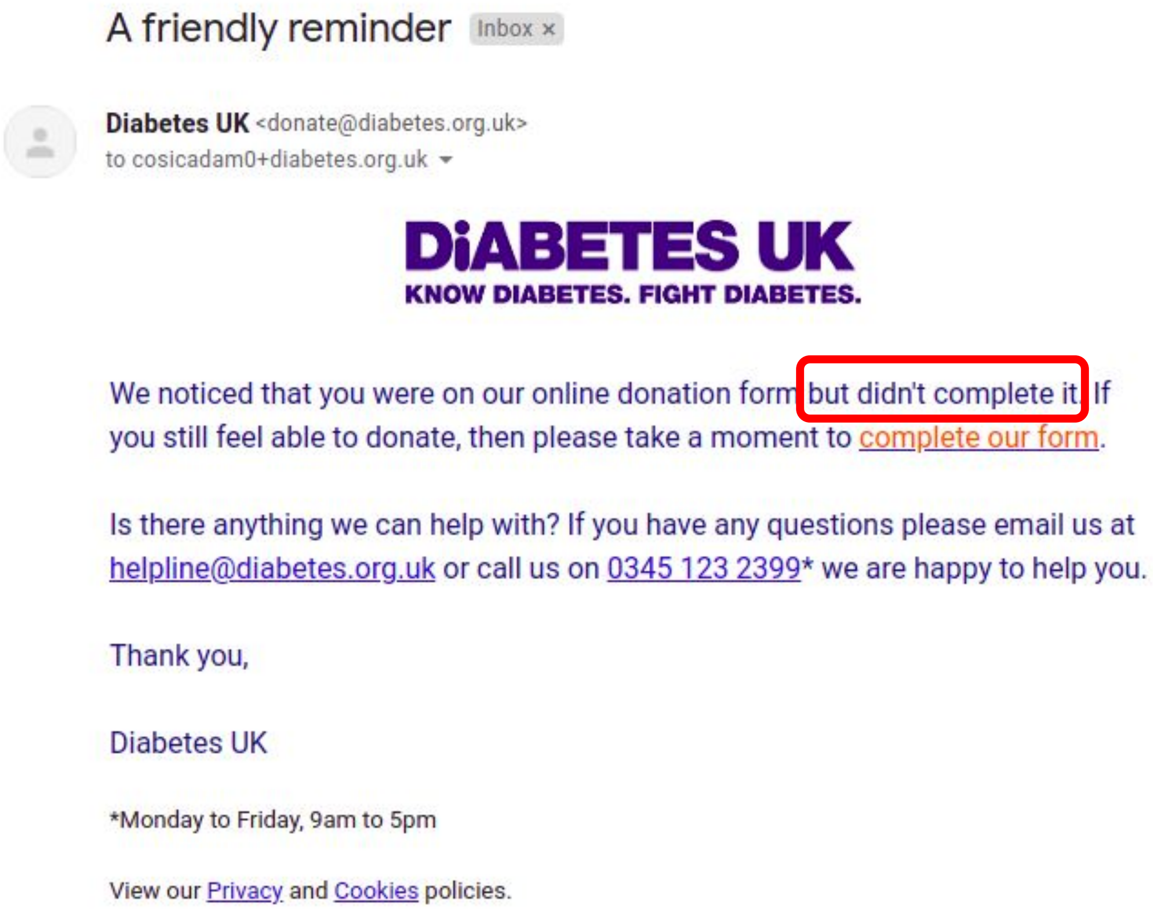


	Leaky/ Filled Sites	Leaky/ Filled Sites
	EU	US
Desktop	1,844 / 60,008 (3.0%)	2,950/ 60,999 (4.8%)
Mobile	1,745 / 55,738 (3.1%)	2,744 / 57,715 (4.8%)

Results - Received Emails

- 290 emails from 88 distinct sites

Email from: diabetes.org.uk
Tracker domain: freshaddress.biz



A friendly reminder Inbox ×

Diabetes UK <donate@diabetes.org.uk>
to cosicadam0+diabetes.org.uk

We noticed that you were on our online donation form but didn't complete it. If you still feel able to donate, then please take a moment to complete our form.

Is there anything we can help with? If you have any questions please email us at helpline@diabetes.org.uk or call us on 0345 123 2399* we are happy to help you.

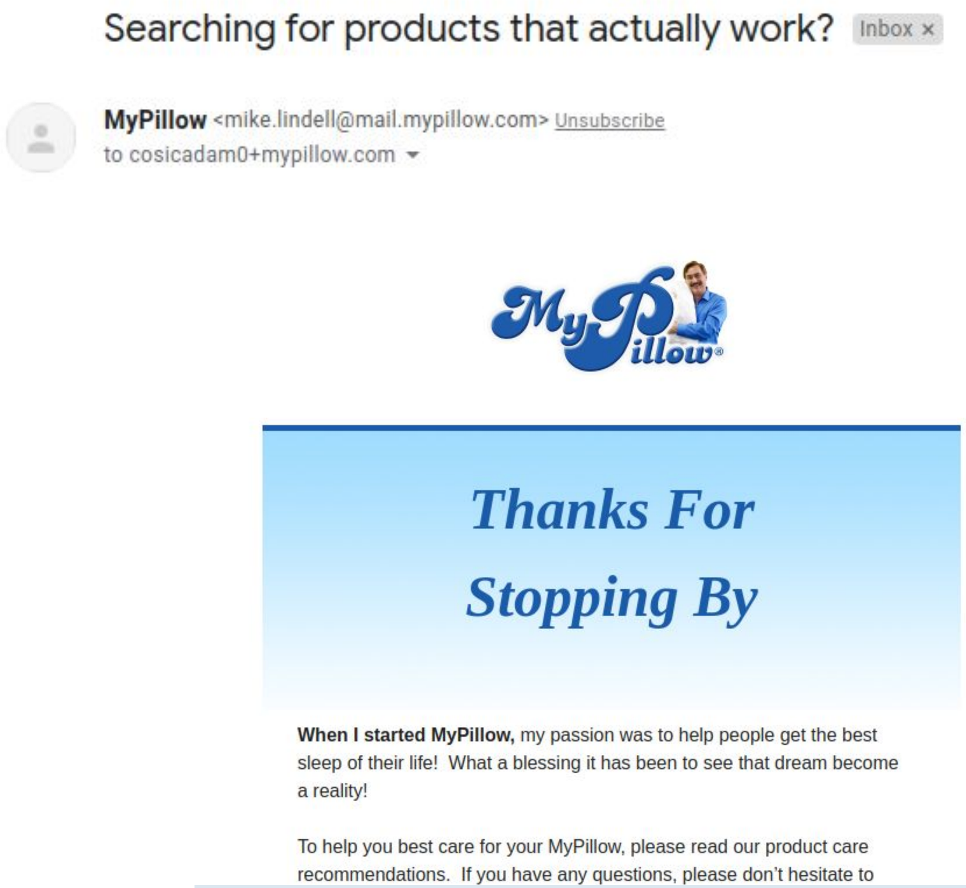
Thank you,

Diabetes UK

*Monday to Friday, 9am to 5pm

View our Privacy and Cookies policies.

