FEROOT 2019 USER SECURITY AND PRIVACY REPORT

Detecting the Hidden Behaviors of Externally Controlled Tools and Scripts

This study looks at the hidden behaviors and concealed activities of **third-** and **fourth-party** tools and scripts on the user side of websites and web apps, to help security and privacy professionals understand where unseen threats and data breaches may occur.

By the Numbers

- **1.1 million webpages scanned**
- **365 organizations reviewed across 13 industries, including government agencies**
- **274,677 unique web tracker detections**
- **64,035 cross-border data transfers**

Research Objective 1

Understand the prevalence of hidden data collection and cross-border data transfers by the third- and fourth-party tools from the point of view of an anonymous visitor or customer (i.e. the user or client side).

Research Objective 2

Assess the risks and regulatory non-compliance of behavior tracking tools on commercial and public interests.

Feroot scanned more than 1.1 million web pages on 365 websites across 13 industries worldwide, including government agencies, to take a closer look at the following:

- Automated collection of personal data and cross-border data transfers on public facing websites and web apps from the point of view of an anonymous user or customer (i.e. the client side);
- Data collection practices of web tracking tools across industries;
- The impact of third- and hidden fourth-party tools and behavior tracker activities on GDPR, CCPA, PCI-DSS, HIPAA, and other regulatory and security standards that impact daily business operations.

Simulated visits were conducted from April 19 to May 31, 2019, and were repeated multiple times with approximately 90 pages per website per day.

Table of Contents

Executive Summary

A rise in regulatory scrutiny and the increase of data breaches worldwide is demonstrating the need for companies to be far more vigilant about the type of data they collect on customers and ensuring that data is protected from potential theft. Privacy teams need to track where data is stored, processed, and transferred, by whom and for what purpose. Security teams need to be hyperaware of the risks for accessing personal and sensitive data.

The challenges faced by most security professionals is the constant growth of the tech stack: third- and fourth-party vendors, web trackers, and homegrown technology tools are always in flux. New tools and trackers are added daily for marketing and sales purposes. Vulnerabilities introduced by these tools, no thanks to externally loaded codes, are challenging to detect and monitor as they rapidly change. Major damages in the form of data breaches from these vulnerabilities were recently experienced by Ticketmaster, British Airways, Forbes, New Egg, and Quest.

Our goal with this report is to equip privacy and security teams with the insights they need to protect user data and prevent it from being misused.

Key research insights

1. **News industry websites are at a higher risk of user-data breach or data misuse compared to other industries**

News websites use twice as many externally controlled scripts and tools compared to the other industries monitored. More than 90% of major news websites have active externally loaded trackers that are conducting cross-border data transfers to foreign countries, in this case to Russia, potentially posing information security and compliance problems.

2. Third-party software (SaaS) tools are increasing the client side attack surface area

Our scans revealed an average of 21 web trackers per website. External software-as-a-service (SaaS) tools have created a new surface area for attack as the growing number of tools leads to more vulnerabilities like a Man-in-the-middle (MITM) attack through JavaScript, chatbots, analytics and advertising tools.

3. E-commerce and news industry websites are at the highest risk of user-data breach compared to other industries

90% of e-commerce login pages are susceptible to security and compliance issues via hidden third- and fourth-party tools and scripts.
"41% of organizations had a third-party related incident in the past 24 months."

"The average cost of a data breach was $3.8M in 2018."

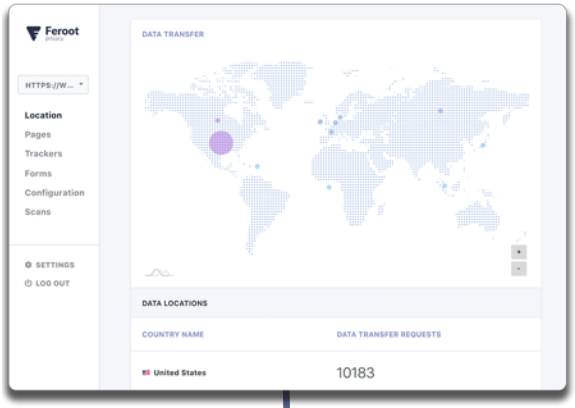
2018 Cyber Risk Report — Ponemon Institute

Research Methodology

More than 1.1 million unique page visits were scanned across 365 organizational websites and web apps in 13 different industries including government agencies. Using the Feroot client side security monitoring system, scans were performed between April 19 - May 31, 2019, and repeated multiple times with approximately 90 pages per website per day. The primary focus was on organizations and government agencies located in the US, Canada, UK, France, Spain, and Germany.

Industries:

1. Airline
2. Automotive
3. Banking
4. Consulting Services
5. E-commerce
6. Government Agencies
7. Hospitality
8. Insurance
9. News
10. Retail
11. Technology
12. Telecom
13. Travel



Feroot client side security monitoring system was used to detect and report:

1. Cross-border data transfers to third- and fourth-party servers

2. Web trackers collecting data before a visitor accepts or rejects “cookies”

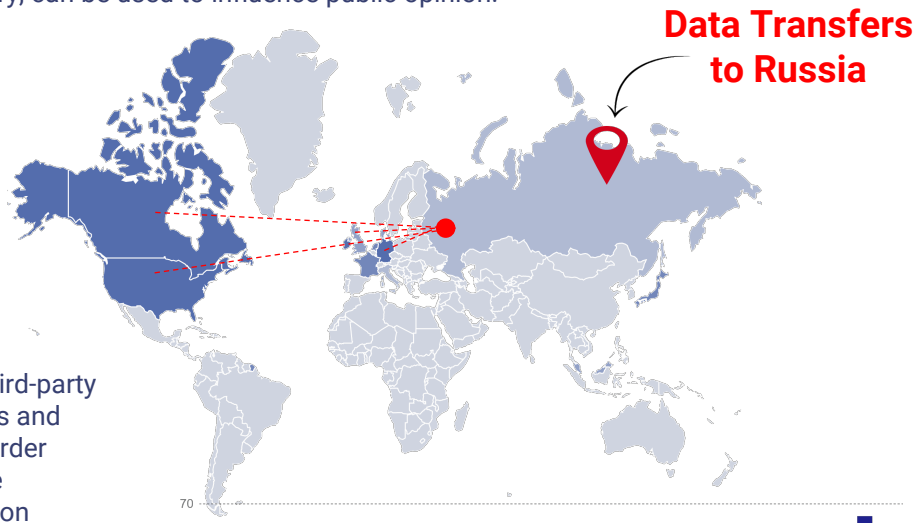
3. Inventory of first- and third-party tools and scripts executed on the user browser (i.e. client side).

Finding 1:

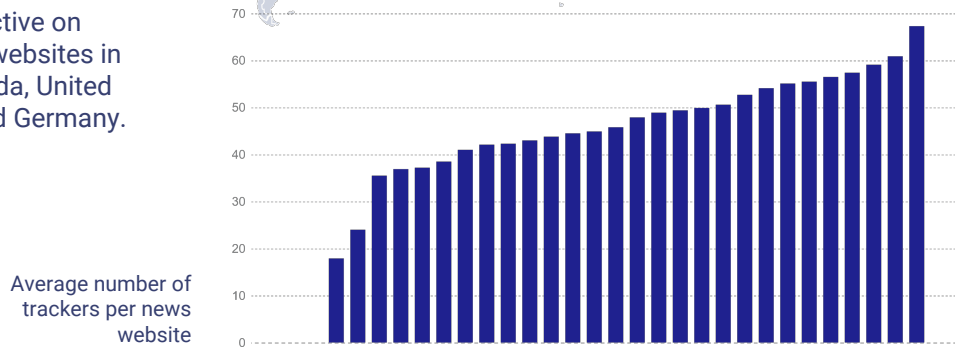
92% of major news websites have data transfers to Russian and are at higher risk of data misuse

Major news publications in the US, Canada, UK, and Germany have on average 40 active third-party web tracking tools on their websites, and five (5) active cross-border data transfers. The media industry sites show **double the amount of web tracking tools** than the other industries surveyed and are the only industry consistently sending user-data to Russia.

