feroot

2023 Feroot Client-Side Security Report

Beware of Pixels & Trackers

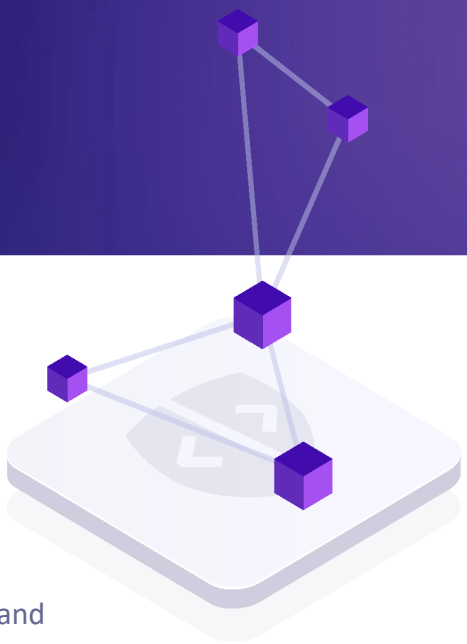
April 5, 2023

As the concern grows regarding data mining companies using pixels/trackers that load into browsers from websites to collect privacy and sensitive user data, compliance regulators and government authorities are increasingly stepping in with bans, restrictions, and executive orders to curb them.

This report provides practical insights for compliance, AppSec, cybersecurity teams, and government regulators to provide them with hard evidence regarding security issues, data breaches, and cyber risks from pixels/trackers, including potential costs of business loss, penalties, fines, and litigation.

Contents

Executive Summary



As concern grew regarding pixels/trackers collecting privacy sensitive user data. A number of articles and researches reported that TikTok and Facebook were particularly worrisome.

Feroot set out to investigate using its client-side web application security tools the realities of these concerns and establish the baseline. Of particular interest were mission-critical webpages (e.g., webpages with login, account creation, registration, or credit card processing functions) where privacy/sensitive user data would be most present (e.g., **usernames, passwords, SSNs, credit card numbers, phone numbers, addresses, health records** and more).

Major findings discovered by the analysis include:

- Pixels/Trackers are common and abundant - an average of 13.16 pixels/trackers were found per website, with Google, Microsoft, Meta (owner of Facebook), ByteDance (owner of TikTok), and Adobe being some of the most common.
- Pixels/Trackers are present on mission-critical webpages increasing the likelihood of risks - an average of 5.96% of websites had pixels/trackers on webpages reading user input forms containing privacy or sensitive data.
- Pixels/Trackers transfer data to foreign locations around the globe - about 5% of the data transferred by pixels/trackers loaded from US-based websites is sent outside the US.
- Pixels/Trackers are collecting and transferring data without first obtaining the explicit consent of visitors - pixels/trackers are actively reading, collecting, and transferring user input before taking action to permit it.
- Pixels/Trackers are loading from domains banned by the US Federal Government and various US States - these pixels/trackers include ones from TikTok and even load from the websites of those same governments.

Executive Summary (continued)

Significant risks identified in the analysis include:

- Privacy compliance violations and penalties - pixels/trackers transferring privacy user data can constitute exposure violations of privacy standards (e.g., GDPR, CCPA, PCI DSS, etc.) and result in possible fines.

- TikTok is often present whether or not the TikTok App is deleted. Likewise, for others banned by governments, TikTok pixels/trackers load into webpages handling mission-critical user data and can collect and transfer it.

- Brand/image damage and lost business - a data breach involving privacy/sensitive data can cause reputation damage, resulting in losing business, customers, and investors (based on such breaches in the past).

- Pixels/Trackers transfer data to countries of concern - pixels/trackers are actively collecting and transferring user data from the webpages loaded into the user's browser from US-based websites to China and Russia.

- TikTok/Bytedance & Facebook/Meta are risk concerns - pixels/trackers associated with TikTok and Facebook are among the top 5 companies collecting and transferring user data (even from mission-critical webpages).

Preventive remediations mentioned in the report include:

- Control or remove suspect pixels/trackers from your webpage code - especially on mission-critical webpages processing sensitive user data (e.g., ones for login, account creation, registration, credit card processing, etc.).

- Add to your risk management program client-side software supply chain (so to prevent pixels/trackers from getting on the webpages where they don't belong and problematic pixels/trackers from getting on any webpages).

- Include client-side security in your cybersecurity program, especially for web application security considerations.

This report aims to equip compliance and security teams with the insights they need to protect user data, prevent its misuse, and avoid the costs of loss business, penalties, fines, ligations, and recoveries from data breaches from client-side security issues caused by pixels/trackers.

Executive Summary (continued)

Figure ES1 shows a sample of a sign up web page and the activities of pixel/trackers. (Organization's name is redacted.)

Figure ES1: An example of a typical new account registration webpage

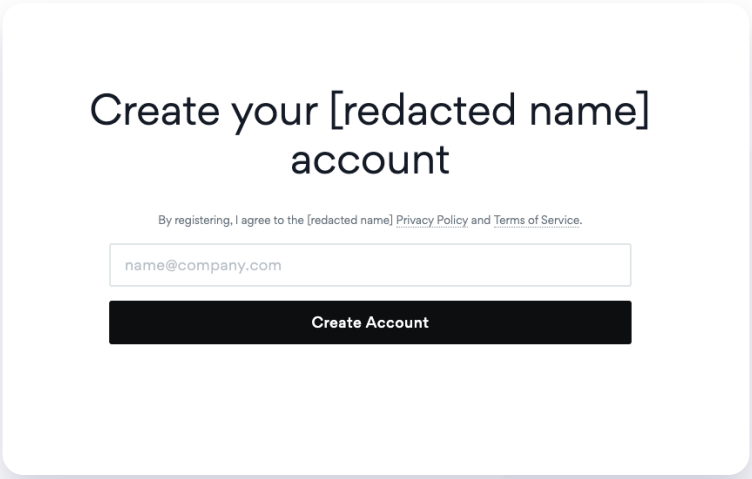
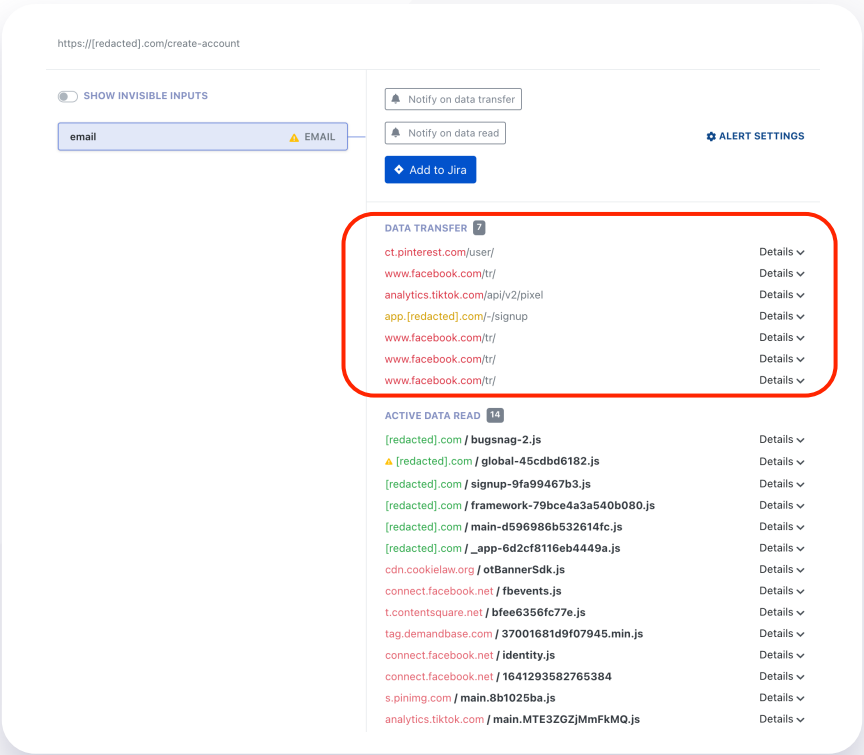


Figure ES2 shows pixels/trackers reading what users are entering into the form and sending collected user data back to their servers. Pixels/trackers and scripts/libraries highlighted in red have unrestricted access to user information on the web page.