Results - Received Emails



Searching for products that actually work? Inbox ×

MyPillow <mike.lindell@mail.mypillow.com> Unsubscribe
to cosicadam0+mypillow.com

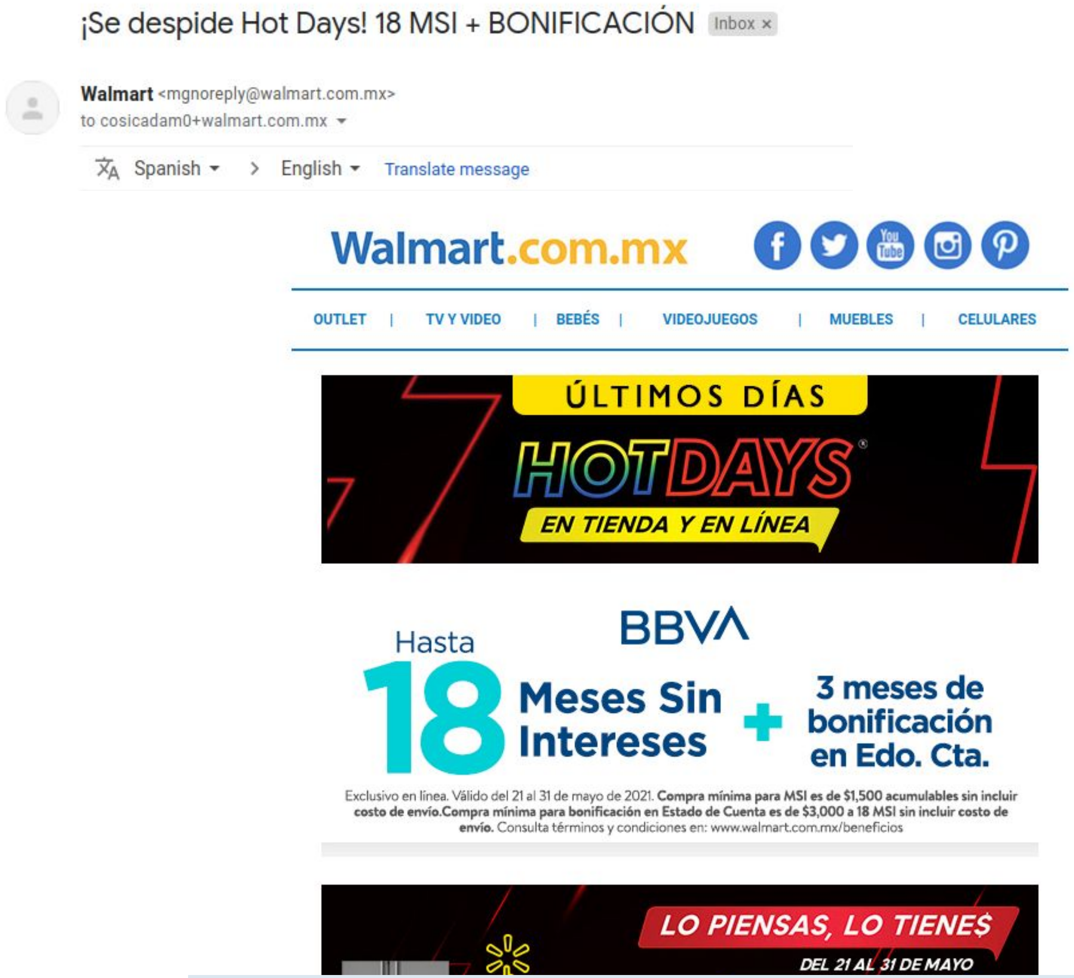
MyPillow

Thanks For Stopping By

When I started MyPillow, my passion was to help people get the best sleep of their life! What a blessing it has been to see that dream become a reality!

To help you best care for your MyPillow, please read our product care recommendations. If you have any questions, please don't hesitate to

Email from: mypillow.com
Tracker domain: listrakbi.com



¡Se despide Hot Days! 18 MSI + BONIFICACIÓN Inbox ×

Walmart <mgnoreply@walmart.com.mx>
to cosicadam0+walmart.com.mx

Spanish > English Translate message

Walmart.com.mx

OUTLET | TV Y VIDEO | BEBÉS | VIDEOJUEGOS | MUEBLES | CELULARES

ÚLTIMOS DÍAS
HOTDAYS
EN TIENDA Y EN LÍNEA

Hasta 18 Meses Sin Intereses + 3 meses de bonificación en Edo. Cta.
BBVA

Exclusivo en línea. Válido del 21 al 31 de mayo de 2021. **Compra mínima para MSI es de $1,500 acumulables sin incluir costo de envío.Compra mínima para bonificación en Estado de Cuenta es de $3,000 a 18 MSI sin incluir costo de envío.** Consulta términos y condiciones en: www.walmart.com.mx/beneficios