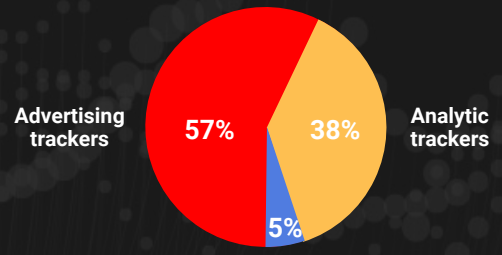
As ad tech and analytic tools used by this industry continue to track the online behavior of millions of people, sensitive profiling information such as data about political or personal beliefs, or browsing history, can be used to influence public opinion.



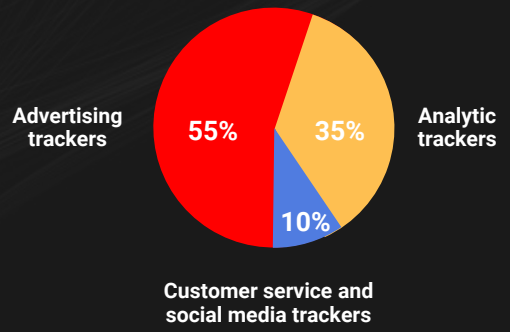
On average, **40** third-party web tracking tools and five (11) cross-border data transfers are constantly active on major news websites in the US, Canada, United Kingdom, and Germany.



Types of web trackers detected in the news industry



Types of web trackers detected across the globe



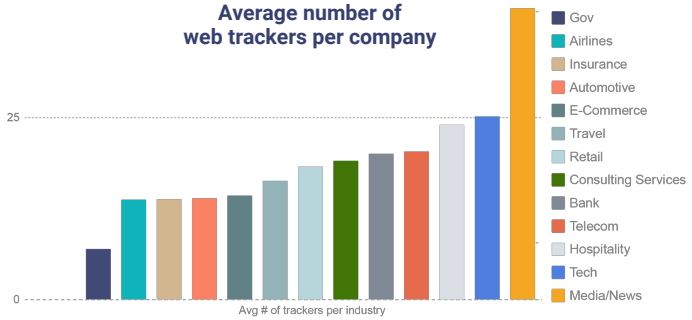
Finding 2:

21 third-party tools are active on the average website but remain unmonitored

Chatbots, ad-trackers, tag managers, analytics and other tools can be used to gain access to sensitive customer data on web apps and websites due to the loss of control over code changes executed on the client (user) side. With 21 web trackers constantly active on the average website, many organizations are at risk of malicious code changes executed in the user browser without ever knowing it. This is what led to data breaches at Ticketmaster, Forbes, Feedify, and more...

97%

of websites use third-party tools



3 main risks from injected code via third- and fourth-party tools :

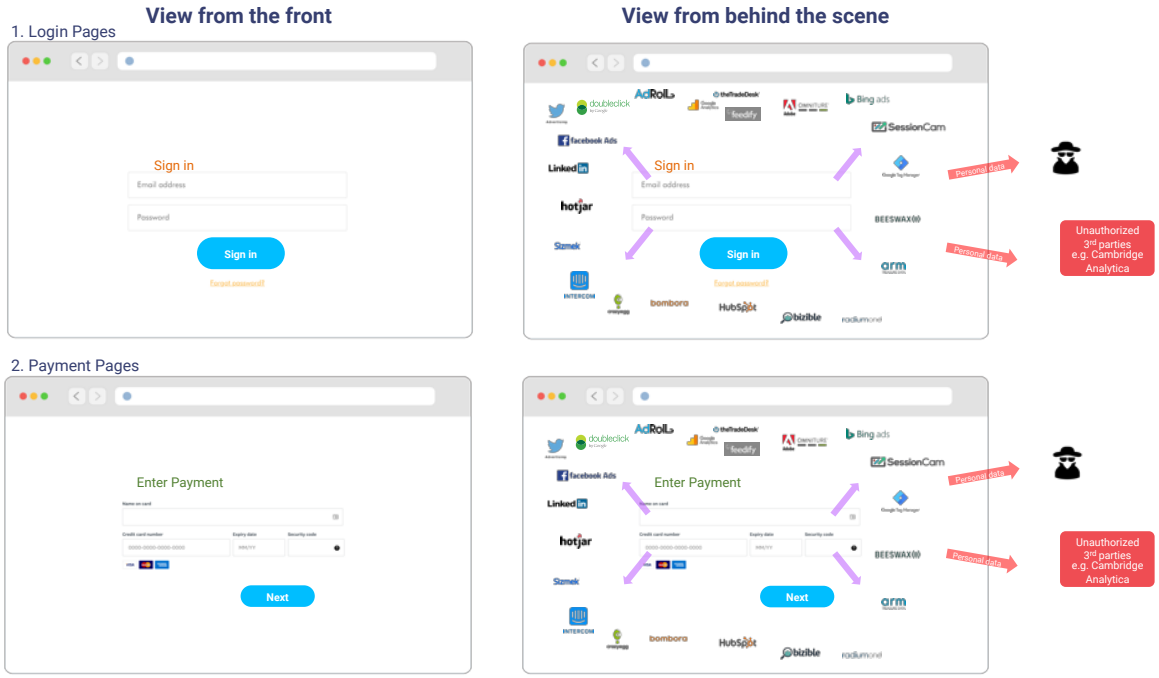
1. Skimming of sensitive data, including user credentials and credit card information.
2. Collecting identifiable user data that can be sold, prior to visitors accepting or rejecting "cookies".
3. Cross-border data transfers from the visitor's web browser to third- and fourth-party servers in foreign destinations.

Finding 3:
90% of e-commerce login pages might provide unrestricted view of passwords to hidden third- and fourth-party tools

After taking a closer look at e-commerce login pages, we found the majority of these pages have web trackers present. This poses a real and ongoing data security and privacy threat because:

- script libraries, tags, and side-loaded code can be injected by third-parties at any time
- the scripts can send customer behavioral data across borders without proper governance or consent

This means organizations are risking regulatory non-compliance with GDPR, CCPA, PCI-DSS, HIPAA, and other regulatory and security standards that have a significant impact on daily business operations.