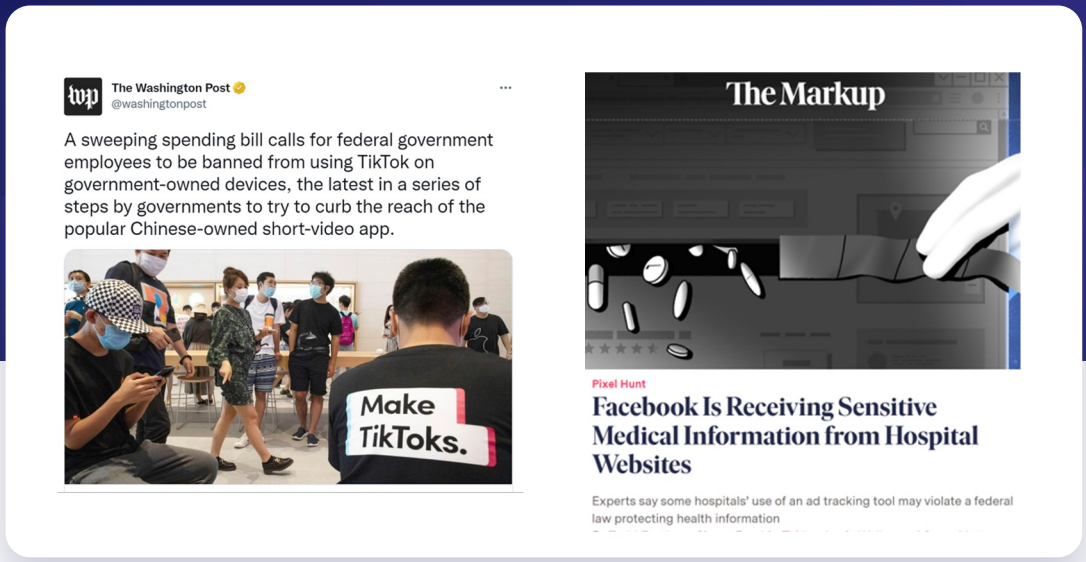
Figure ES2: Pixels/Trackers transferring user data entered into webpage registration form



Introduction

Purpose

At the beginning of 2023, concern grew over pixels and trackers, which load into the browser as a part of the software supply chain, being used by data harvesting platforms to collect user data. The data is then transferred to the servers of the companies owning the pixels/trackers as a part of their advertising and marketing business. Aggressive data harvesting practices increase the likelihood and/or actual transfer of sensitive data, which may cause unintended consequences, including expensive fines and litigations.



The harvested data included:

- Usernames and passwords
- Credit card and banking information
- Personal health details

Alarming locations included:

- China, a jurisdiction under the control of the Chinese Communist Party (CCP)
- Russia, a jurisdiction under the control of FSB - KGB's successor
- Data centers and cloud hosting services of companies banned by the state and federal executive orders.
- Data centers of data-mining social media companies (which all sell advertising)

Research conducted by STAT+ and The Markup was reported in the article ”Out of control: Dozens of telehealth startups sent sensitive health information to big tech companies.” The article found that several social media platforms and sites were tracking sensitive patient information on telehealth companies, including:

- TikTok
- Facebook
- Google
- Snapchat
- Pinterest
- LinkedIn
- Twitter
- AddThis

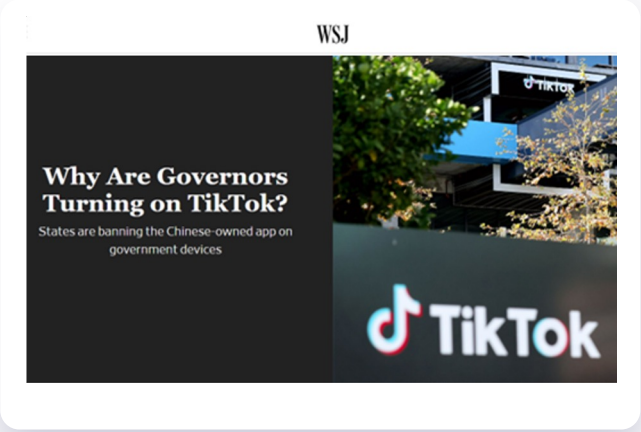
Given the extent of these concerns, Feroot launched an investigation to ascertain the exact magnitude and pervasiveness of social media pixels/trackers collecting and transferring personal, sensitive, and private data using pixels or trackers. Feroot’s client-side security platform made it possible to get detailed facts regarding active client-side e-skimming.

This report presents the facts and findings discovered from Feroot’s investigation.

Methodology

By examining the details in the client-side pixel and tracker scripts loaded into a browser upon visiting a website, Feroot sought to answer why pixels/trackers are a security issue, including:
an 8-week period spanning January and February of 2023:

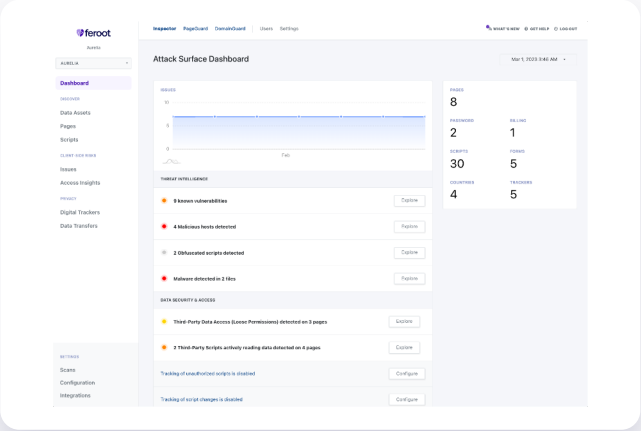
- how ubiquitous are pixels/trackers and which specific ones are most prevalent
- what data was collected by those pixels/trackers and what data was the most prevalently collected
- how often do pixels/trackers appear on mission-critical webpages. e.g., webpages for login, account creation, registration, etc.
- where do those pixels/trackers send the data they collect and what locations are most prevalent for collection
- do these vary by data-mining, advertising, or social media platform and exactly how
- do the above answers vary by industry and exactly in what ways they differ



Technology

Feroot Inspector was used for its ability to gather data directly relevant to answering these questions. Inspector is a crawler, similar to Googlebot, to assess what gets loaded into the browser when a given webpage is requested. It observes and assesses activities of scripts and the like, including:
how ubiquitous are pixels/trackers and which specific ones are most prevalent

- presence of pixels and/or trackers
- types of data collected
- destinations to which the collected data is sent, which also includes malicious hosts, which were the identified items of interest in this investigation.



With the specific details that Inspector provides about these items, Feroot then analyzes and reports the exact extent of pixels/trackers, the security issues associated with their presence, and the related business risks for those issues for different industries.

Furthermore, Feroot Inspector also collected data about the software supply chain and its dependencies, including other third-party and downstream fourth-party scripts, additional client-side scripts reading and transferring data, cross-border transfers, obfuscated scripts, and more. This was done in order to get a complete map of one's client-side attack surface.

Data Collection

3,675 organizations

3,142 websites

7 sectors

108,836 webpages

227 trackers

7,000,000 data transfers

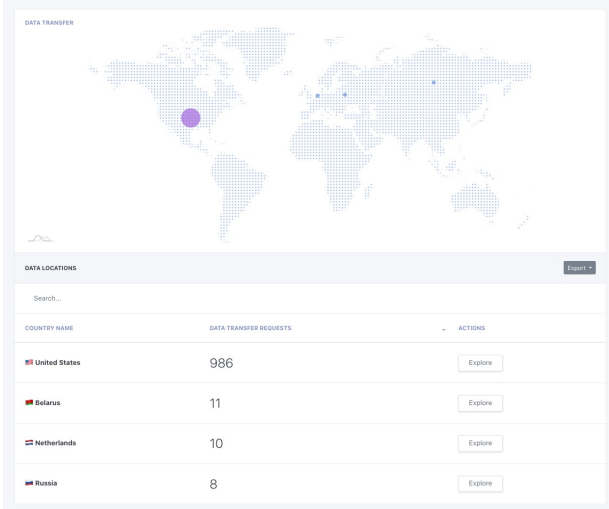
Feroot Inspector collected data on pixels/trackers over an 8-week period spanning January and February of 2023:

- The research examined over **3,675** organizations with unique websites. Of these, **3,142** websites were analyzed in depth.
- 7 sectors (Airlines, e-Commerce, Banking & Financial Services, Healthcare & Telehealth, US Federal and US State Governments).
- Across **108,836** unique web pages, including mission-critical webpages (e.g., those with login, registration, and credit card processing functions).
- **227** unique trackers, including social media ones were discovered.
- **255** domains owned by 17 companies banned by executive orders in the U.S were found in the client-side software supply chain.
- More than **7,000,000** unique outbound data transfers were detected and analyzed.
- More than 1**,000,000** scripts and libraries were discovered as part of the client-side software supply chain of assessed organizations.

Analyses

Feroot analyzed the data it collected regarding pixels/trackers collecting and transferring data correlated against:

- Known banned companies, their applications, pixels/trackers, etc.
- Handling of privacy and sensitive user data
- Known business and operational risks related to data breaches and calculated percentages and distributions of the results for the relevant cases of interest.