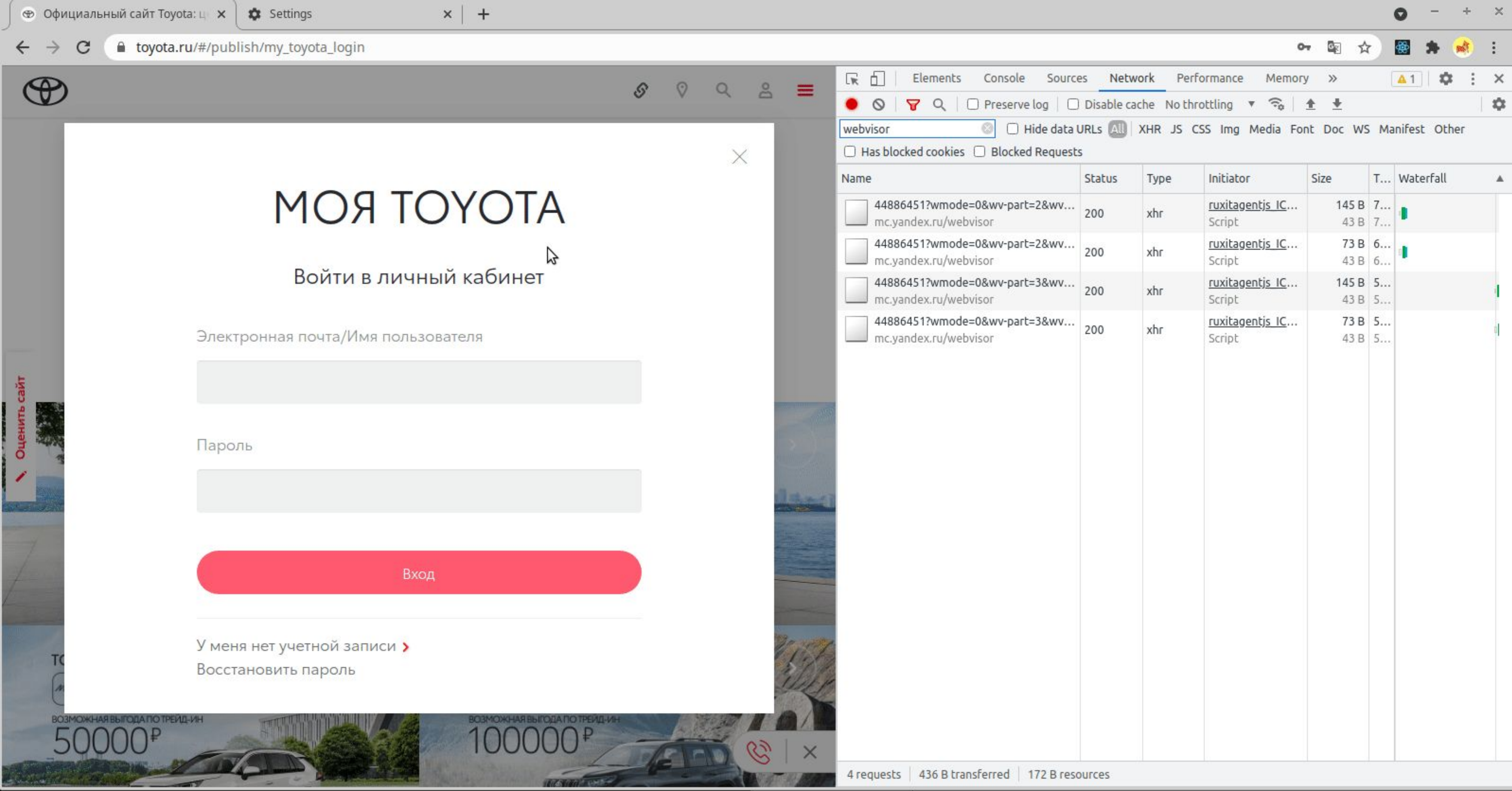
LO PIENSAS, LO TIENE$
DEL 21 AL 31 DE MAYO

Email from: walmart.com.mx
Tracker domain: veinteractive.com

Results - Password Leaks on 52 websites

Incidental collection by

- Yandex Metrica: due to React framework (50 websites)
- Mixpanel: due to outdated SDK usage (1 website)
- LogRocket: No response (1 website)



☐ Preserve log ☐ Disable cache No throttling

webvisor ☐ Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other

☐ Has blocked cookies ☐ Blocked Requests

Name	Status	Type	Initiator	Size	T...	Waterfall
44886451?wmode=0&wv-part=2&wv... mc.yandex.ru/webvisor	200	xhr	ruxitagentjs_IC... Script	145 B 43 B	7... 7...	
44886451?wmode=0&wv-part=2&wv... mc.yandex.ru/webvisor	200	xhr	ruxitagentjs_IC... Script	73 B 43 B	6... 6...	
44886451?wmode=0&wv-part=3&wv... mc.yandex.ru/webvisor	200	xhr	ruxitagentjs_IC... Script	145 B 43 B	5... 5...	
44886451?wmode=0&wv-part=3&wv... mc.yandex.ru/webvisor	200	xhr	ruxitagentjs_IC... Script	73 B 43 B	5... 5...	

4 requests | 436 B transferred | 172 B resources

МОЯ TOYOTA

Войти в личный кабинет

Электронная почта/Имя пользователя

Пароль

Вход

У меня нет учетной записи ›

Восстановить пароль

GDPR Requests

First parties: 30/58 replied

- Were not aware & removed
  - fivethirtyeight.com (via Walt Disney’s DPO)
  - trello.com (Atlassian)
- Marriott: Glassbox is used for **customer care, technical support, and fraud prevention**