90% of login pages of e-commerce websites are susceptible to attacks

On average, 4,800 websites compromised with Formjacking code each month

2019 Symantec Internet Security Threat Report (ISTR) link

Global Report

13 Industries at a Glance

5
Avg. # Data Transfers/Company

21
Avg. Numb of Trackers/Company

HIGH RISK OF USER CREDENTIALS THEFT
Customer account sign in fields are often in clear view of multiple externally controlled tools and scripts on majority of websites

HIGH RISK OF SENSITIVE DATA THEFT
Credit card payment, user name, and password fields are occasionally in clear view of multiple externally controlled tools and scripts

RISK OF PROFILING DATA MISUSE BY FOREIGN GOVERNMENT
92% of major news websites sporadically use **Russian-based** ad-trackers with automatic data transfer to Russia

Top 10 Countries

RECEIVING DATA

1. United States
2. Ireland
3. Germany
4. France
5. Japan
6. Netherlands
7. Canada
8. Unidentified
9. United Kingdom
10 Singapore

Top 10 Trackers

DETECTED

1.Google Analytics (6%)
2. Google Tag Manager (5%)
3. DoubleClick (5%)
4. Facebook Business (4%)
5. Facebook Connect (4%)
6. Google Analytics Audiences (4%)
7. Google Remarketing (4%)
8. Google AdWords (3%)
9. AppNexus (3%)
10. LiveRamp (2%)

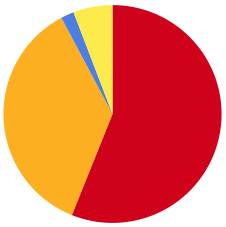
Top 3 Companies

RECEIVING DATA

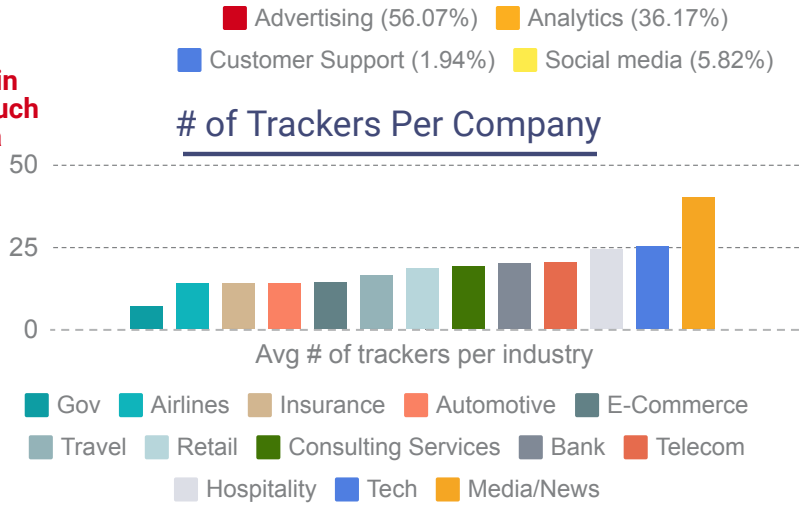
1. Google (26%)
2. Facebook (9%)
3. Adobe (4%)

Types of Trackers

ACROSS COMPANIES



Risks of data misuse in countries of concern such as Russia and China



Airline Industry

4
Avg. # Data Transfers/Company

13
Avg. Numb of Trackers/Company

ELEVATED RISK OF USER CREDENTIALS THEFT
User name and password fields of travel accounts are often in clear view of multiple externally controlled tools and scripts

Top 10 Countries

RECEIVING DATA

1. United States
2. Ireland
3. France
4. Japan
5. Germany
6. Denmark
7. Unidentified
8. Netherlands
9. Singapore
10. Sweden

Top 10 Trackers

DETECTED

1. Google Tag Manager (6%)
2. Google Analytics (6%)
3. Facebook Business (6%)
4. Facebook Connect (6%)
5. DoubleClick (6%)
6. Google Analytics Audiences (5%)
7. Omniture (Adobe Analytics) (4%)
8. Google Remarketing (3%)
9. Google AdWords (3%)
10. Bing Ads (3%)

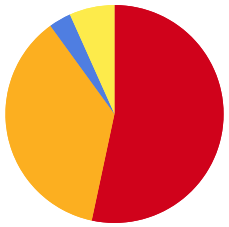
Top 3 Companies

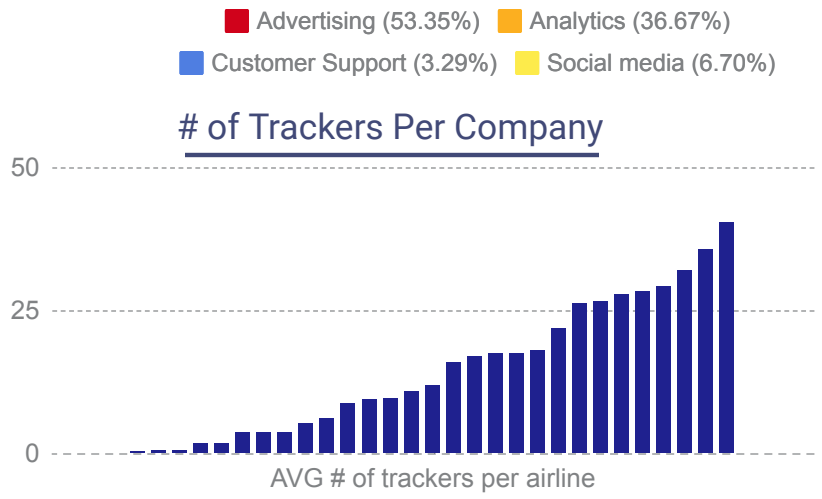
RECEIVING DATA

1. Google (34%)
2. Facebook (12%)
3. Adobe (6%)

Types of Trackers

ACROSS COMPANIES





Automotive Industry

4
Avg. # Data Transfers/Company

14
Avg. Numb of Trackers/Company

ELEVATED RISK OF USER CREDENTIALS THEFT
User name and password fields of car-owner web accounts are often in clear view of multiple externally controlled tools and scripts

Top 10 Countries

RECEIVING DATA

1.United States
2. Ireland
3. United Kingdom
4. Japan
5. Singapore
6. Netherlands
7. France
8. Canada
9. Germany
10. Unidentified

Top 10 Trackers

DETECTED

1. Google Analytics (10%)
2. Google Tag Manager (9%)
3. DoubleClick (9%)
4. Omniture (Adobe Analytics (5%)
5. Google Analytics Audiences (5%)
6. Facebook Connect (5%)
7. Adobe Marketing Cloud (4%)
8. Facebook Business (4%)
9. Google Remarketing (3 %)
10. Google AdWords (3%)

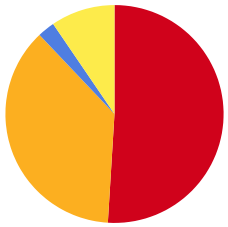
Top 3 Companies

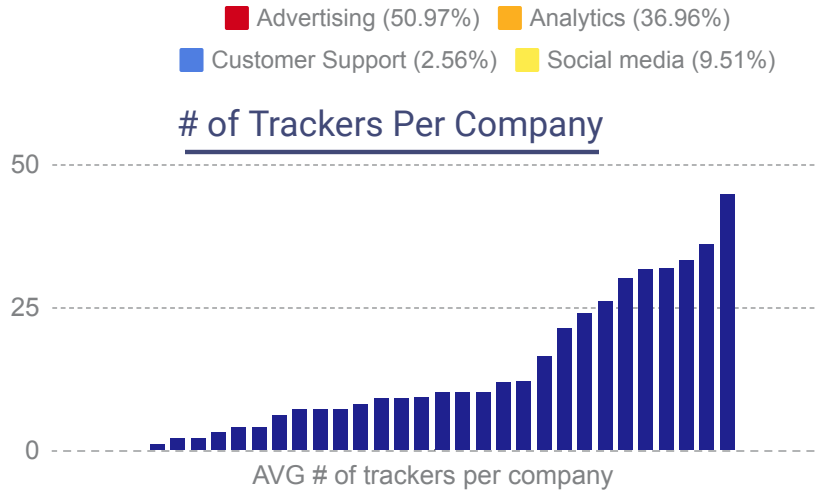
RECEIVING DATA

1. Google (40%)
2. Adobe (9%)
3. Facebook (9%)

Types of Trackers

ACROSS COMPANIES





Banking Industry

4
Avg. # Data Transfers/Company

20
Avg. Numb of Trackers/Company

ELEVATED RISK OF USER CREDENTIALS THEFT
Online banking account sign in fields are often in clear view of multiple externally controlled tools and scripts

