BEYOND CONSENT: ONLINE PRIVACY NEEDS BETTER TECH

LOKKER
POWERING PRIVACY

Improving Online Privacy Doesn’t Need More User Consent, Website Owners Need Better Tools

It’s 2022, and it’s time to evolve web privacy beyond complex policies and cookie consent management. We need to empower companies with software to operationalize effective privacy practices.

In this report, we’ll share the latest insights of Lokker’s Privacy Edge™ analysis of 90,000+ websites across 11 industry segments and the trends that are impacting customer data privacy. With greater visibility to the threats, and state-of-the-art tools to proactively manage your relationships, you can power privacy and evolve your policies with effective practices to become a leader in providing safer, more private experiences for your customers.

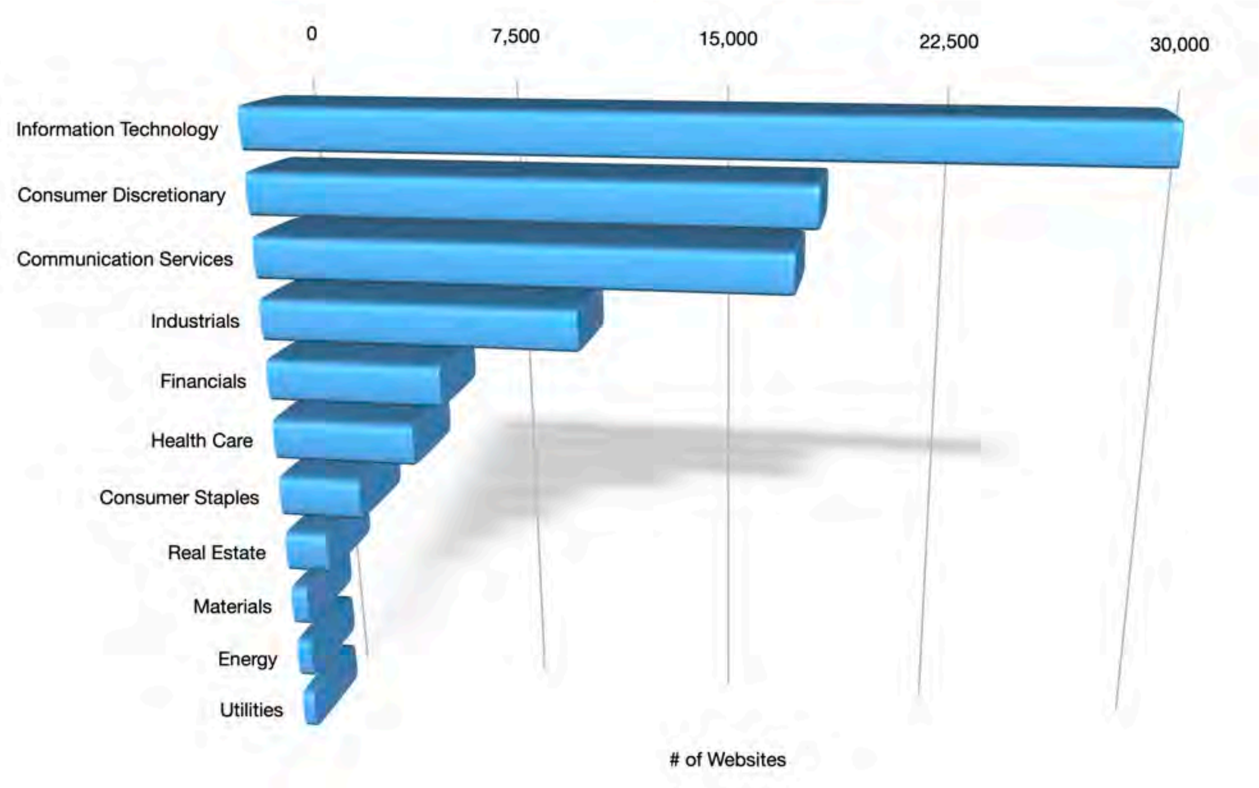
While consent is an essential step in meeting customer demand for greater protection of their personal information, managing first- and third-party cookies only addresses a small percentage of risks of online data exposure. **On average, the homepage of a Fortune 1000 website has 135 third parties making requests for data** via trackers and Javascript that lead to unauthorized data sharing. These aren’t cookies. These are clever, hidden scripts that you can only detect from the web browser, and they can contain privacy threats that you can only block from the browser through better technology.