Third parties: 15/28 replied

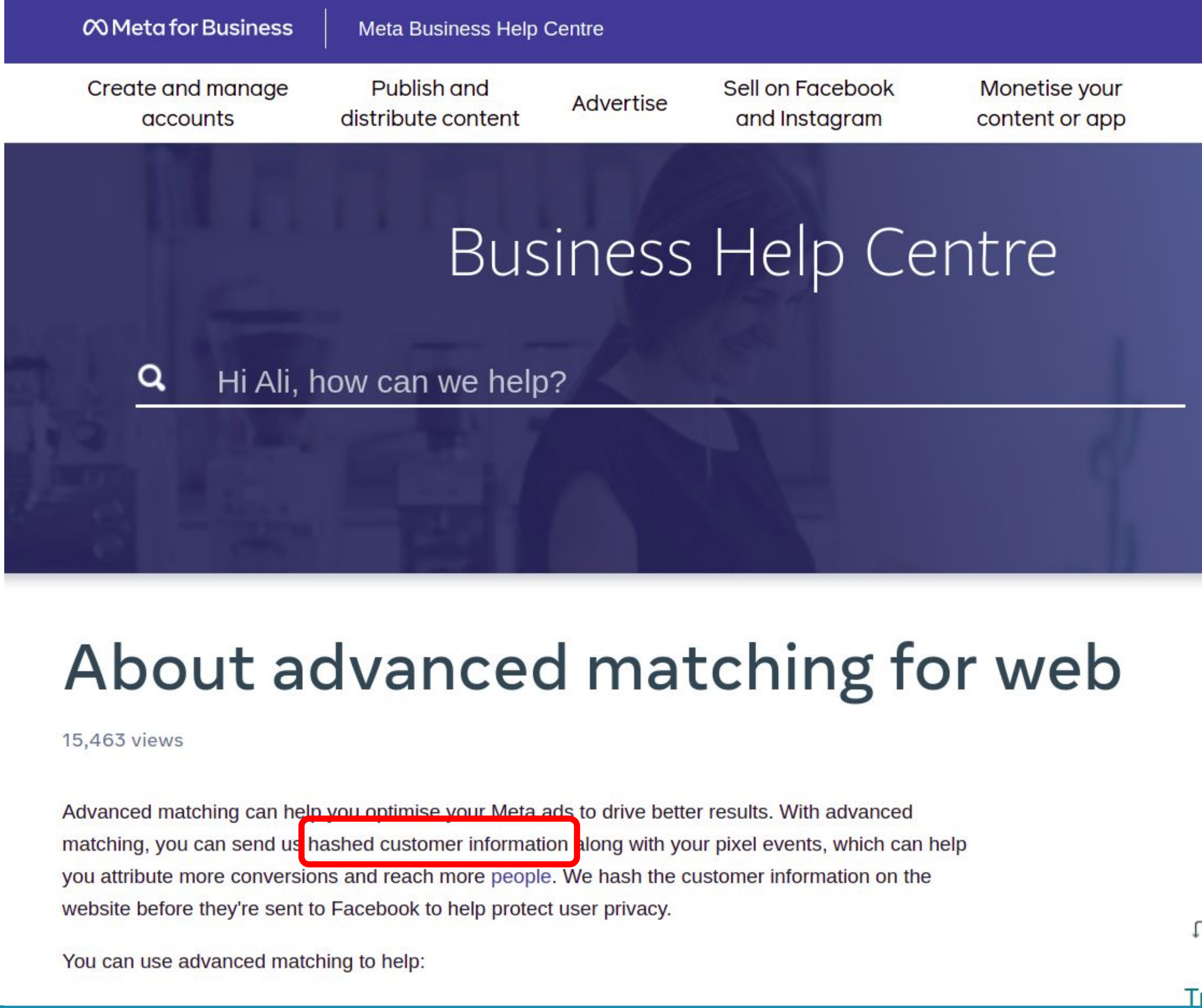
- Adobe and Yandex: Referred to corresponding first parties
- Taboola: ad & content personalization, CMP misconfiguration

0/33 first parties replied
(Websites in the US crawl)

- No response from these 33 websites.

Leaks to Facebook & TikTok

- Due to Automatic Advanced Matching feature of Facebook/Tiktok Pixel (scrapes forms)


Meta for Business
Meta Business Help Centre
Create and manage accounts
Publish and distribute content
Advertise
Sell on Facebook and Instagram
Monetise your content or app
Business Help Centre
Hi Ali, how can we help?

About advanced matching for web

15,463 views

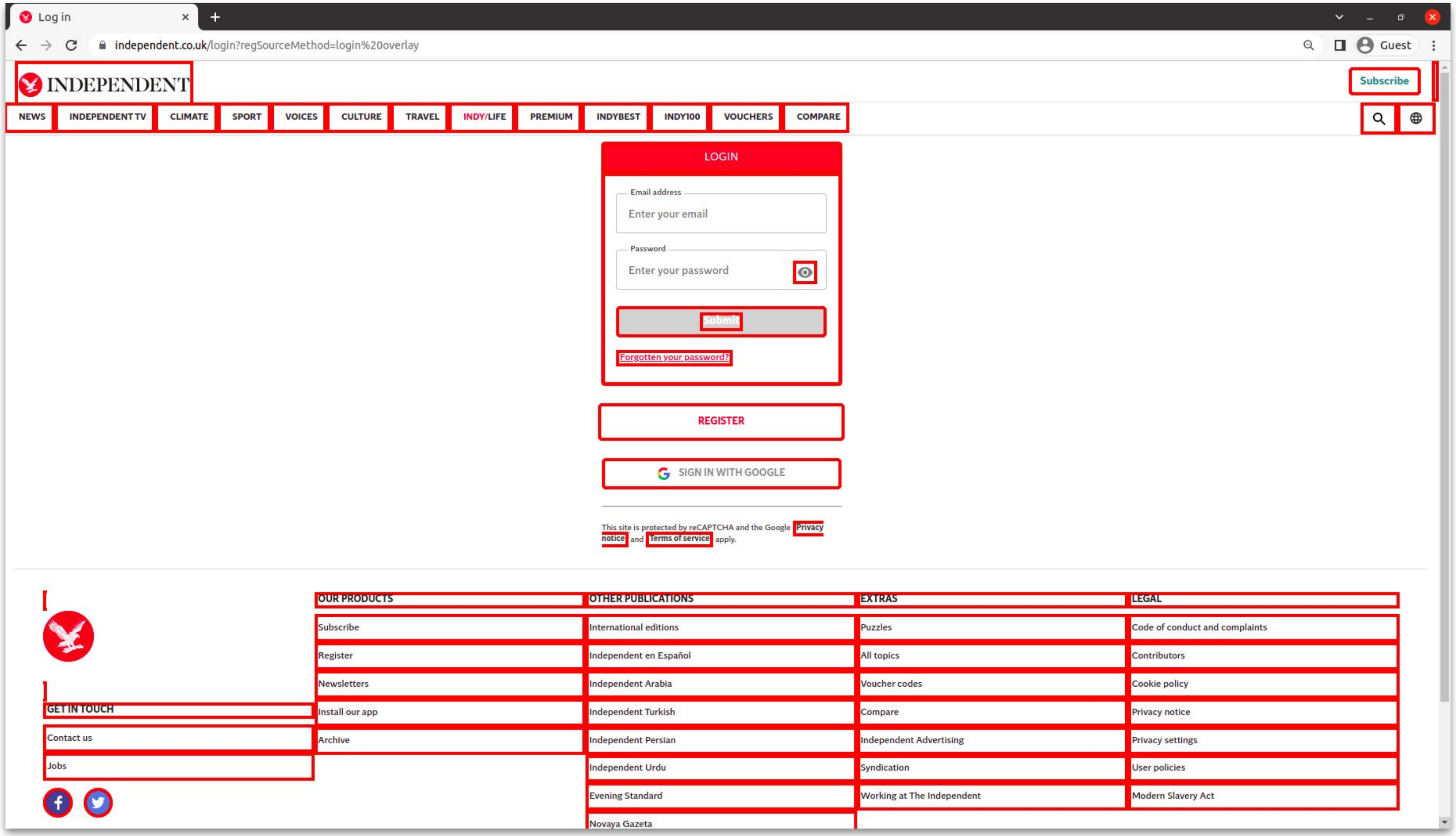
Advanced matching can help you optimise your Meta ads to drive better results. With advanced matching, you can send us hashed customer information along with your pixel events, which can help you attribute more conversions and reach more people. We hash the customer information on the website before they're sent to Facebook to help protect user privacy.