Top 10 Countries

RECEIVING DATA

1. United States
2. Ireland
3. United Kingdom
4. Canada
5. France
6. Germany
7. Singapore
8. Italy
9. Netherlands
10. Denmark

Top 10 Trackers

DETECTED

1. DoubleClick (6%)
2. Google Analytics (5%)
3. Google Tag Manager (5%)
4. Facebook Business (5%)
5. AppNexus (4%)
6. Google Remarketing (4%)
7. Google Analytics Audiences (4%)
8. Omniture (Adobe Analytics) (4%)
9. Rubicon (4%)
10. Twitter Analytics (4%)

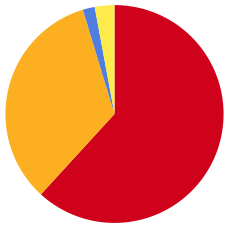
Top 3 Companies

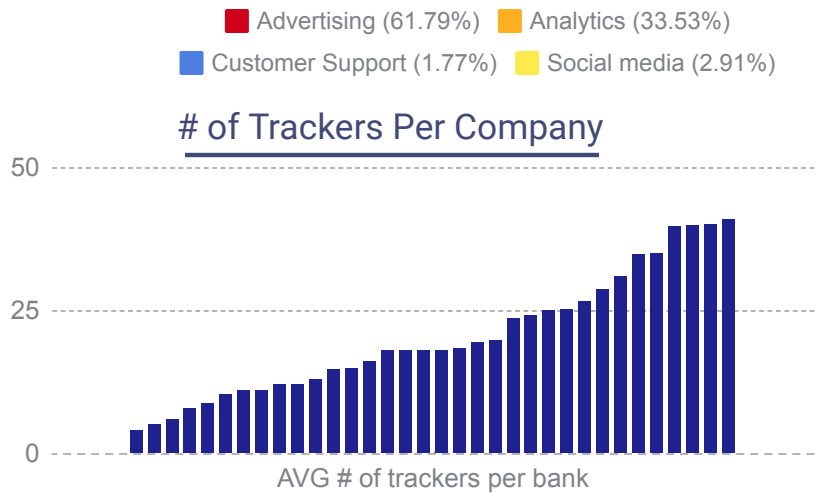
RECEIVING DATA

1. Google (27%)
2. Facebook (7%)
3. Adobe (8%)

Types of Trackers

ACROSS COMPANIES





Consulting Services

4
Avg. # Data Transfers/Company

19
Avg. Numb of Trackers/Company

RISK OF PRIVACY ISSUES
Third-party advertising trackers, tag-management tools, and externally controlled scripts are occasionally present on public pages, login fields, and forms

Top 10 Countries

RECEIVING DATA

1. United States
2. Ireland
3. Japan
4. Netherlands
5. Germany
6. Denmark
7. United Kingdom
8. Singapore
9. Canada
10. Unidentified

Top 10 Trackers

DETECTED

1. Google Analytics (8%)
2. Google Tag Manager (6%)
3. DoubleClick (6%)
4. Facebook Connect (5%)
5. LinkedIn Ads (5%)
6. Facebook Business (5%)
7. Google Remarketing (5%)
8. Adobe Marketing Cloud (5%)
9. Omniture (Adobe Analytics) (4%)
10. Google Analytics Audiences (4%)

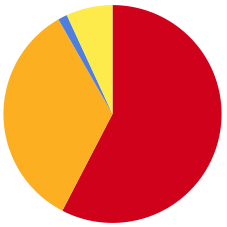
Top 3 Companies

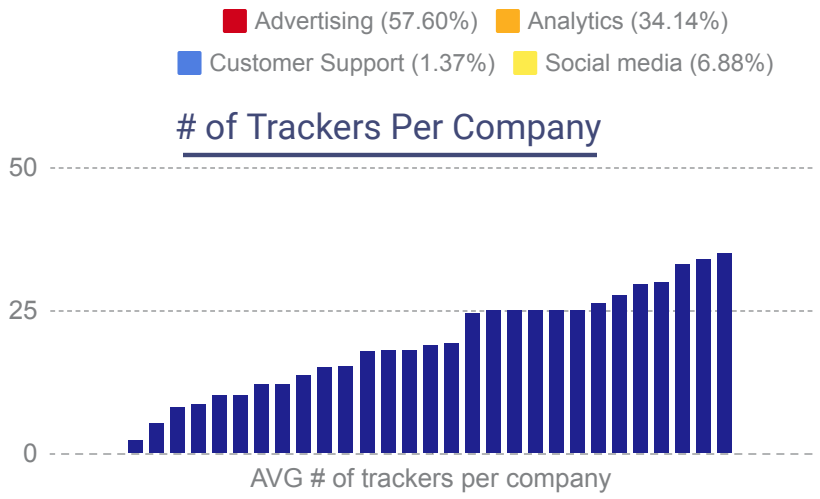
RECEIVING DATA

1. Google (32%)
2. Linkedin (11%)
3. Facebook (10%)

Types of Trackers

ACROSS COMPANIES





E-commerce Industry

3
Avg. # Data Transfers/Company

14
Avg. Numb of Trackers/Company

HIGH RISK OF SENSITIVE DATA THEFT
Credit card payment, user name, and password fields are occasionally in clear view of multiple externally controlled tools and scripts

Top 10 Countries

RECEIVING DATA

1. United States
2. Ireland
3. Unidentified
4. Netherlands
5. Singapore
6. Canada
7. Germany
8. France
9. Denmark
10. United Kingdom

Top 10 Trackers

DETECTED

1. Google Analytics (11%)
2. DoubleClick (10%)
3. Facebook Connect (9%)
4. Facebook Business (9%)
5. Google Analytics Audiences (7%)
6. Amplitude (4%)
7. Quantcount (4%)
8. SkimLinks (4%)
9. Scorecard Research (4%)
10. Google Tag Manager (3%)

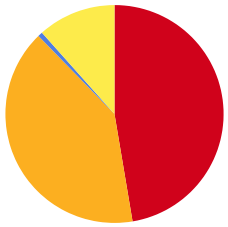
Top 3 Companies

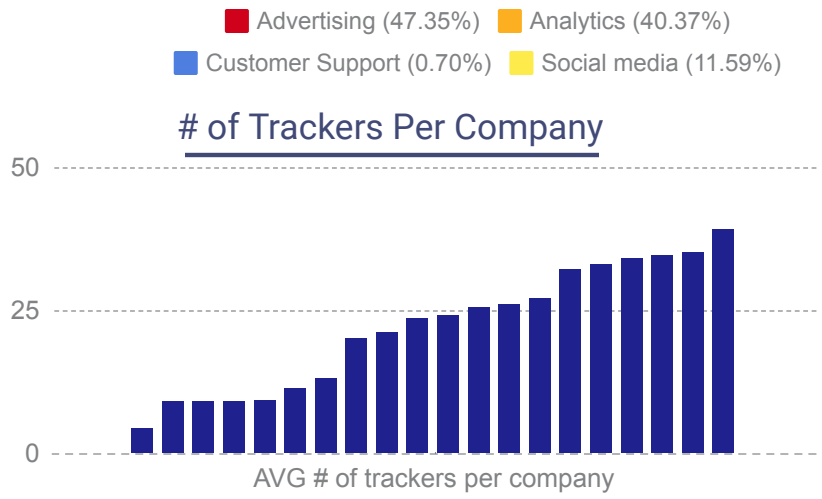
RECEIVING DATA

1. Google (36%)
2. Facebook (19%)
3. Twitter (3%)

Types of Trackers

ACROSS COMPANIES





Government Agencies

In the US, Canada, France, Germany, Spain, & UK

3
Avg. # Data Transfers/Company

7
Avg. Numb of Trackers/Company

RISK OF PRIVACY ISSUES
Third-party advertising trackers, tag-management, and externally controlled scripts are occasionally present on public pages and login fields