In addition, Feroot performed additional analyses in terms of cross-comparisons across specific industries, specific social media platforms, and the combinations thereof. The key findings, weaknesses/vulnerabilities, and business risks/impacts resulting from the analyses are presented in the subsequent pages of this report.

Findings

Performing a study on the client-side security of a web application aims to identify potential risks and vulnerabilities that could compromise the security and/or privacy compliance of the application and its data. By doing so, businesses can develop strategies to mitigate or manage these risks, reduce negative impacts, and protect their reputation, credibility, financial interests, and customers' data. The major findings of this study appear in this section.

Finding #1: Pixels/Trackers are common and abundant

Table F1-1 shows how pervasive pixels/trackers are on the webpages scanned associated with each website of all the companies that were analyzed.

Table F1-1: Presence of pixels/trackers on websites - by sector

Sectors	Average number of pixels/trackers per website	Number of unique websites analyzed	Percentage of websites with pixels/trackers
Financial Services & Banking	12.53	431	94.20%
Healthcare & Telehealth	12.90	541	98.06%
Technology and SaaS	16.81	553	97.74%
e-Commerce	17.90	551	96.73%
Airlines	7.40	485	85.83%
US Federal Government	5.70	159	99.05%
US State Government	12.41	422	97.51%
Average/Total	**13.16**	**3,142**	**95.35%**

Finding #1: Continued

Figure F1-1 shows Google is the absolute dominant collector of client-side data at 92% present on websites across all the sectors studied. Microsoft, Facebook round up the Top 3.

TikTok (ByteDance) related pixels/trackers are at 7.41% and growing.

Figure F1-1: Percentage of websites with pixels/trackers by platform

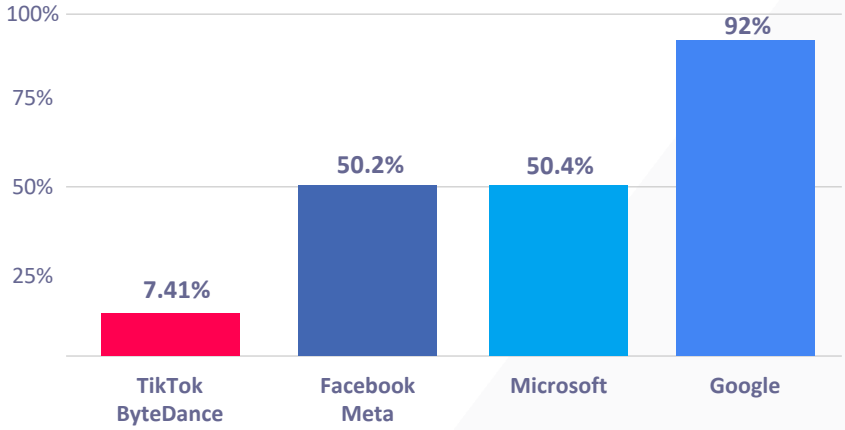
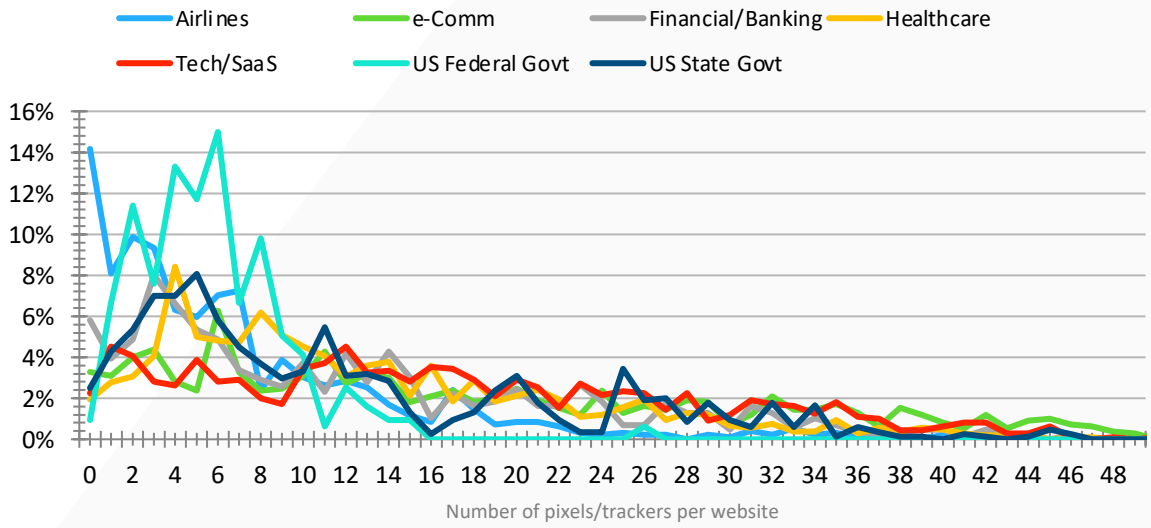


Figure F1-2 shows distributions for percentages of websites within each of 7 sectors relative to the number of trackers occurring on those websites with the overall average being 13.16.

Figure F1-2: Distribution of percentage of analyzed websites over number of trackers



Finding #1: Continued

Figure F1-3 through Figure F1-9 show the distribution of pixels/trackers found for each sector as a percentage of websites where found.

Figure F1-3: Distribution of percentage of analyzed websites over number of trackers

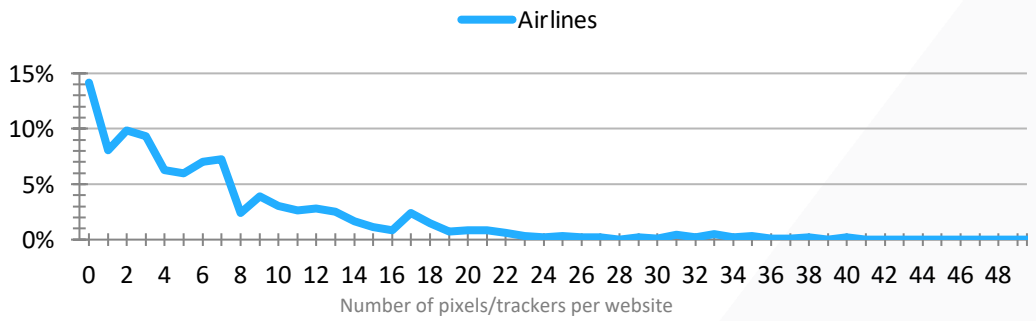


Figure F1-4: Distribution of percentage of analyzed websites over number of trackers

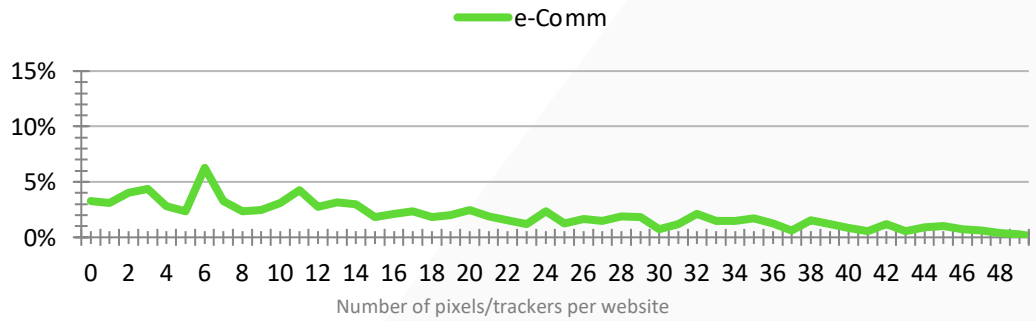
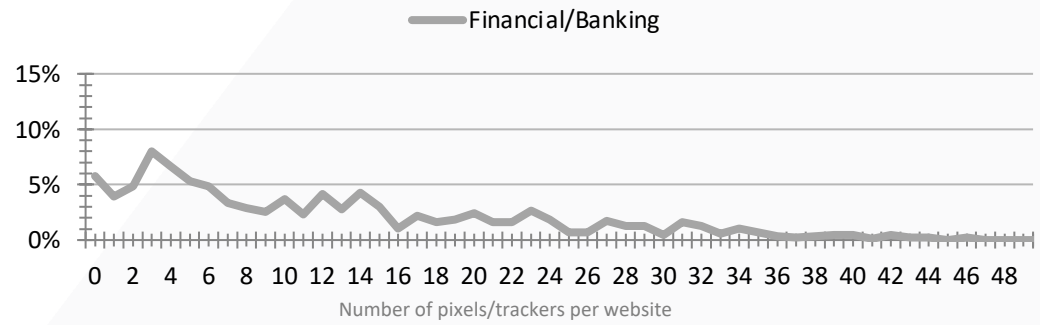


Figure F1-5: Distribution of percentage of analyzed websites over number of trackers