You can use advanced matching to help:

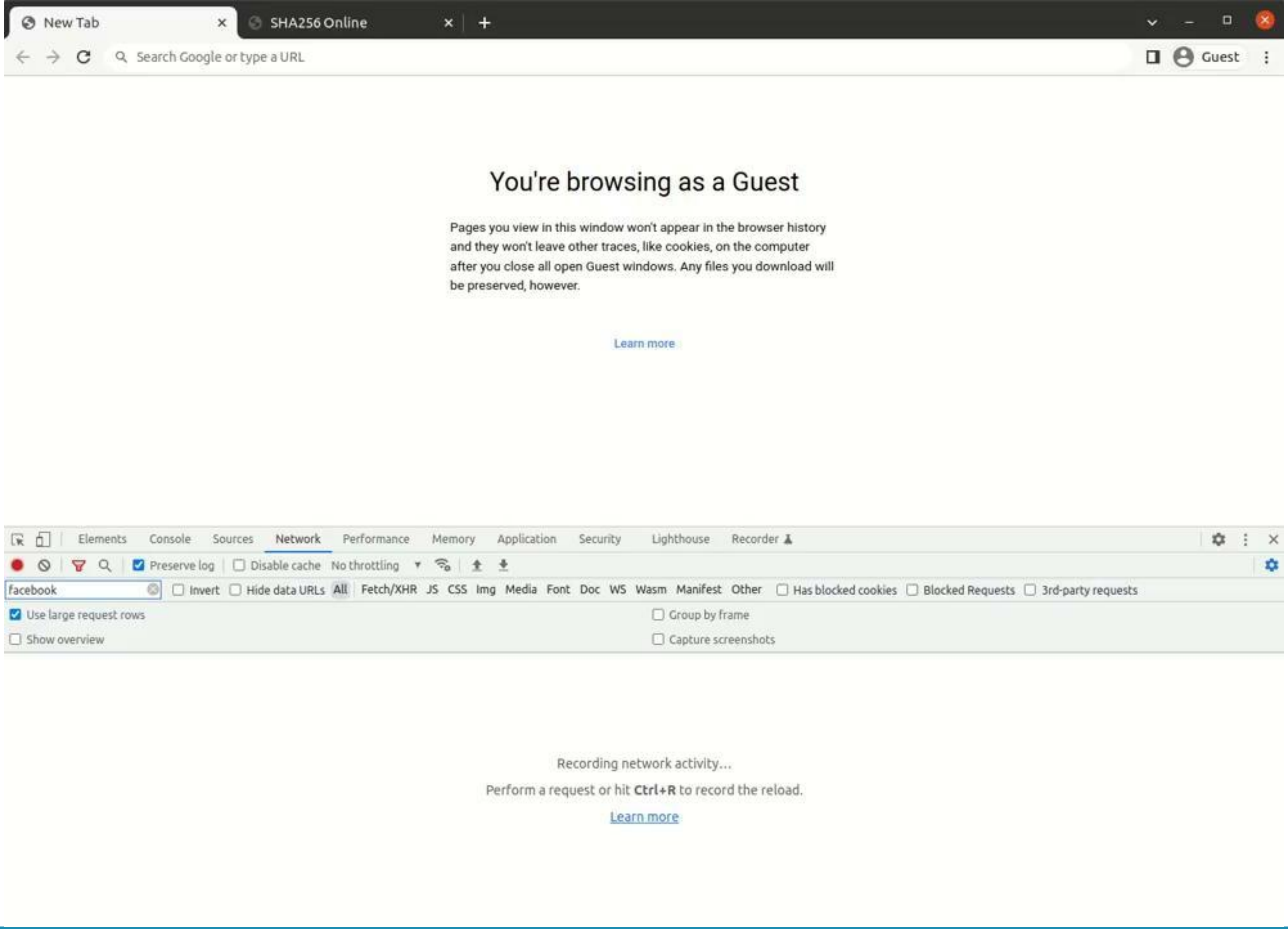
Leaks to Facebook & TikTok

- Triggered when the user clicks any link (Facebook) or button on the page.

	EU	US
Facebook	7,379	8,438
TikTok	147	154



This site is protected by reCAPTCHA and the Google Privacy notice and Terms of service apply.



You're browsing as a Guest

Pages you view in this window won't appear in the browser history and they won't leave other traces, like cookies, on the computer after you close all open Guest windows. Any files you download will be preserved, however.

Learn more

☑ Preserve log ☐ Disable cache No throttling

facebook ☐ Invert ☐ Hide data URLs ☐ Has blocked cookies ☐ Blocked Requests ☐ 3rd-party requests