Top 10 Countries

RECEIVING DATA

1. United States
2. United Kingdom
3. Ireland
4. France
5. Canada
6. Luxembourg
7. Japan
8. Netherlands
9. Germany
10. Unidentified

Top 10 Trackers

DETECTED

1. Google Analytics (26%)
2. DoubleClick (13%)
3. Google Tag Manager (13%)
4. New Relic (6%)
5. Facebook Connect (5%)
6. Twitter Button (5%)
7. Twitter Syndication (5%)
8. Facebook Business (3%)
9. Hotjar (3%)
10. Google Analytics Audiences (3%)

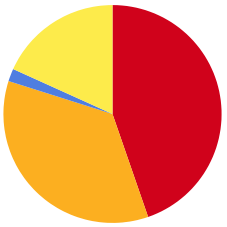
Top 3 Companies

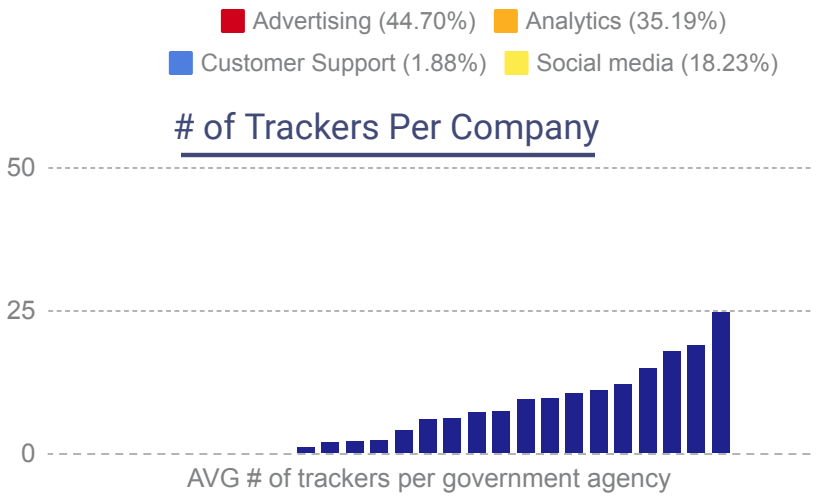
RECEIVING DATA

1. Google (56%)
2. Twitter (9%)
3. Facebook (9%)

Types of Trackers

ACROSS COMPANIES





Hospitality Industry

6
Avg. # Data Transfers/Company

24
Avg. Numb of Trackers/Company

RISK OF SENSITIVE DATA THEFT
Credit card payment, user name and password fields are occasionally in clear view of multiple externally controlled tools and scripts

Top 10 Countries

RECEIVING DATA

1. United States
2. Ireland
3. France
4. Germany
5. Japan
6. Unidentified
7. Netherlands
8. China
9. United Kingdom
10. Singapore

Top 10 Trackers

DETECTED

1. Facebook Connect (4%)
2. Google Analytics (4%)
3. Facebook Business (4%)
4. Google Remarketing (4%)
5. AppNexus (4%)
6. Google Tag Manager (4%)
7. Google AdWords (4%)
8. DoubleClick (3%)
9. LiveRamp (3%)
10. Rubicon (3%)

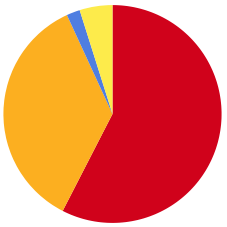
Top 3 Companies

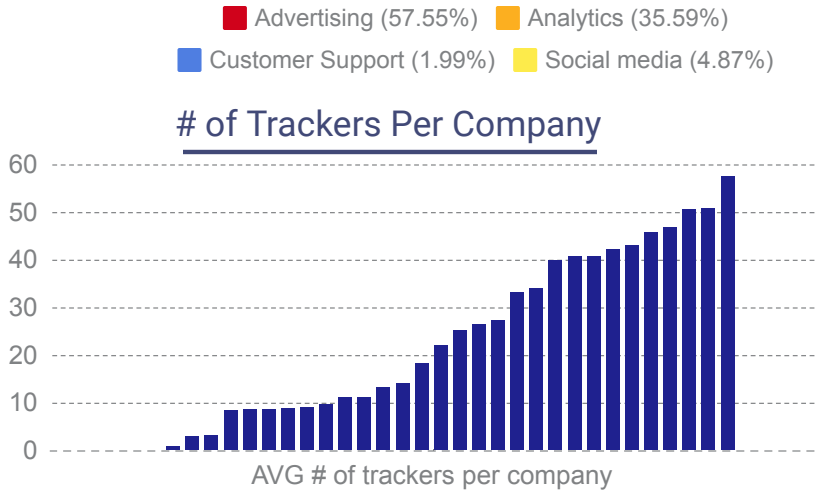
RECEIVING DATA

1. Google (22%)
2. Facebook (8%)
3. Adobe (5%)

Types of Trackers

ACROSS COMPANIES





Insurance Industry

4
Avg. # Data Transfers/Company

14
Avg. Numb of Trackers/Company

RISK OF PRIVACY ISSUES
Third-party advertising trackers, tag-management tools, and externally controlled scripts are occasionally present on public pages, login fields, and secure pages with sensitive information

Top 10 Countries

RECEIVING DATA

1. United States
2. Ireland
3. France
4. Netherlands
5. Germany
6. Japan
7. Denmark
8. United Kingdom
9. Italy
10. Switzerland

Top 10 Trackers

DETECTED

1. Google Analytics (7%)
2. Google Tag Manager (6%)
3. DoubleClick (6%)
4. LinkedIn Ads (5%)
5. Facebook Connect (4%)
6. Facebook Business (4%)
7. Google Analytics Audiences (4%)
8. LinkedIn Analytics (3%)
9. Google Remarketing (3%)
10. Google AdWords (3%)