Finding #1: Continued

Figure F1-6: Distribution of percentage of analyzed websites over number of trackers

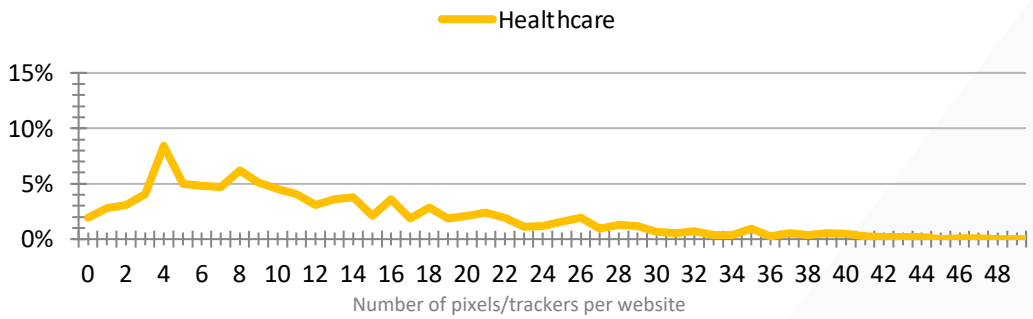


Figure F1-7: Distribution of percentage of analyzed websites over number of trackers

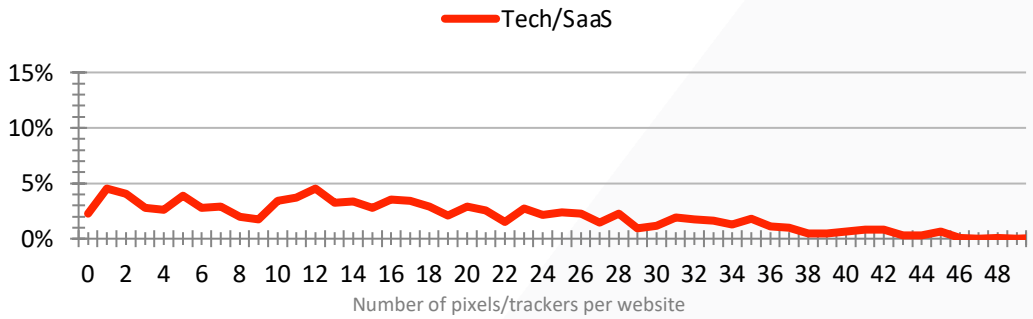


Figure F1-8: Distribution of percentage of analyzed websites over number of trackers

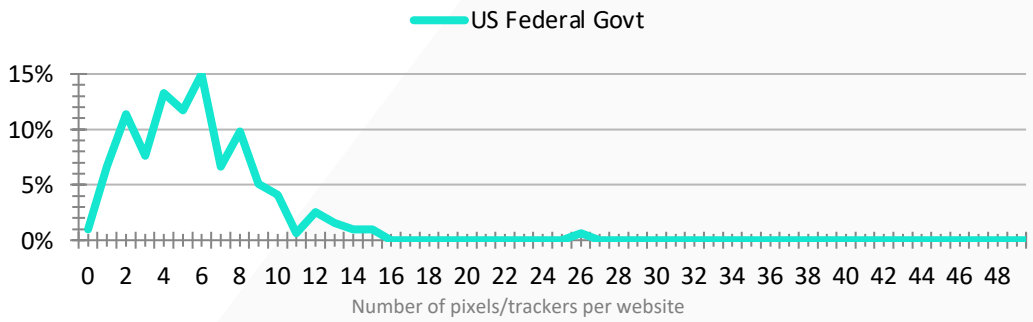
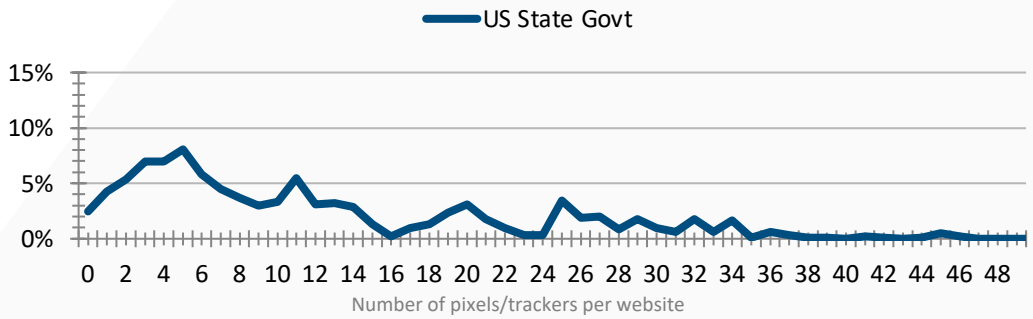


Figure F1-9: Distribution of percentage of analyzed websites over number of trackers



Finding #2: Pixels/Trackers are present on mission-critical webpages increasing the likelihood of risks

Figure F2-1 shows the degree to which pixels/trackers are present on webpages that are performing login and registration functions and have ability to access what users are typing into forms. Ideally, the number of such instances should be close to 0 on a company's mission-critical web pages.

Figure F2-1: Percentage of websites with pixels/trackers on mission-critical pages by sector

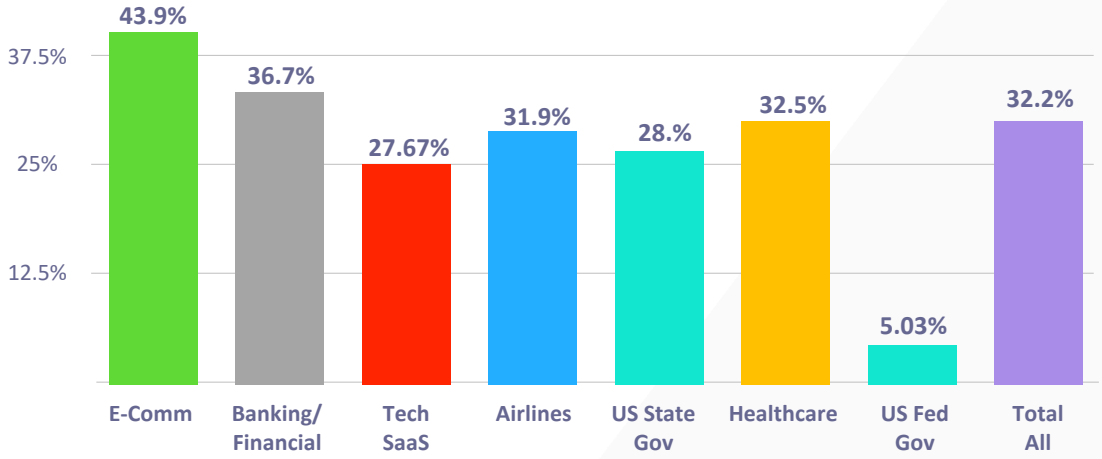


Table F2-1 shows the degree to which pixels/trackers are present on webpages that are performing login and registration functions are actually reading IAM (identity and access management) and/or PII (personal identity information) from user input fields into data fields of the pixels/trackers (ordered most to least). Ideally, the number of such instances should be 0 on a company's mission-critical web pages. That would be the case if the pixels/trackers were not on these web pages.

Table F2-1: websites with pixels/trackers collecting user data on mission-critical webpages
(e.g., webpages with login, account creation, registration, or credit card processing functions)

Sectors	Login and/or reg webpages with pixels/trackers		Login and/or sign-up/registration webpages handling IAM or PII data with pixels/trackers reading user input into form fields		
	Number of websites with such webpages	Number of such webpages	Number of mission-critical webpages with pixels/trackers reading user input into fields	Percentage of mission-critical webpages with pixels/trackers reading user input into fields	Percentage of websites with pixels/trackers reading user input into fields on mission-critical webpages
Financial Services & Banking	534	2,306	101	4.38%	3.00%
Healthcare & Telehealth	462	1,723	17	0.99%	2.17%
Technology & SaaS	536	3,706	58	1.57%	5.60%
e-Commerce	533	3,582	348	9.72%	15.95%
Airlines	342	2,020	136	6.73%	5.56%
US Federal Government	118	161	0	0.00%	0.00%
US State Government	346	2,122	31	1.46%	2.32%
Overall	**2,869**	**15,620**	**691**	**4.42%**	**5.86%**

Finding #2: Continued

Table F2-2 shows the extent to which pixels/trackers exist on websites and associated webpages with login and account creation functions (ordered most to least). Keep in mind, usernames, passwords, authentication codes, and possibly more are entered on these webpages. This user data can possibly be captured by these pixels/trackers.