The job of protecting your users’ web privacy is often owned by a diffuse group. Whether you’re the General Counsel, Chief Information Security Officer (CISO), Chief Privacy Officer (CPO) or Chief Marketing Officer (CMO), you may be responsible for data privacy controls. But do you have visibility, beyond cookies, to all of the 3rd, 4th and Nth parties that are collecting information from your website visitors?

Over 90,000 Sites Inspected Turned Up 130 Million Third-party Requests That Create Privacy Risks

Modern website architecture increasingly relies heavily on third-party cloud services. This includes everything from essential functionality and analytics to dynamic content generation and tracking for advertising and retargeting. These third-party solutions also have relationships with downstream partners that may be collecting, re-packaging, or re-selling your customers' data. With increasing web traffic, transactions, and site registrations, your customers' data is proliferating among data brokers that are building models and profiles from your efforts.

Lokker Analysis of over 90,000 Global Websites

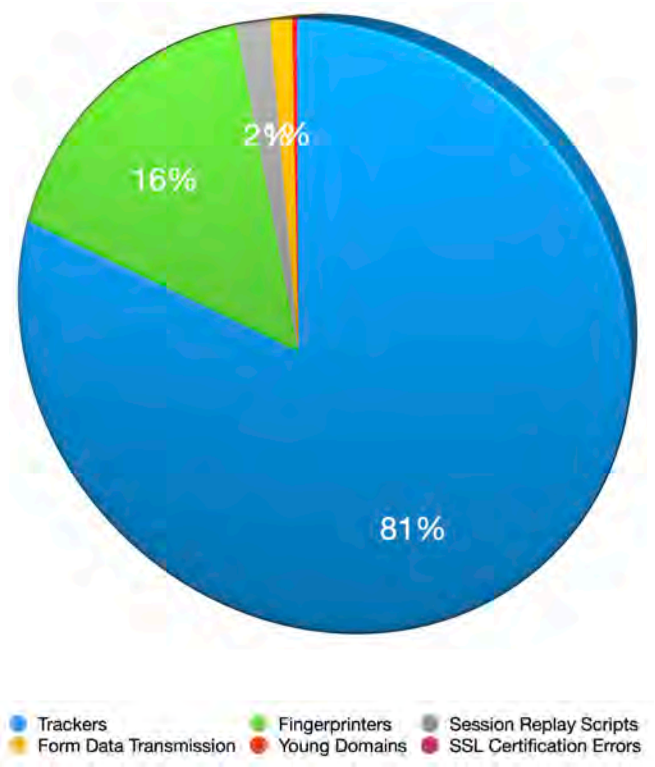


Lokker's Privacy Edge™ analysis of thousands of websites from around the world identified a broad set of 'invisible' activities that have a major impact on website visitors' privacy. In order to simplify the inspection of these risks, we focus on 6 categories of third-party activity:

1. Trackers
2. Fingerprinters
3. Young Domains
4. SSL Certification Errors
5. Session Recorders
6. Data Skimmers

The goal of this inspection is to enable our customers to see the depth and breadth of activity taking place below the surface of their web properties so they can control with WHOM they are sharing information and WHERE the data is going. With greater insight, we can all make more intelligent decisions on how we build and manage our websites while also protecting our customers' personal information.

Third-party Privacy Risks



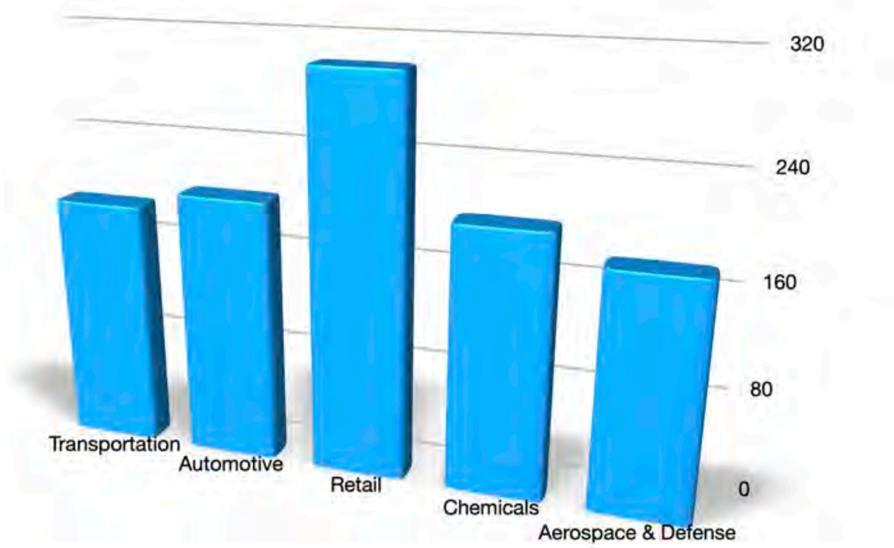
Over 28,000 Website Scripts Share Data with China and Russia