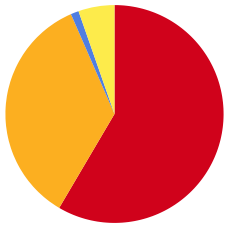
Top 3 Companies

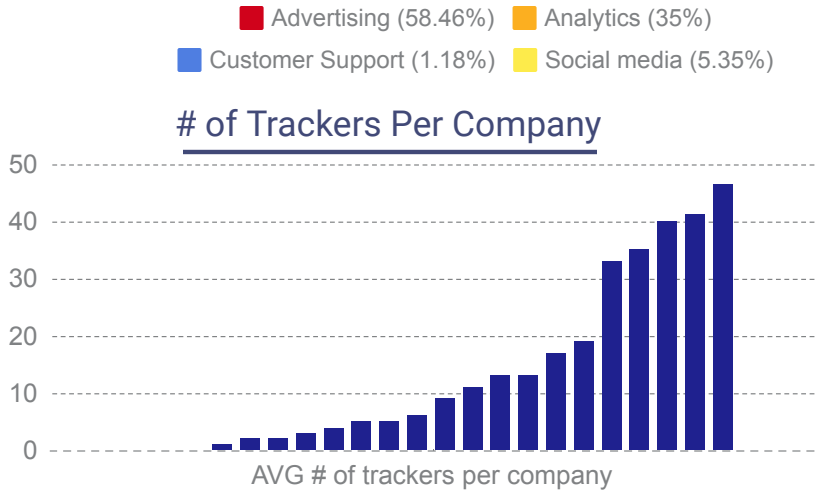
RECEIVING DATA

1. Google (29%)
2. Facebook (9%)
3. LinkedIn (8%)

Types of Trackers

ACROSS COMPANIES





News Industry

11
Avg. # Data Transfers/Company

40
Avg. Numb of Trackers/Company

RISK OF PRIVACY ISSUES
92% of major news websites sporadically use Russian based ad-trackers with automatic data transfer to Russia

RISK OF SENSITIVE DATA THEFT
Credit card payment, user name and password fields are occasionally in clear view of multiple externally controlled tools and scripts

Top 10 Countries

RECEIVING DATA

1. United States
2. Germany
3. Ireland
4. Canada
5. Unidentified
6. France
7. Netherlands
8. Japan
9. Denmark
10. Singapore

Top 10 Trackers

DETECTED

1. Index Exchange (5%)
2. Scorecard Research (4%)
3. AppNexus (4%)
4. LiveRamp (3%)
5. OpenX (3%)
6. Facebook Connect (3%)
7. Facebook Business (3%)
8. Google Analytics (3%)
9. DoubleClick (3%)
10. Adobe Marketing Cloud (3%)

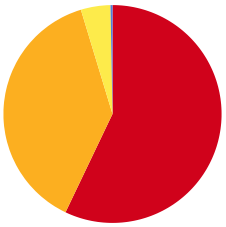
Top 3 Companies

RECEIVING DATA

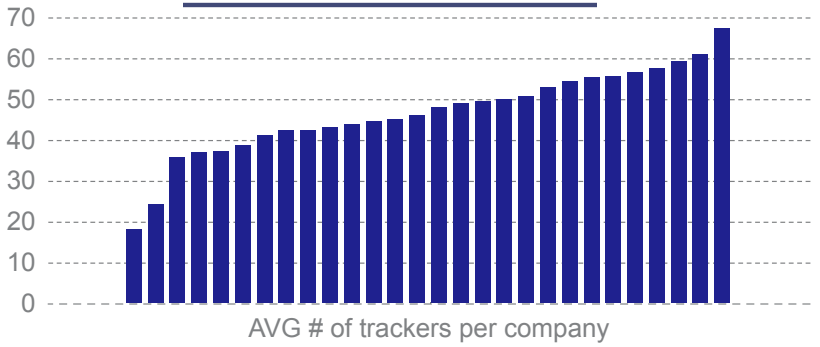
1.Google (14%)
2. Facebook (6%)
3. Twitter (4%)

Types of Trackers

ACROSS COMPANIES



of Trackers Per Company



Retail Industry

4
Avg. # Data Transfers/Company

18
Avg. Numb of Trackers/Company

RISK OF SENSITIVE DATA THEFT
Credit card payment, user name and password fields are occasionally in clear view of multiple externally controlled tools and scripts

Top 10 Countries

RECEIVING DATA

1. United States
2. Ireland
3. United Kingdom
4. Netherlands
5. Canada
6. Japan
7. Unidentified
8. Singapore
9. France
10. Denmark

Top 10 Trackers

DETECTED

1. Facebook Connect (6%)
2. Google Tag Manager (6%)
3. Google Analytics (6%)
4. Facebook Business (6%)
5. DoubleClick (5%)
6. Google Remarketing (4%)
7. Google Analytics Audiences (4%)
8. Google AdWords (4%)
9. AppNexus (3%)
10. New Relic (3%)

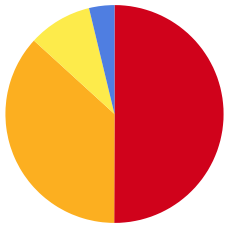
Top 3 Companies

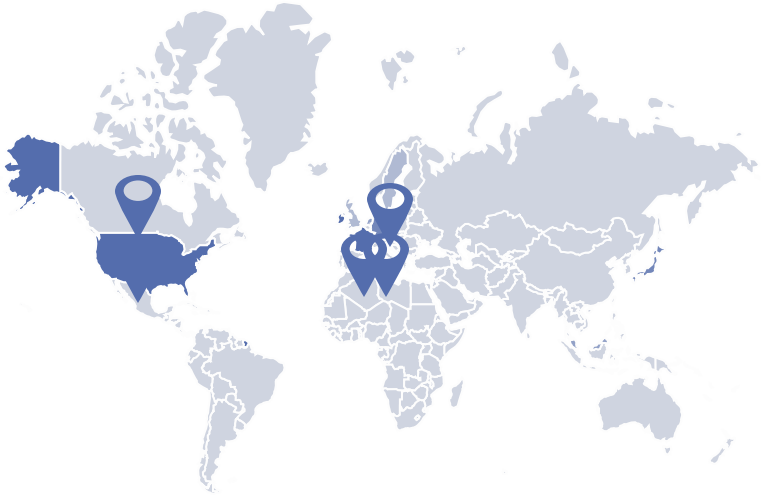
RECEIVING DATA

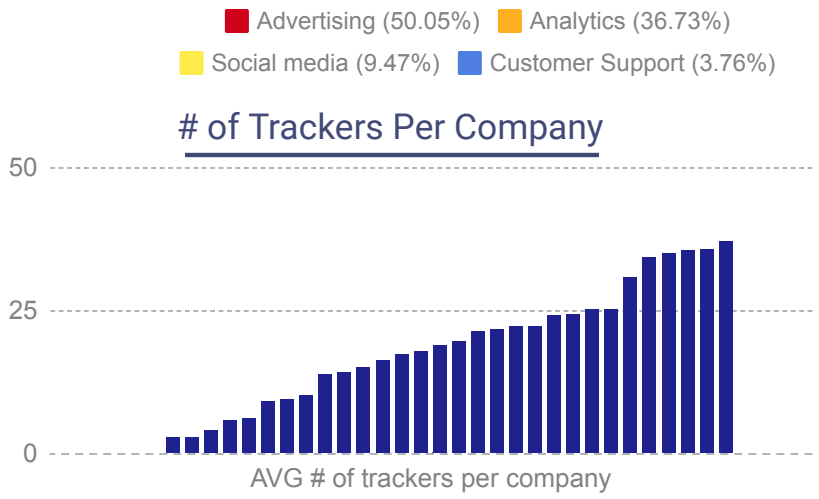
1. Google (28%)
2. Facebook (12%)
3. Twitter (6%)

Types of Trackers

ACROSS COMPANIES







Tech Industry

4
Avg. # Data Transfers/Company

25
Avg. Numb of Trackers/Company

RISK OF PRIVACY ISSUES
Some websites sporadically use Russian based tools with automatic data transfer to Russia

HIGH RISK OF SENSITIVE DATA THEFT
Credit card payment, user name, and password fields are occasionally in clear view of multiple externally controlled tools and scripts