Table F2-2: Websites with pixels/trackers on login webpages

Sectors	Number of websites with pixels/trackers on login webpages	Percentage of websites with pixels/trackers on login webpages	Number of login webpages with trackers	Average number of login webpages per website	Number of unique trackers on login webpages per website
Financial Services & Banking	158	36.66%	1,407	8.91	10.35
Healthcare & Telehealth	176	32.53%	431	2.45	5.13
Technology & SaaS	153	27.67%	558	3.65	7.86
e-Commerce	241	43.83%	1,455	6.02	13.04
Airlines	155	31.96%	1,225	7.91	7.35
US Federal Government	7.5	4.72%	41.5	5.53	3.73
US State Government	120	28.47%	639	5.33	6.15
Total/Average	**1,011**	**32.18%**	**5,758**	**5.69**	**8.70**

Similarly to the previous Table, Table F2-3 shows the case for websites and associated webpages with registration functions. First and last names, company names, email addresses, phone numbers, home addresses, SSNs, and other types of sensitive information are often entered on these web pages. As mentioned above, these pixels/trackers can potentially capture this user data.

Table F2-3: Websites with pixels/trackers on registration webpages

Sectors	Number of websites with pixels/trackers on registration webpages	Percentage of websites with pixels/trackers on reg webpages	Number of registration webpages with pixels/trackers	Average number of registration webpages per website	Number of unique pixels/trackers on reg webpages per website
Financial Services & Banking	203	46.98%	899	4.44	8.07
Healthcare & Telehealth	286	52.77%	1,292	4.53	3.12
Technology & SaaS	383	69.17%	3,147	8.23	3.04
e-Commerce	292	52.90%	2,127	7.3	10.46
Airlines	187	38.45%	795	4.26	6.05
US Federal Government	110	69.18%	120	1.09	0.25
US State Government	226	53.50%	1,334	5.91	3.17
Total/Average	**1,684**	**53.60%**	**9,712**	**5.77**	**5.11**

Finding #3: Pixels/Trackers transfer data to foreign locations around the globe

Table F3-1 shows the destinations of data being transferred by pixels/trackers collecting data from US-based websites.

Table F3-1: Top 40 countries receiving data (most to least)

Rank	Country	Number of unique data transfers	Percentage of transfers by Country (out of 7,092,114)	Associated with nation state surveillance/spying
1	United States of America	6,706,851	94.57%	
2	Canada	87,237	1.23%	
3	France	42,005	0.59%	
4	Ireland	38,790	0.55%	
5	Germany	32,172	0.45%	
6	U.K.	26,375	0.37%	
7	Russian Federation	16,299	0.23%	Yes
8	Netherlands	15,594	0.22%	
9	China *(People's Republic of China)*	12,540	0.18%	Yes
10	Australia	8,873	0.13%	
11	Japan	7,115	0.10%	
12	Hong Kong *(People's Republic of China)*	6,820	0.10%	Yes
13	Singapore	6,106	0.09%	
14	Mexico	5,751	0.08%	
15	Denmark	5,333	0.08%	
16	Sweden	4,766	0.07%	
17	India	4,647	0.07%	
18	Turkey	4,453	0.06%	
19	South Korea	4,365	0.06%	
20	Czechia	3,712	0.05%	
21	Poland	3,549	0.05%	
22	Greece	3,306	0.05%	
23	Saudi Arabia	3,039	0.04%	
24	Finland	2,801	0.04%	
25	Colombia	2,781	0.04%	
26	Brazil	2,545	0.03%	
27	Switzerland	2,417	0.03%	
28	Spain	2,400	0.03%	
29	Portugal	2,183	0.03%	
30	Panama	2,004	0.03%	
31	South Africa	1,737	0.02%	
32	Israel	1,577	0.02%	
33	Vietnam	1,419	0.02%	
34	Belgium	1,274	0.02%	
35	El Salvador	1,244	0.02%	
36	United Arab Emirates	1,256	0.02%	
37	Argentina	1,207	0.02%	
38	Romania	1,130	0.02%	
39	Pakistan	1,030	0.01%	
40	Lithuania	962	0.01%	

Finding #4: Pixels/Trackers are collecting and transferring data without first obtaining the explicit consent of visitors

Table F4-1 shows the extent to which pixels/trackers are collecting and/or transferring data prior to the explicit consent (e.g., cookie acceptance) of the website visitor, user, or customer. While a couple do not require actual consent for one reason or another, the consent is not explicitly made. In a few cases, actual consent when opening a webpage is not required as it is contained in the service agreement with the pixel/tracker; nonetheless, it is not explicitly made.

Table F4-1: Percentage of ownership of pixels/trackers by Top 10 companies

Company	Names of pixels/trackers	Percentage of all pixels/trackers	Percentage of websites with such pixels/trackers
Google	Google Tag Manager Google Analytics Google Remarketing Google Analytics Audiences Google AdWords DoubleClick YouTube	51.34%	90.24%
Microsoft	LinkedIn Ads AppNexus LinkedIn Analytics Bing Ads	14.95%	50.42%
Meta (Facebook, etc.)	Facebook Business Facebook Connect	11.99%	50.22%
Yahoo/Verizon	Yahoo	3.39%	27.31%
Adobe	Adobe Audience	3.09%	26.15%
Rubicon	Rubicon	2.96%	23.99%
Axicom (LiveRamp)	LiveRamp	2.58%	20.97%
The TradeDesk	theTradeDesk	2.22%	50.22%
ByteDance (TikTok, etc.)	TikTok Analytics	2.15%	7.41%
Contentsquare	HotJar	2.12%	2.22%

Finding #4: Continued

Figure F4-1 shows a sample report for a website where 21 pixels/trackers load and collect user information.

- No consent requested
- No consent given

Figure F4-1

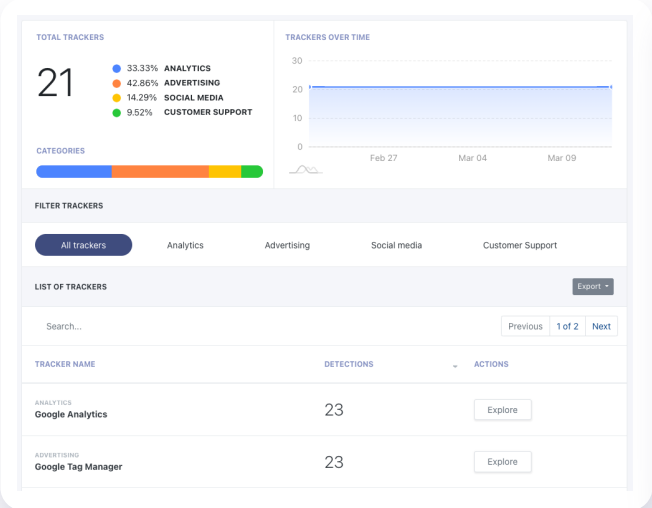


Figure F4-2

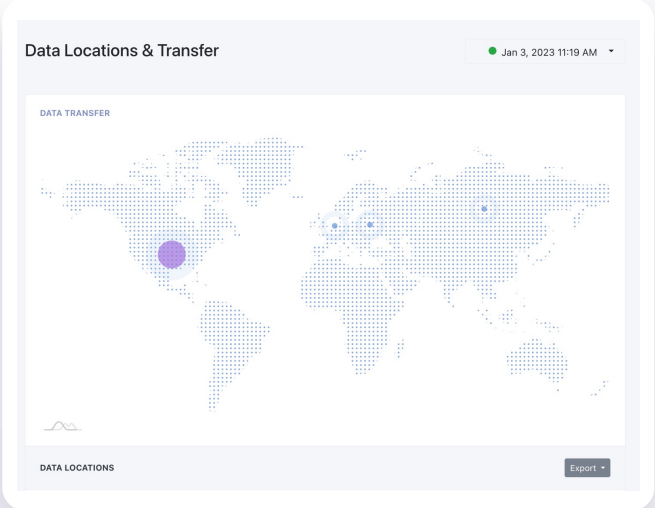
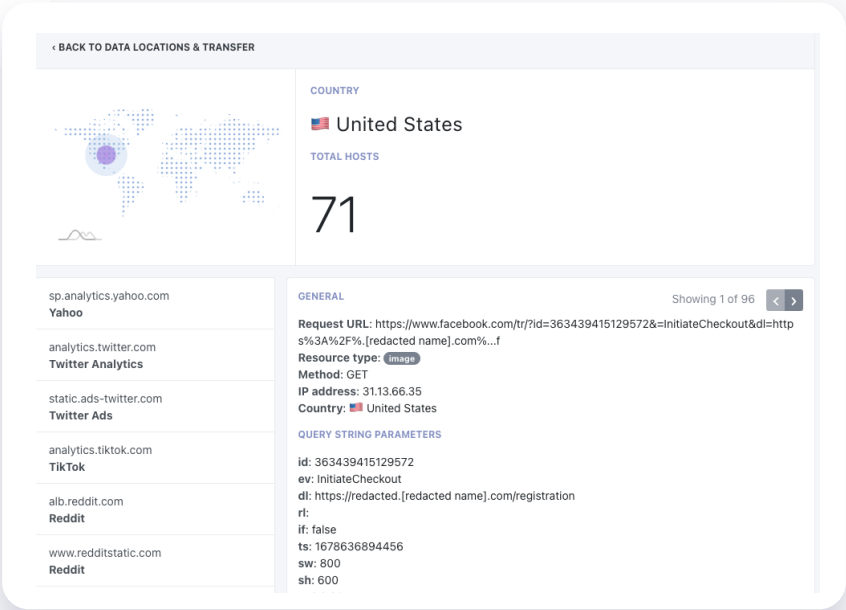