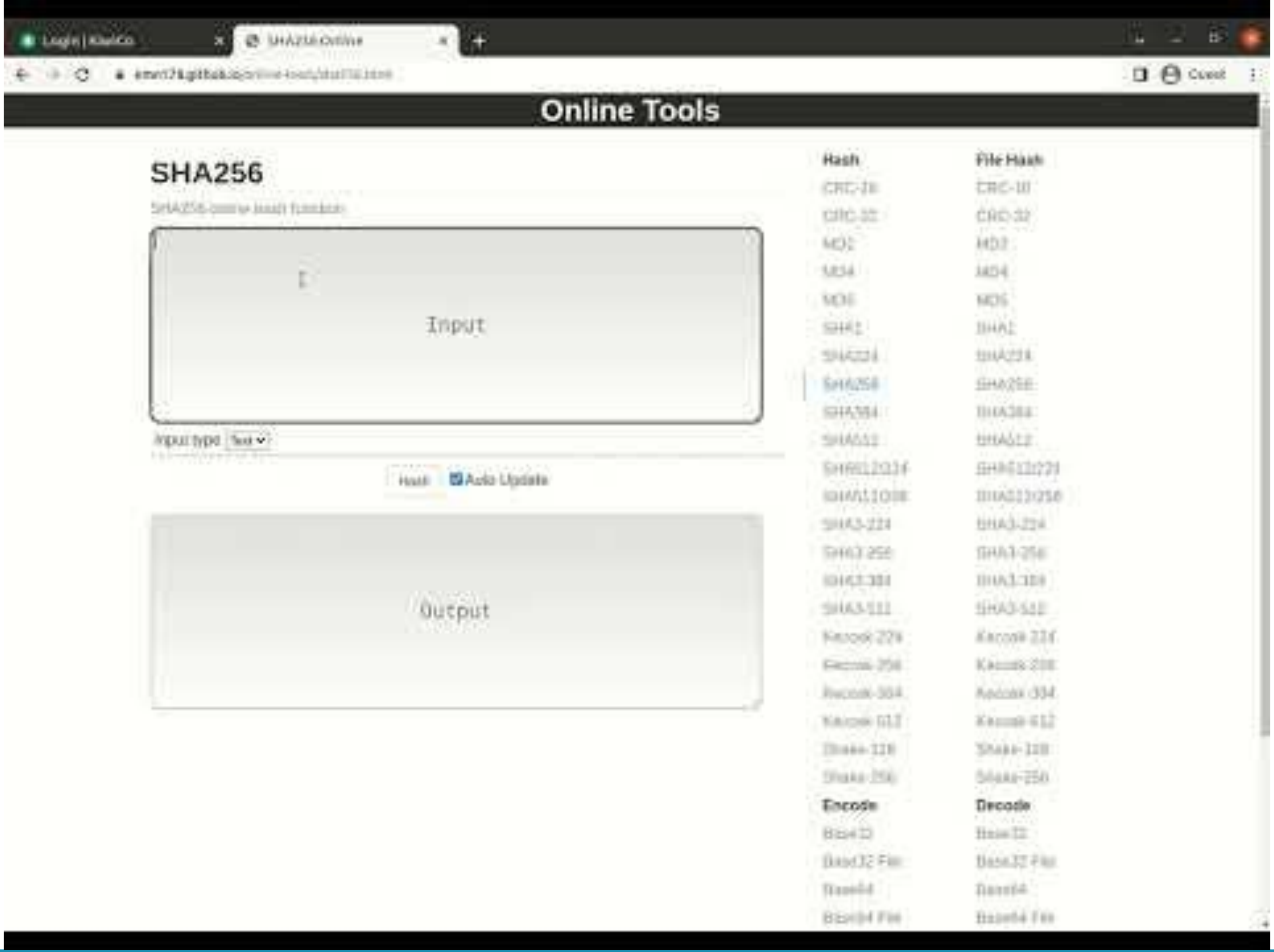
☑ Use large request rows ☐ Group by frame

☐ Show overview ☐ Capture screenshots

Recording network activity…

Perform a request or hit **Ctrl+R** to record the reload.

Learn more



SHA256

SHA256 online hash function

Input type: Text

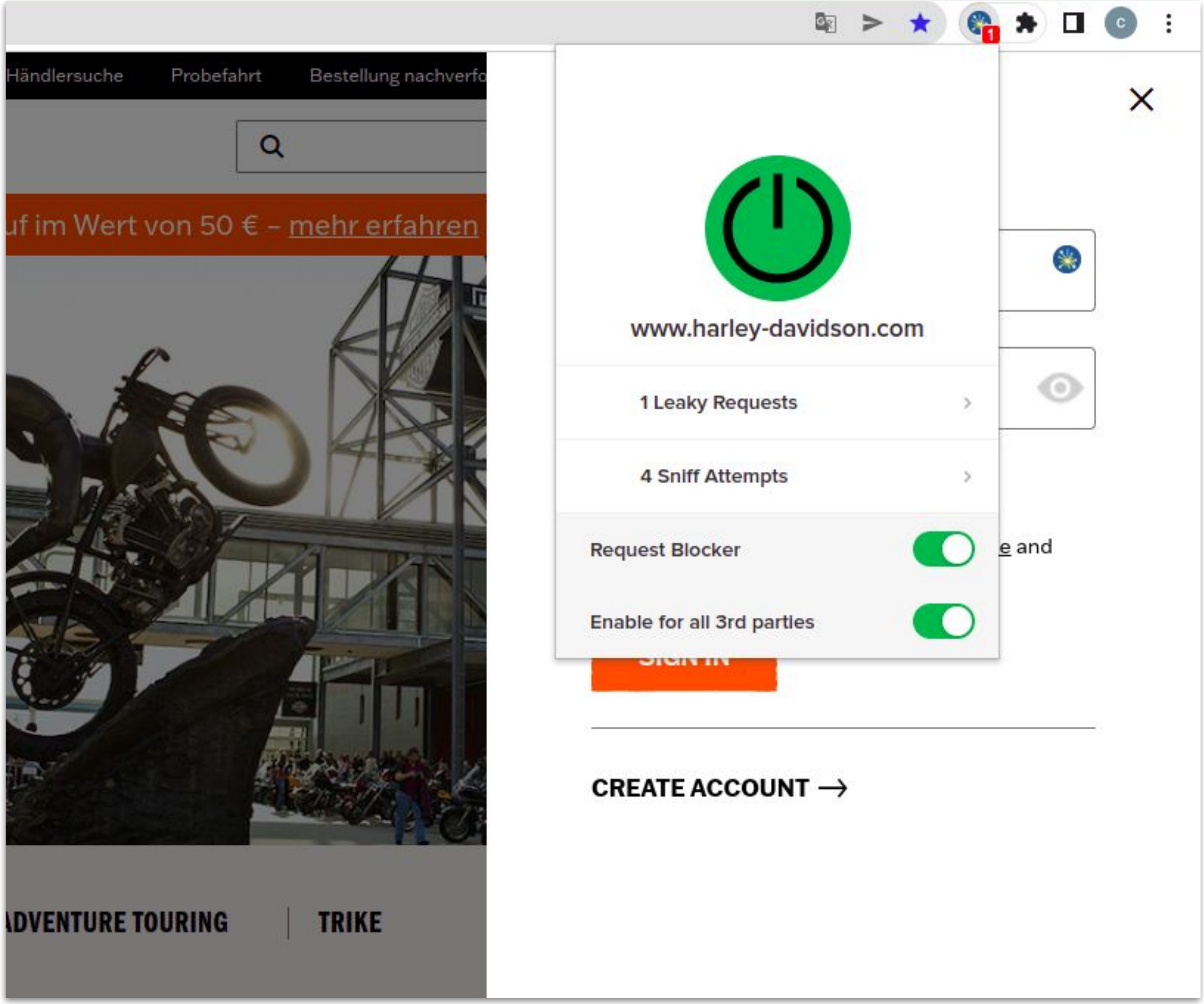
☑ Auto Update

Countermeasures

- Browser add-ons **block requests** to tracker domains
- Private **email relay** services hide users’ emails
  - Apple, Mozilla, DuckDuckGo
  - e.g. testuser@duck.com-> testuser@gmail.com
- **NO** tool for detection and prevention of **sniff & exfiltration** on online forms