Data sovereignty is one of the key issues that regulations like GDPR and CCPA attempt to enforce. Yet, without proper tools in place, many organizations are unable to manage the effort to control with whom and to which countries the data may be flowing. In our recent research, we investigated over 90,000 websites around the world and uncovered almost 30,000 instances of foreign domains (scripts originating in countries outside of the website's home country) that are requesting and collecting web visitor information. And, no surprise, Russian and Chinese hosted domains are among the top offenders. The surprise, however, is that these scripts are operating out of sight of the website operators that host them.

Lokker is continually analyzing tens of thousands of websites across the Internet – Alexa's top 100,000 sites, the Fortune 1000, the top 5,000 companies by market cap are just a few of the sources of our website data. Our proprietary tools make the invisible visible. We identify the breadth of third-party scripts, trackers, and fingerprinters that are collecting and sharing data from website visitors to identify potentially malicious scripts. In addition to the known third-parties (like Google Analytics and Facebook trackers), we also uncover a massive list of unauthorized downstream parties that have relationships with a company's vendors that may use customer information without consent.

On Average, the Fortune 1000 companies have over 130 third-party resources collecting customer data on their websites

Lokker's inspection of the Fortune 1000 companies' websites has unearthed myriad trackers, fingerprinters, and Javascripts that are siphoning off customer data. In segments such as Transportation, Automotive, Chemicals, Aerospace & Defense, the numbers soar to over 200. Retailers top the list with over 300 external resources gathering and re-distributing consumer website



# of third-party scripts/trackers per industry

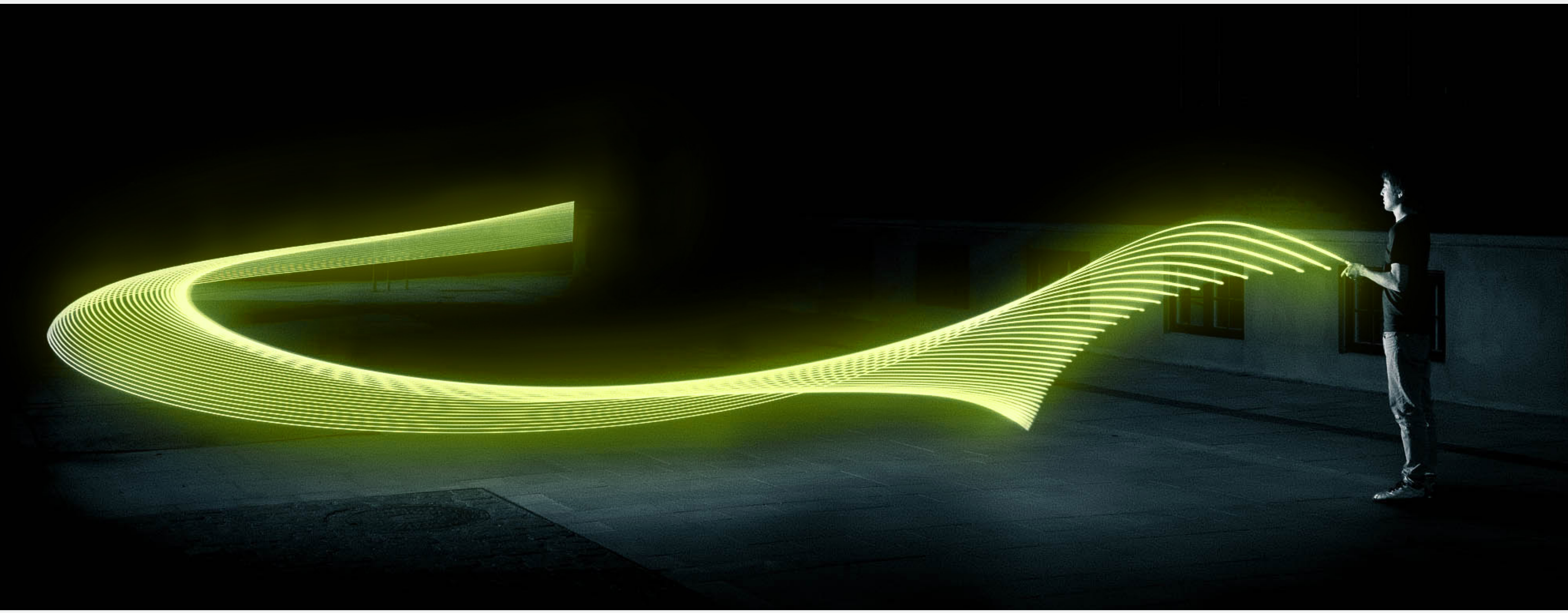
Data Skimming in Financial Services and Healthcare Needs Immediate Attention