Figure F4-3 shows sample findings for website where pixels/trackers and scripts are transferring user data to 71 servers in the US with:

- No consent requested
- No consent given

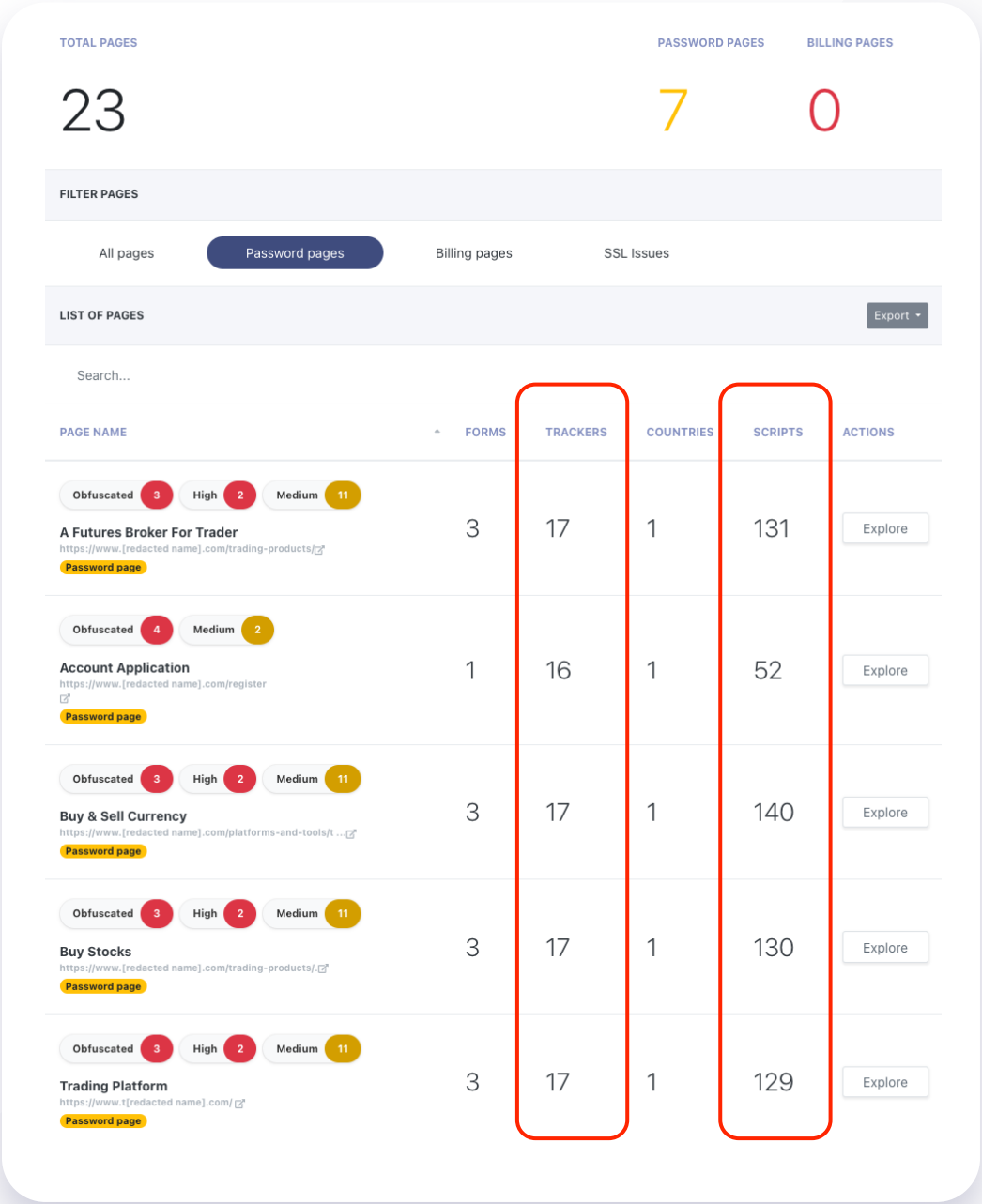
Figure F4-3



Finding #4: Continued

Figure F4-4 illustrates how the amount of pixels/trackers and scripts in supply chain code can vary significantly among different web pages. This is shown through the number of pixels, trackers, and scripts reported in the Trackers and Scripts columns. As a result, each web page that deals with sensitive user information may have its own specific privacy and security risks that need to be considered.

Figure F4-4



Finding #5: Pixels/Trackers are loading from domains banned by the U.S. Federal Government and various U.S. States

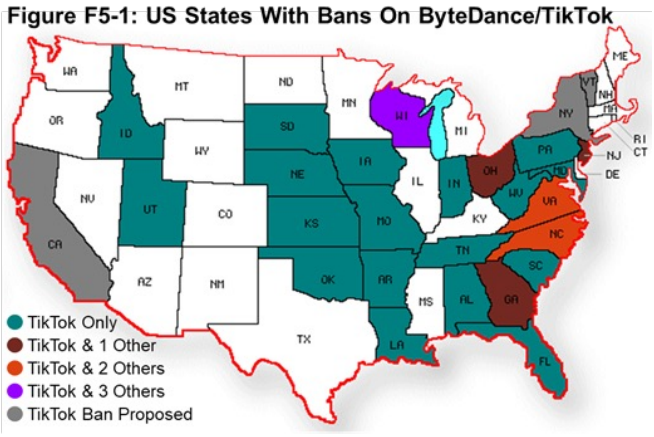
"[China can] manipulate content, and if they want to, to use it for influence operations."
- **FBI Director Chris Wray**

"To maintain the security of data owned by the state of Nebraska, and to safeguard against the intrusive cyber activities of China's communist government, we've made the decision to ban TikTok on state devices."
- **NB Governor Pete Ricketts**

"Protecting citizens' data is our top priority, and our IT professionals have determined, in consultation with federal officials, that TikTok raises multiple flags in terms of the amount of data it collects and how that data may be shared with and used by the Chinese government."
- **OH Governor Doug Burgum**

"South Dakota will have no part in the intelligence gathering operations of nations who hate us."
- **SD Governor Kristi Noem**

Figure F5-1: US States With Bans On ByteDance/TikTok



"Maintaining the cybersecurity of state government is necessary to continue to serve and protect Oklahoma citizens and we will not participate in helping the Chinese Communist Party gain access to government information."
- OK Governor Ken Stitt

Table F5-1: Banned companies by US Federal Government & State Governments (as of Jan 15, 2023)