Browser add-on: LEAKINSPECTOR

- Detects sniff attempts
- Blocks leaky requests
- https://github.com/leaky-forms/leak-inspector



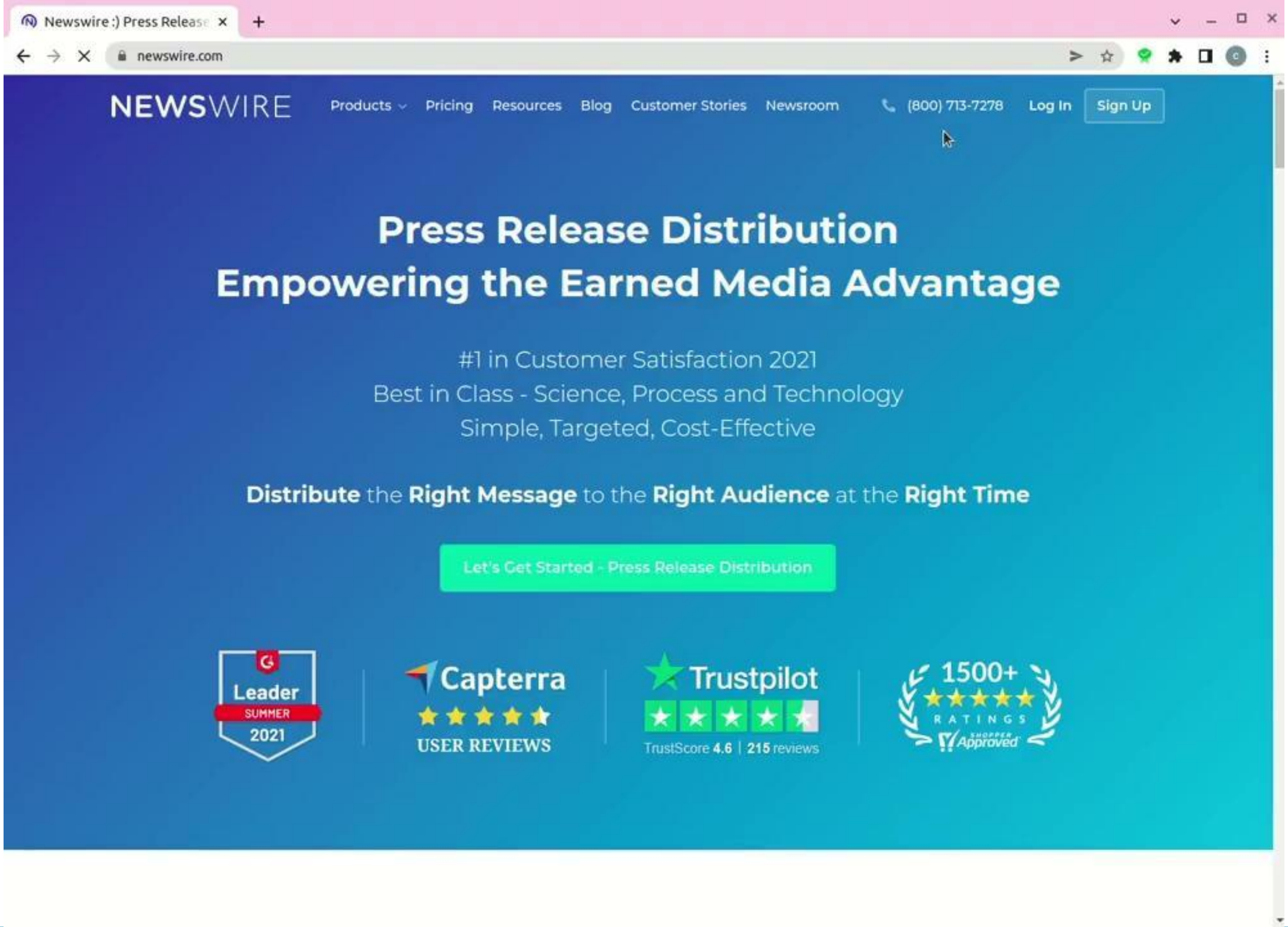
www.harley-davidson.com

1 Leaky Requests ›

4 Sniff Attempts ›

Request Blocker: on

Enable for all 3rd parties: on



Press Release Distribution Empowering the Earned Media Advantage

#1 in Customer Satisfaction 2021
Best in Class - Science, Process and Technology
Simple, Targeted, Cost-Effective