Top 10 Countries

RECEIVING DATA

1. United States
2. Ireland
3. Japan
4. Netherlands
5. Unidentified
6. Singapore
7. Canada
8. Germany
9. United Kingdom
10. Denmark

Top 10 Trackers

DETECTED

1. Google Analytics (6%)
2. Google Tag Manager (5%)
3. DoubleClick (5%)
4. Google Analytics Audiences (5%)
5. Facebook Connect (5%)
6. Facebook Business (4%)
7. LinkedIn Ads (4%)
8. Google Remarketing (3%)
9. Google AdWords (3%)
10. LinkedIn Marketing (3%)

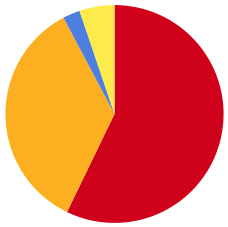
Top 3 Companies

RECEIVING DATA

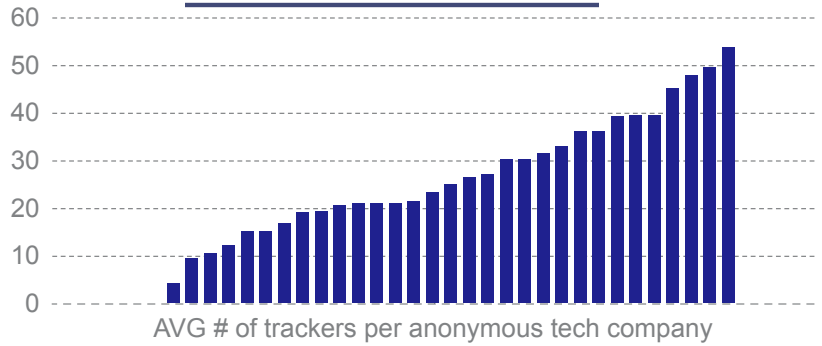
1. Google (28%)
2. Facebook (9%)
3. LinkedIn (9%)

Types of Trackers

ACROSS COMPANIES



of Trackers Per Company



Telecom Industry

5
Avg. # Data Transfers/Company

20
Avg. Numb of Trackers/Company

RISK OF SENSITIVE DATA THEFT
Credit card payment, user name, and password fields are occasionally in clear view of multiple externally controlled tools and script

Top 10 Countries

RECEIVING DATA

1. United States
2. Ireland
3. Germany
4. Canada
5. United Kingdom
6. France
7. Netherlands
8. Switzerland
9. Spain
10. Australia

Top 10 Trackers

DETECTED

1. DoubleClick (6%)
2. Google Tag Manager (6%)
3. Omniture (Adobe Analytics) (5%)
4. Google Remarketing (5%)
5. Google Analytics Audiences (5%)
6. Google Analytics (5%)
7. Google AdWords (5%)
8. Facebook Business (4%)
9. Facebook Connect (4%)
10. Twitter Analytics (3%)

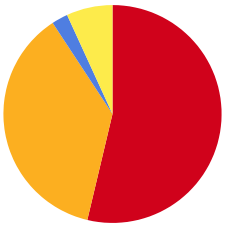
Top 3 Companies

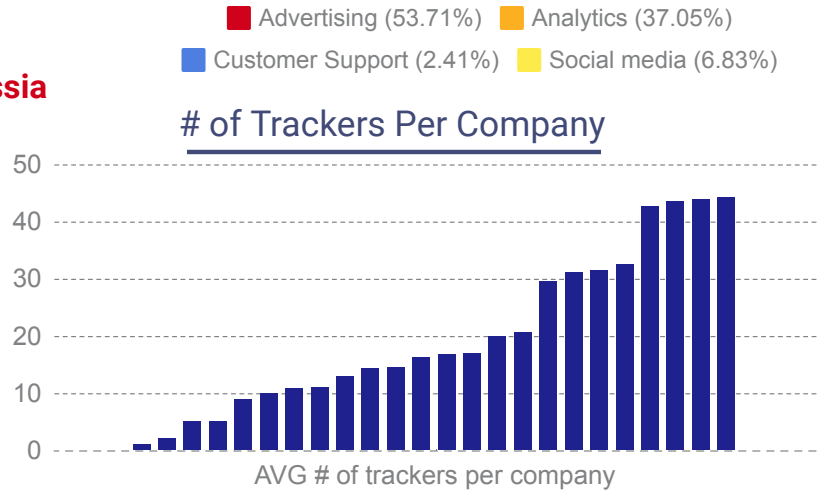
RECEIVING DATA

1. Google (30%)
2. Adobe (8%)
3. Facebook (8%)

Types of Trackers

ACROSS COMPANIES





Travel Industry

4
Avg. # Data Transfers/Company

16
Avg. Numb of Trackers/Company

ELEVATED RISK OF PRIVACY ISSUES
Third-party trackers and scripts from digital ad networks and analytics tools are present on pages that collect personal information.

Top 10 Countries

RECEIVING DATA

1. United States
2. Ireland
3. Germany
4. Netherlands
5. Canada
6. Japan
7. Denmark
8. Singapore
9. Unidentified
10. United Kingdom

Top 10 Trackers

DETECTED

1. Google Analytics (9%)
2. Google Tag Manager (7%)
3. DoubleClick (6%)
4. Google Analytics Audiences (5%)
5. Facebook Connect (5%)
6. Facebook Business (4%)
7. Google Remarketing (3%)
8. Google AdWords (3%)
9. Bing Ads (3%)
10. AppNexus (2%)

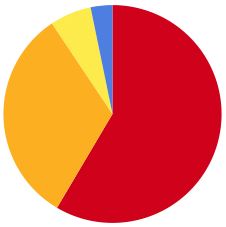
Top 3 Companies

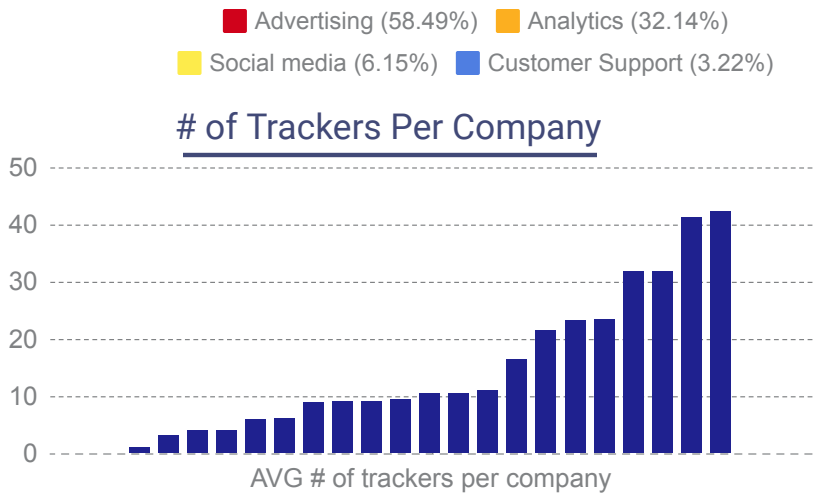
RECEIVING DATA

1. Google (32%)
2. Facebook (9%)
3. Twitter (2%)

Types of Trackers

ACROSS COMPANIES

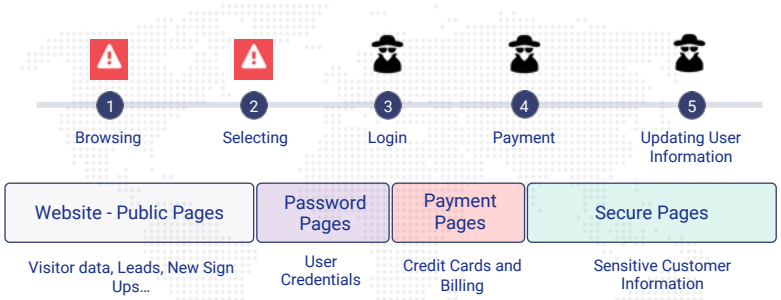




Conclusion:

Hidden activities of third-party tools and scripts expose up to 97% of organizations to theft of customer data.