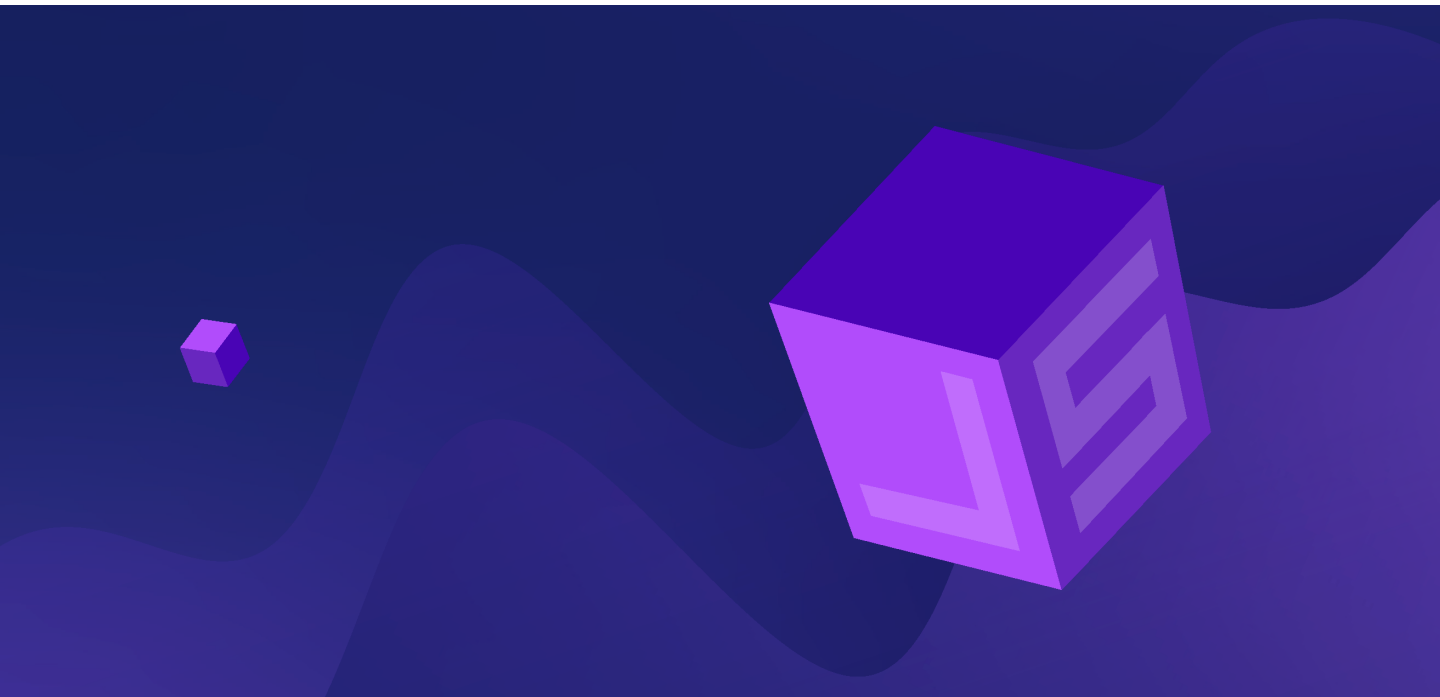
	US Fed Gov't	US States																												
		AL	AR	FL	GA	IA	ID	IN	KS	LA	MD	MO	NC	ND	NE	NH	NJ	OH	OK	PA	SC	SD	TN	TX	UT	VA	WI	WV
ByteDance/TikTok	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tencent/WeChat					✓								✓			✓	✓	✓									✓	✓		
BrothersNikolai/Telegram					✓																									
SinaCorp/Weibo																		✓												
DingTalk																		✓												
Alibaba/Huawei																✓	✓											✓		
Kaspersky																												✓		

Finding #5: Continued

Table F5-2: Percentage of websites by sector that use pixels/tracking tools and/or scripts/libraries that are associated with companies banned by executive orders; and/or send user data to companies banned by executive orders.

Table F5-2: Percentage of websites by sector that use pixels/tracking tools and/or scripts/libraries that are associated with companies banned by executive orders; and/or send user data to companies banned by executive orders

Sectors	Percentage of websites
Financial Services and Banking	4.87%
Healthcare and Telehealth	1.76%
Technology and SaaS	7.78%
e-Commerce	20.78%
Airlines	6.70%
US Federal Government	0.00%
US State Government	7.11%



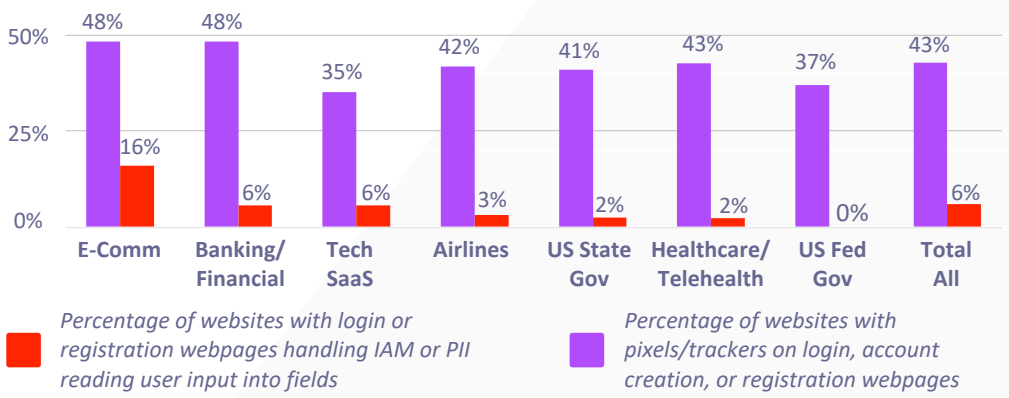
Risks

By identifying these and other risks, businesses can develop strategies and plans to mitigate or manage them, thereby reducing the likelihood of negative impacts on the application, the data it processes, and the business as a whole. It also helps organizations to maintain their reputation and credibility, prevent financial loss, and protect their customers' data.

Risk #1: Privacy compliance violations & penalties

Finding #2 ("Pixels/Trackers are present on mission-critical webpages which increases the likelihood of risks") showed pixels/trackers are present on mission-critical webpages where sensitive personal information entered by a website visitor is read and transferred. Moreover, Finding # 3 ("pixels/trackers transfer data to foreign locations around the globe") showed that this is done before receiving the visitor's explicit consent.

Figure R1-1: Websites with pixels/trackers on mission critical web pages - in order of greatest risk exposures



Such data transfers can constitute violations of a number of regulations and standards for IAM (identity access management) and/or PII (personal identifiable information) these include:

- GDPR: fines up to €10 million based on the severity of the infringement (which also applies to US companies providing services to EU customers)
- CCPA: $2,500 for each violation or $7,500 if intentional for companies doing business in California
- PCI-DSS: fined $5,000 to $100,000 per month depending on the state of your non-compliance.

The average cost of a breach for organizations with high levels of compliance failures was $5.57m according to IBM's 2022 Cost Of Data Breach Report.

In the event where the collected and transferred data are user credentials, there is the additional risk of intrusions and then further attacks conducted from the inside. According to the Verizon 2022 Data Breach Investigations Report (DBIR), the use of stolen credentials accounted for 67% of web application intrusions and 42% of system intrusions. In addition, the DBIR reported that web applications account for 56% of attacks on assets.

Risk #2: TikTok is often present whether or not the TikTok App is deleted and likewise for others banned by governments

TikTok, as well as others, use more than mobile apps on devices to collect and transfer data about users. Other methods include specifically pixels/trackers. Since pixels/trackers are part of the code that loads into the browser from a website. For illustrative purposes here, consider it a client-side "application."

Finding #5 ("pixels/trackers are loading from domains banned by the US Federal Government and various US States") showed that, while governments banned apps and the companies that own them from government devices, the client-side "applications" (i.e., pixels/trackers, scripts, and/or libraries from those same companies) are also loaded to user sessions from those banned apps and companies. These pixels/trackers may be loaded directly in the website html and other code or loaded indirectly within 3rd party software chains.

While one would expect that such pixels/trackers from companies would definitely not appear on agency websites of the governments that banned those same governments, Table R2-1 shows that is not the case for those analyzed from US State Governments.

Table R2-1: Percentage of government websites that use pixels or tracking tools that are owned by companies banned by executive orders

Sectors	Number of websites	Percentage of websites
US States	30	7.11%
US Federal Government	0	0.0%

Clearly, this risk is not limited to government websites alone; it can exist with any website. Namely, a visitor, user, or customer of a website can delete or block an app which is undesirable to them - e.g., TikTok, Facebook, Snapchat, Google, etc. - however, pixels/trackers from the company that owns the app still can load, capture, and transfer data via the browser of the user.

Risk #3: Brand/image damage & lost business

Finding #2 ("Pixels/Trackers are present on mission-critical webpages which increases the likelihood of risks"), Finding # 3 ("pixels/trackers transfer data to foreign locations around the globe"), and Finding #4 ("Pixels/Trackers are collecting and transferring data without first obtaining the explicit consent of visitors") make clear the possibility of a data breach is high - one associated with sensitive and/or privacy data of users.

After becoming public, a data breach of a company can cause reputation damage that negatively impacts the company's brand and image. This in turn can result in loss of both existing and prospective customers as well as similar results in stock markets. In addition, revenue losses can occur from business disruption dealing with the breach.

Table R3-1 shows the level of risk of a sensitive and/or privacy data breach for sectors that historically suffered such repercussions from a data breach when made public. Lost business was the largest share of data breach costs for 5 years in a row (2016-2021) according to IBM's Cost Of Data Breach Report.

Table R3-1: Websites with pixels/trackers collecting privacy data on mission-critical web pages - for sectors particularly impacted when data breaches become publicly known

(e.g., webpages with login, account creation, registration, or credit card processing functions)

Sectors	Number of of websites with login or reg webpages handling IAM or PII data with pixels/trackers reading user input into fields	Percentage of websites with login or reg webpages handling IAM or PII data with pixels/trackers reading user input into fields
e-Commerce	85	15.95%
Financial/Banking	16	3.00%
Healthcare/Telehealth	10	2.17%

Risk #4: Pixels/Trackers transfer data to nations of concern

Finding #3 (“pixels/trackers transfer data to locations abroad”) identified Russia, China, and Hong Kong as destinations for data transfers by pixels/trackers for the analyzed websites. These countries are nation states associated with possible spying, state surveillance, and computer system intrusions.