Whether from on-site search, registration forms, or purchasing processes, site visitors' data is being skimmed from 'secure' pages. **Of 127 Financial Services sites evaluated, 21% were found to have hidden third-party scripts sharing user-input data.** Some sites had as many as 643 external parties peering in on their website activity and there were 33 instances where the data was being requested from domains in Russia or China.

Healthcare companies, from labs to insurance to pharma, had as many as 377 external parties fingerprinting or tracking data from site visitors. Not only is this alarming given the efforts of these companies to comply with regulations, but the sensitive nature of their services exposes very personal information of their customers. Over 25 of these companies also had form data being shared with downstream data collectors.

1,200 Session Recording and Replay Tools Create Privacy Risk

Most modern sites, while in development, use advanced tools to record activities of their site visitors to help improve the customer experience and optimize site features. However, hackers use these tools to capture personal data (usernames, passwords, financial information, phone numbers, addresses) as users are completing forms on those sites.



This data is then used to enrich profiles of previously anonymous site visitors, packaged and re-sold to data brokers. Our evaluation identified 1200 instances of sites with screen or session recording in place on their live, public websites.

23% of Retail and eCommerce Companies Share Web Form Data

The most advanced efforts to drive traffic and convert visitors to purchasers have also led to broad (and deep!) threats to consumer privacy. An examination of the Fortune 1000 and top 5000 companies (by market cap) revealed an average of 147 external resources collecting user data. For some sites in the Retail sector, Lokker has found as many as 530 3rd-, 4th- and more parties requesting data including location, IP address, browser history, and other fingerprinting data. Most alarming, this sector also leads all categories with a whopping 23% of sites sharing data from the forms on their sites.