The scope of this study reveals an average of 21 tracking tools per web page capturing data in real-time on 97% of websites. Because these technologies rely heavily on outside services managed by third- and fourth-party vendors, they open the organization to a new surface attack area, in particular, the **Man-in-the-middle (MITM) attack vector**. This area requires ongoing monitoring due to the fact that the externally controlled scripts are often introduced through the user browser (or the client side) rather than the tools themselves.



Recommendations

1. Ensure that only third-party tools with applicable compliance level (i.e. PCI-DSS, HIPAA, etc) are present on pages with payment, health information, and other pages with regulatory obligations.

2. Consider strong containment of third- and fourth-party scripts via iFrame sandboxing, Content Security Policy and other hardening techniques.

3. Actively monitor the client side third- and fourth-party controlled scripts access to data on production websites and web apps.

4. Don't limit security and privacy testing to dedicated test and development environments. Instead, continuously monitor and test production environments

Resources:

2019 Symantec Internet Security Threat Report (ISTR), link

2018 Cost of Data Breach Study: Impact of Business Continuity Management, link
by Ponemon Institute

Payment Card Industry (PCI) Data Security Standard Report on Compliance, link

Using metadata tagging tools for PCI DSS compliance, link
by TechTarget

Magecart: Breach of Ticketmaster and more... , link
by RiskIQ

Web Application Security Guidance, link
by OWASP

Third-Party JavaScript Management Cheat Sheet, link
by OWASP

Definitions

Advertising technology (or adtech) - the term that refers commonly to all technologies, software and services used for delivering and targeting online advertisements.

Advertising trackers – a utility, script or program that monitors the performance of advertising campaigns

Analytic trackers – a utility, script or program that gathers statistical data from connected web sources for analysis. (Source: https://linktrack.info/p/ad_tracker)

Attack Vector - a path or means by which a hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome.

Customer Service trackers - a utility, script or program that gathers and organizes information related to customer activities.

CCPA - The California Consumer Privacy Act (CCPA) is a bill that enhances privacy rights and consumer protection for residents of California, USA.

Chatbot – a computer program designed to simulate conversation with human users, especially over the Internet.

Code Injection - the general term for attack types which consist of injecting code that is then interpreted/executed by the application.

Cross-border data transfers - The transfer of information, or data, is often referred to as data flows. Placed in a global context, data flows which cross country borders is cross border data flows.

Controller - The data controller is the one who owns the data. They make the decision to collect personal data in the first place.

Cookies (Internet) - messages that **web** servers pass to your **web** browser when you visit **Internet** sites. Your browser stores each message in a small file, called **cookie**.txt . When you request another page from the server, your browser sends the **cookie** back to the server.

Data leaks - the unauthorized transmission of data from within an organization to an external destination or recipient.

Data (singular and plural) - raw, unorganized facts that need to be processed. Data can be something simple and seemingly random and useless until it is organized.

Data Protection - the process of safeguarding important information from corruption, compromise or loss.

GDPR - *The General Data Protection Regulation* is a regulation in EU law on data protection and privacy for all individuals and citizens of the European Union (EU) and European Economic Area (EEA).

Fourth-Party - someone your third-party vendor outsources to. Some companies call them sub-processors, providers, strategic partners etc.

Formjacking - a term to describe the use of malicious JavaScript code to steal credit card details and other information from payment forms on the checkout web pages of e-commerce sites.

HIPAA - The *Health Insurance Portability and Accountability Act.*

Information - when data is processed, organized, structured or presented in a given context so as to make it useful, it is called information.

Informed Consent - permission for something to happen is granted with the knowledge of possible consequences, risks and benefits.

JavaScript - a programming language commonly used in web development to add dynamic and interactive elements to websites.

Libraries (Script or JavaScript) – a file that contains a bunch of functions, and those functions accomplish some useful task for your webpage.

Man-in-the-middle attack - an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other.

Malicious code - an application security threat. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors and malicious active content.

Outlier - a data point that differs significantly from other observations.

PCI-DSS - The *Payment Card Industry Data Security Standard (PCI DSS)* is an information security standard for organizations that handle branded credit cards from the major card schemes.

Personal Data - any information relating to an identified or identifiable natural person ('data subject'), such as a name, an identification number, location data, an online identifier, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Pixel tracking - an HTML code snippet which is loaded when a user visits a website or opens an email.

Privacy - the state or condition of being free from being observed or disturbed by other people and having control relating to the use of your own data.

Processor - the person, public authority, agency or other body that processes the data on behalf of the data controller.

Sub-processor - a process that makes up part of a larger processor. Contractual requirements between processor and sub-processor stay the same as between the data controller and the processor.

Sensitive Data - personal data is considered 'sensitive' and is subject to specific processing conditions when data is revealing racial or ethnic origin; political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation.

SaaS - a method of software delivery and licensing in which software is accessed online via a subscription.

Social media trackers - a utility, script or program that gathers information from social media channels such as blogs, wikis, news sites and micro blogs such as Twitter and social network sits.

Side-loaded code - Sideloading is the installation of an application on a mobile device without using the device's official application-distribution method. Sideloading can result in attack where there is unintended code execution.

Supply chain attack - A supply chain attack, also called a value-chain or third-party attack, occurs when someone infiltrates your system through an outside partner or provider with access to your systems and data.

Third-Party - any organization outside of your company that provides a product or service (such as data processing) and has access to your system.

Trackers or Tags - objects or scripts used on websites to collect and store data on user behavior for advertising, marketing, site optimization, and security purposes. These scripts are the underlying technology that places tracking cookies on consumers browsers.

Web Tracking - Web tracking is the activity (and ability) of a website (using software tools) to keep track of website visitors.

Website – a location connected to the Internet that maintains one or more pages on the World Wide Web

Web Apps and Web-Apps – a web application is a software application that runs on a remote server.

Web Form — a web form or HTML form on a web page allows a user to enter data that is sent to a server for processing.

Two Comprehensive Glossaries

- NICSS Glossary of Common Cybersecurity Terms: https://niccs.us-cert.gov/about-niccs/glossary
- Glossary of Privacy Terms (IAPP) https://iapp.org/resources/glossar

Feroot

Client Side Security Monitoring

Feroot helps security and compliance departments monitor the client-facing attack surface.

Unlike server side security monitoring, Feroot gives visibility into issues introduced by third- and fourth-party tools and scripts such as web trackers, tag managers, chatbots, and analytic tools that are loaded on visitor browsers.

When you activate Feroot to, you will:

- Discover, catalog, and track changes of all tools and scripts that attackers can exploit
- Detect hidden data transfers from visitor browsers to external servers
- Prioritize risks to focus security teams on the highest threats

325 Front St. W. 4th floor
Toronto, ON, Canada, M5V 2Y1

www.feroot.com
security@feroot.com