Table R4-1 lists the three countries (most to least) in terms of the # of transfers made specifically to domains/servers in those countries.

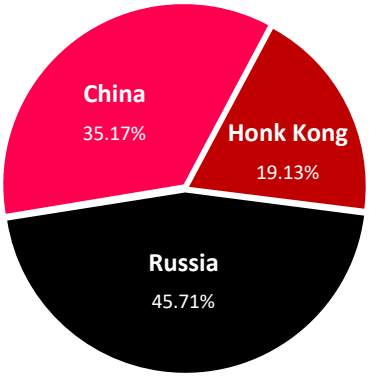


Table R4-1: Nation states of concern receiving data (most to least)

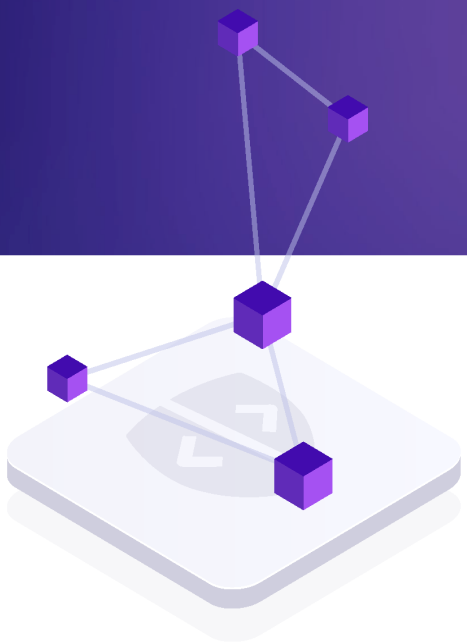
Country	Number of transfers	Percentage of transfers
Russia	16,299	45.71%
China	12,540	35.17%
Hong Kong	6,820	19.13%
Total/Average	35,659	100%

Risk #5: TikTok/Bytedance & Facebook/Meta are compliance risk concerns

Finding #1 (“pixels/trackers are common and abundant”) shows ByteDance (e.g., TikTok, etc.) and Meta (Facebook, Instagram, etc.) and other platforms are collecting and transferring data. Finding #2 (“pixels/trackers are present on mission-critical webpages which can increase the likelihood of risks”). Coupled together presents a risk that these platforms can collect and transfer privacy and sensitive data from visitors, users, and clients of websites across all sectors.

Finding #5 (“pixels/trackers are loading from domains banned by the US Federal Government and various US States”) would suggest that TikTok is a major concern in this regard. Given the nature of the internet, websites, and web applications, the same is happening pretty much in all sectors. Additionally, all websites and companies should be concerned about these type of risks.

Summary



The findings and risks highlighted in this report should provide important insights and facts to application security teams, compliance officers, cyber risk managers, CISOs, etc., to help comply with growing privacy regulations and compliance concerns. Realities associated with pixels/trackers, including those from TikTok and Facebook, should now be clear. In addition to these, the observations, concerns, and remediations below should aid in taking the next steps.

Top 3 Notable Observations

1. TikTok can be present on a website in pretty much any sector in the form of TikTok pixels/trackers. There is no strong reason for TikTok pixels/trackers (or any TikTok code) to have access to mission-critical user data on healthcare, government, or financial websites. For other industry sectors, it may be necessary to make a judgment call on the value of TikTok advertising tools and risks of their pixels/trackers.

2. Privacy and sensitive data from a user of a website can be captured and transferred by pixels/trackers prior to the user explicitly giving any permissions, including accepting cookies. These pixels/trackers load into the user's browser along with everything else to populate the webpage. In many cases, the pixels/trackers immediately start executing and have little to nothing to do with the immediate business of the website owner.

3. Data captured by pixels/trackers from US-based websites is predominantly sent to domains in the US. However, this does not preclude malicious actors from doing the same and then moving the data from a US-based server to a foreign location to avoid evident detection.

Top 3 Key Concerns

1. Pixels/Trackers load into certain web pages where they gain full access to sensitive user data. These include web pages that perform a login access, account creation, registration, and credit card processing processes. Capturing and transferring user data on these pages, for even legitimate advertising, is unnecessary and creates undesirable risks.

2. Locations within nation-states known for spying and surveillance are receiving data from pixels/trackers loading from US-based websites; these include China and Russia. Companies operating in these countries are required by law to grant access to the governments of those countries any and all of their data. The companies must when requested, forward that data to the respective government - which would include data transferred by pixels/trackers.

3. Companies banned by the US Federal Government and over half the US State Governments are actively receiving data from those companies' pixels/trackers, which are loaded into browsers of users accessing US-based websites, including TikTok pixels/trackers.

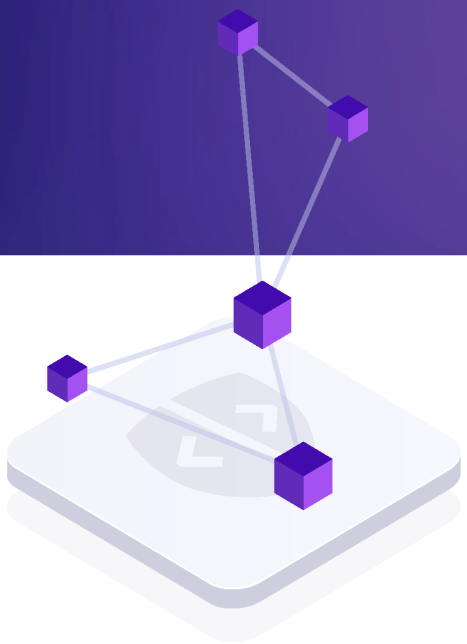
Top 3 Remediations and Preventive Measures

1. Control or remove suspect pixels/trackers from the code in the webpages of your website and, most importantly, all pixels/trackers from mission-critical webpages or ensure pixels/trackers do not have access to sensitive user data (e.g., those with functions for login, account creation, registration, credit card processing, etc.).

2. Add client-side software supply chain to your risk management program (so to prevent pixels/trackers from getting on the webpages where they don't belong and problematic pixels/trackers from getting on any web pages).

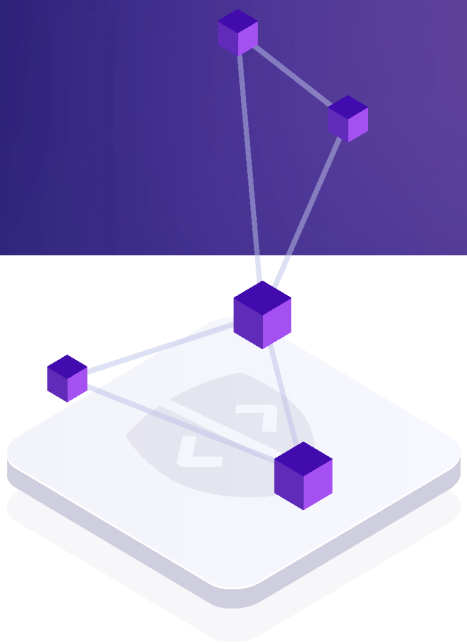
3. Include client-side application protection in your web application security considerations as well as your overall cybersecurity strategy and program.

Resources



- **“Out Of Control”: Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies**
  - STAT & The Markup (December 13, 2022)
- **Sweeping Spending Bill Would Ban TikTok On Government Devices**
  - The Washington Post (December 20, 2022)
- **Why Are Governors Turning On TikTok**
  - Wall Street Journal (January 15, 2023)
- **IBM’s Cost of Data Breach Report 2022**
  - IBM
- **Verizon Data Breach Investigations Report [DBIR] 2022**
  - Verizon Communications

Glossary



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 the residents of California, USA.

Chatbot - a computer program designed to simulate a 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 are 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.

Glossary

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 - data processed, organized, structured or presented in a given context so as to make it useful.

Informed Consent - permission for something to happen that 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 collection of functions which 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 freedom from being observed or disturbed by other people and having control relating to the use of your own data.

Glossary

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

Sub-processor - a processor that makes up a part of a larger processor. Contractual requirements between a 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 the 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.

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 sites.

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 an attack with unintended code execution.

Supply chain attack - A supply chain attack, also called a value chain or third-party attack, occurs when your system is infiltrated 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 to keep track of website visitors using software tools.

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

Web Apps or 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.

Additional Glossaries

NICSS Glossary of Common Cybersecurity Terms:
https://niccs.us-cert.gov/about-niccs/glossary

Glossary of Privacy Terms (IAPP)
https://iapp.org/resources/glossary

Common Software and Application Security Terms Explained
https://blogs.grammatech.com/common-software-and-application-security-terms-explained