The Honeypot That's Not So Sweet

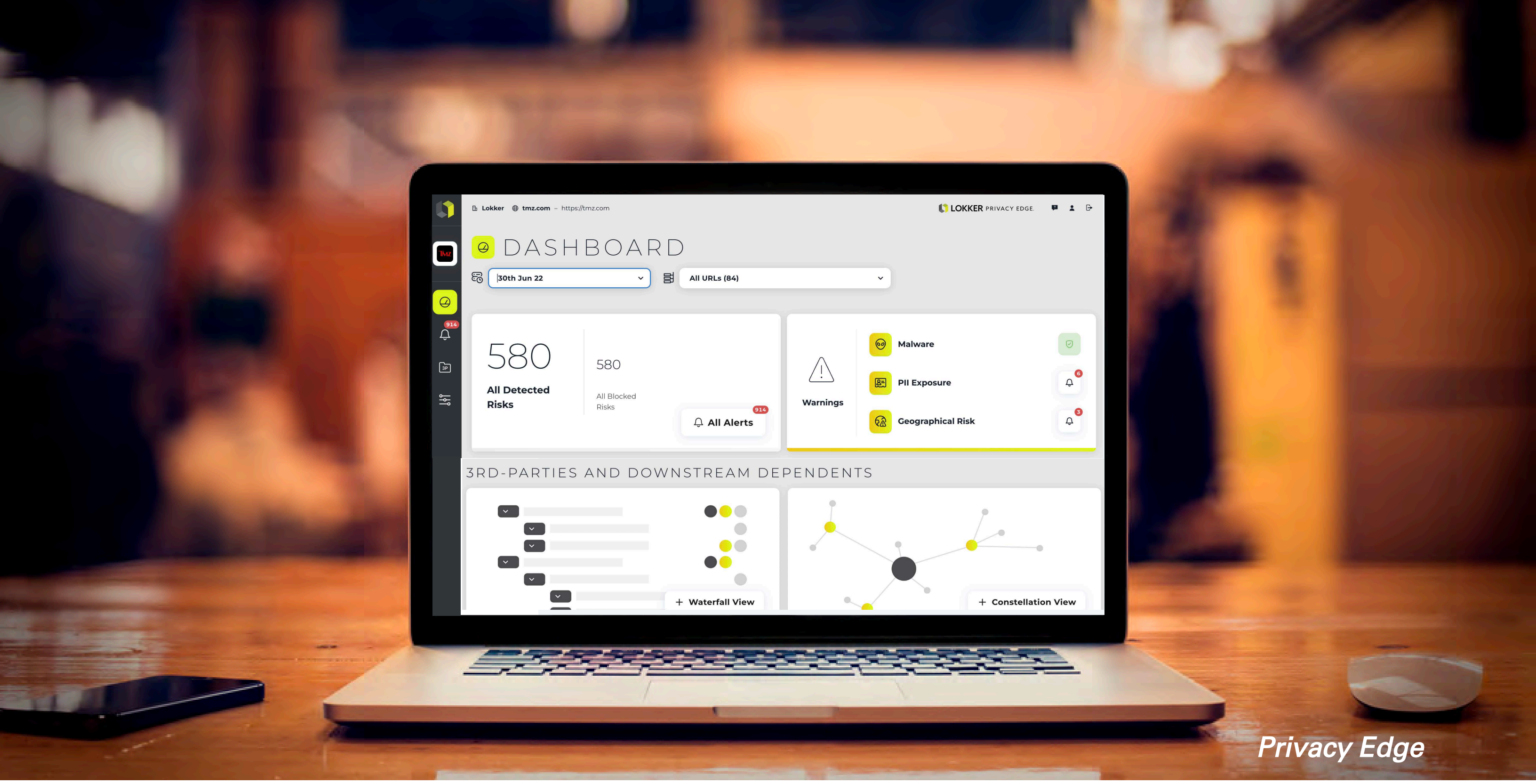
In addition to our evaluation of global websites referenced in this paper, Lokker has also conducted an experiment to see what happens to form data entered on webpages across 155,000 sites. This 'honeypot' approach used a unique email identifier that we tracked to see where the email goes downstream from the site on which it was entered.

Across all the sites where we entered our unique email address, we received 3,116 emails from unexpected senders, meaning they didn't come from the site where we entered the information. Thus, all the spam we are all bombarded with. These emails originated from 649 domains that we did not visit.

So what?

Well, if the information you are putting into a form on a webpage for Company X is being shared with external parties and you get a solicitation email from Company Y, not only does this indicate abuse of data sharing, but likely violates Company X's privacy policy and, worse, compromises trust between Company X and their customer.

Now imagine if you put personal information (social security #, phone number, or credit card information) into a form, and that is being shared with multiple third parties with whom you never intended to share that information.



Privacy Edge

The Internet is broken. Let's fix it.

This isn't all meant as a scare tactic or as dramatic evidence that the Internet is broken (but, it is, clearly).

It does, hopefully, shine a light on the amount of internet activity that is occurring 'behind the scenes' of the customer experience. It highlights the flaws of the current web infrastructure that create a mountain of challenges for privacy professionals attempting to protect consumers' privacy. And none of this has to do with 'cookie consent.' The data outlined in this report are intended to bring awareness to corporations that their websites need to be fixed. Online privacy isn't about regulatory compliance nor asking users permission to exploit their data. While cookie consent management approaches attempt to bring greater awareness to consumers, what are we actually asking them to consent to? Should we even be asking?

At Lokker, we propose that website owners proactively take responsibility for upholding privacy and managing the data being transmitted to and from their sites, well before asking their customers to consent to the tracking and data collection taking place. And, we are committed to enabling companies to make a huge leap forward in their privacy practices with better insight and better tools.

We have developed our Privacy Edge™ tools to not only surface these risks but provide companies with easy-to-implement software tools to control the third-party scripts running throughout their websites. And, given the dynamic nature of web publishing, each new visitor, each new page request, each new feature added to the site, introduces new data privacy vulnerabilities that should be monitored and controlled.

---

*For more information about our data, emerging privacy risks, and how Lokker's Privacy Edge™ can help you mitigate the third-party risks on your site, contact Jeremy Barnett, Chief Commercial Officer at **jeremy@lokker.com***

LOKKER
POWERING PRIVACY