Distribute the **Right Message** to the **Right Audience** at the **Right Time**

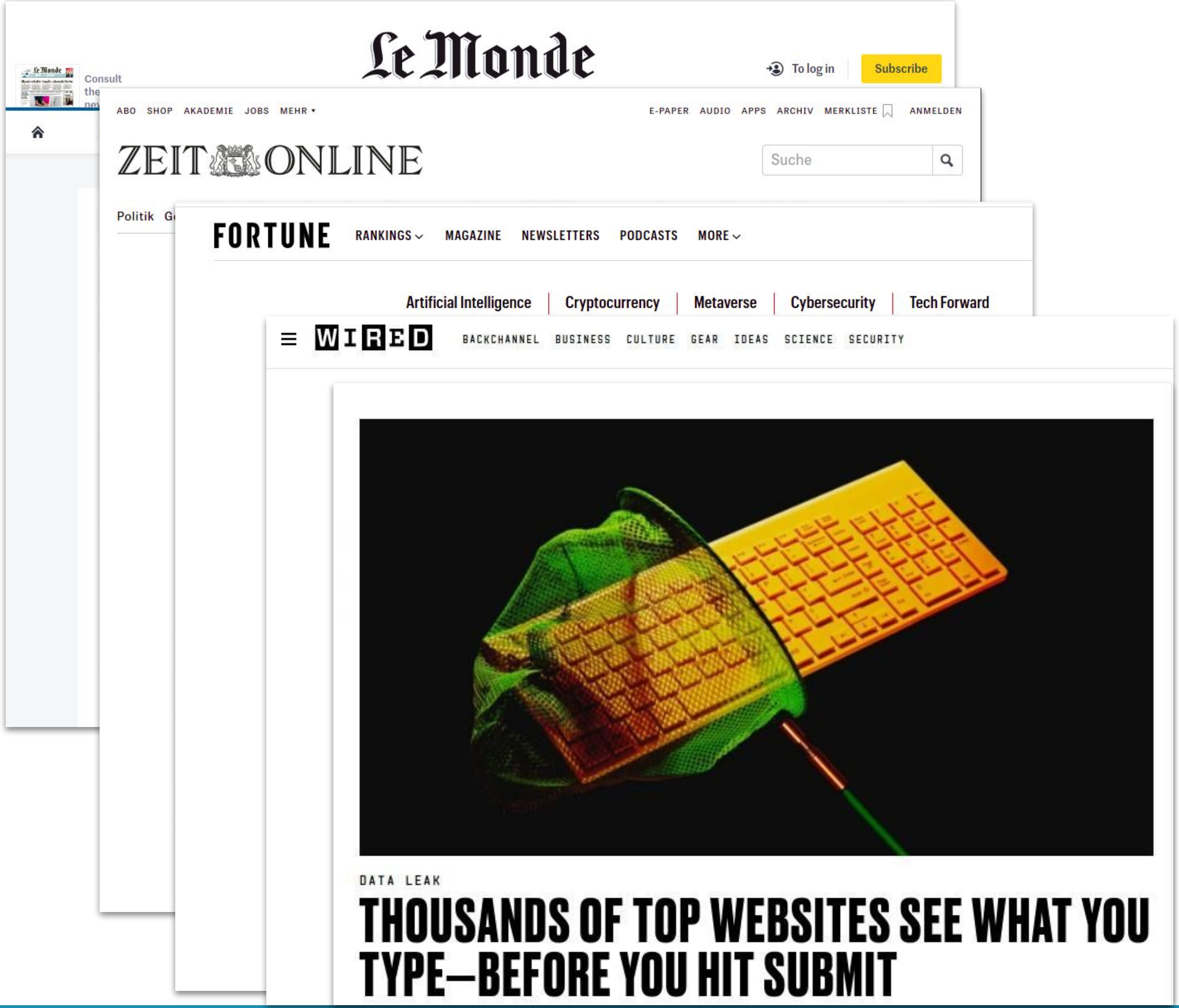
Let's Get Started - Press Release Distribution
Leader
SUMMER
2021
Capterra
USER REVIEWS
Trustpilot
TrustScore 4.6 | 215 reviews
1500+
RATINGS
Shopper Approved

Summary

- Email leaks on 1,844 (EU), 2,950 (US) websites
- Password leaks on 52 websites due to session replay scripts
- Uncovered 41 unlisted tracking domains
- Developed a transparency browser add-on that detects and blocks personal data exfiltration from online forms

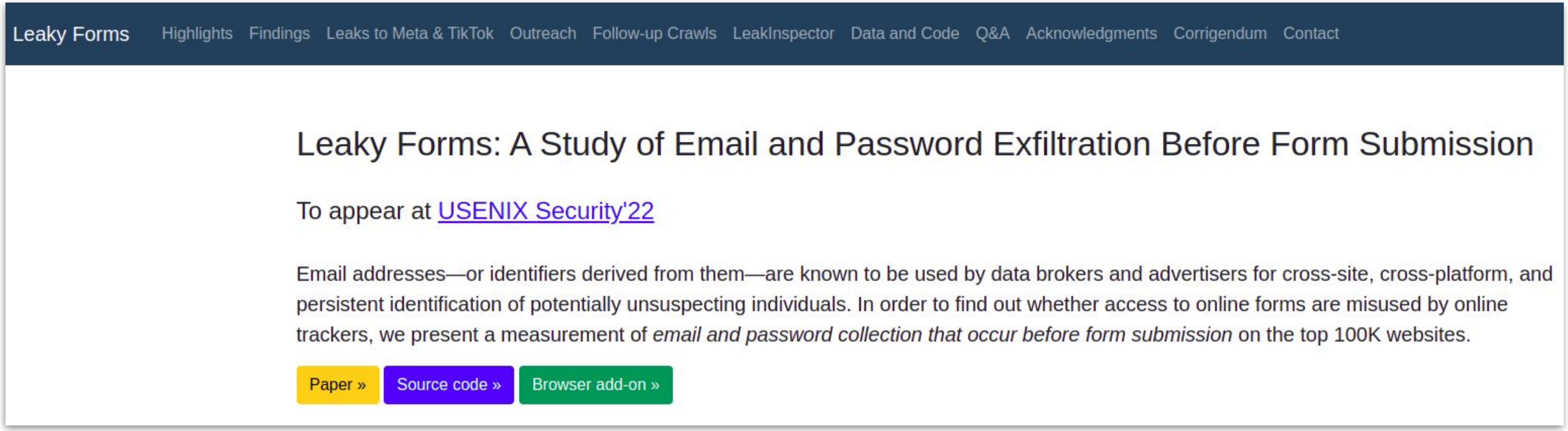
Press

- WIRED
- Le Monde
- Zeit
- Fortune
- ….


Le Monde
Consult the new
To log in
Subscribe
ABO SHOP AKADEMIE JOBS MEHR
E-PAPER AUDIO APPS ARCHIV MERKLISTE ANMELDEN
ZEIT ONLINE
Suche
Politik G
FORTUNE
RANKINGS MAGAZINE NEWSLETTERS PODCASTS MORE
Artificial Intelligence | Cryptocurrency | Metaverse | Cybersecurity | Tech Forward
WIRED
BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY
DATA LEAK

THOUSANDS OF TOP WEBSITES SEE WHAT YOU TYPE—BEFORE YOU HIT SUBMIT

Any Questions?



Leaky Forms Highlights Findings Leaks to Meta & TikTok Outreach Follow-up Crawls LeakInspector Data and Code Q&A Acknowledgments Corrigendum Contact

Leaky Forms: A Study of Email and Password Exfiltration Before Form Submission

To appear at USENIX Security'22

Email addresses—or identifiers derived from them—are known to be used by data brokers and advertisers for cross-site, cross-platform, and persistent identification of potentially unsuspecting individuals. In order to find out whether access to online forms are misused by online trackers, we present a measurement of *email and password collection that occur before form submission* on the top 100K websites.

Paper » Source code » Browser add-on »

Source code: https://github.com/leaky-forms/leaky-forms

Project website: https://homes.esat.kuleuven.be/~asenol/leaky-forms