Cybersecurity Law Report cslawreport.com

Jan. 31, 2024

Tech Meets Legal

Tracking Technologies: A Deep Dive on What They Are and How They Work

By Dan Frechtling, *Boltive*; Matt Pollard, *Slalom Consulting*; Leslie Shanklin, *Proskauer*

The ancient version of tracking began as footprint and scent detection to aid hunting. It is now powered by satellite uplinks and mobile data telephony to aid wildlife migration mapping.

Online tracking is evolving just like its offline predecessor. While prehistoric tracking was essential for survival, online tracking is essential to B2C business models and many B2B models. Tech evolution is happening both in response to and, in many respects, independent of changing legal mandates. The complexities presented by these ever-shifting sands are numerous.

Online trackers will never be eliminated, but the massive changes in societal attitudes and laws about privacy mean they must be governed. Understanding their forms and methods is the first step.

This second article in a four-part series on tracking technologies takes a deep dive into the technologies that enable the type of digital data collection that is most commonly referred to as "tracking," but which some constituents, including regulators, privacy activists and plaintiffs' counsel, are increasingly labelling "commercial surveillance." Part one looked at the history of legal regulation around online tracking technologies and examined use risks that organizations across the digital ecosystem must consider. Part three will offer a practical governance roadmap for managing digital tracking, and part four will focus on compliance challenges and solutions, including those specific to the advertising industry.

See "IAB Unveils Multistate Contract to Satisfy 2023 Laws' Curbs on Targeted Ads" (Feb. 22, 2023).

Why Are Tracking Technologies Used?

Essential Functions of a Digital Service

Tracking technologies serve a wide array of purposes on websites, mobile applications and other internet-connected devices and services. The much-maligned cookie in its earliest days was designed as a simple means to know if someone had previously visited a website and to enable emerging e-commerce functionality, such as allowing users to save items in a shopping cart. Tracking technologies continue to enable a multitude of essential features and functions on digital services, such as saving items and language preferences. They also support other important functional purposes, such as monitoring page and video load times and crashes, and protecting users by monitoring the security of online services and preventing fraud. Most of these "essential" uses of tracking technologies have been accepted conceptually by regulators, but as discussed in part one of this series, there are many legal nuances to navigate even with trackers that support the functioning and security of a digital service.

Measurement

Trackers also provide important measurement functions. Just as any brick and mortar business needs to know how many people visit its shop on a given day and what products they purchase, website and app analytics provide insights into number of visitors, what regions of the country or world those visitors come from, and what content and products have the greatest degree of interest and engagement. All of this information is essential to allowing businesses to best adapt to consumer interests and needs and to ensure their websites are able to handle the volume of traffic and allow users to easily find what they are looking for.

In the area of digital advertising, trackers measure whether and how users interact with ads, which allows digital publishers and advertisers to reconcile the money owed for a particular digital advertising campaign and provides essential data on ad effectiveness. From a measurement perspective, digital advertising trackers also enable "frequency capping," preventing overexposure of ads to the same user, enhancing user experience and ad effectiveness. Marketers also rely on trackers to measure the effectiveness of email marketing campaigns by providing insights on opens and clicks.

Content Personalization

By giving digital businesses insights into what consumers are most interested in when they visit a site or app, tracking technologies allow businesses to tailor the content, products or services presented to a consumer or group of consumers in a way that is most likely to meet users' expectations, leading to a more satisfied and engaged consumer. By monitoring a consumer's behavior over time and across not just the publisher's website but a variety of digital services, tracking technologies allow businesses to build rich profiles on users and enable hyperpersonalized content experiences and also, as discussed below, targeted advertising.

Ad Personalization and Targeting

The final principal use of tracking technologies, and that which has garnered the greatest degree of regulatory and consumer concern, is highly personalized targeted advertising and marketing. As with content personalization, the data collected via trackers enables marketers to create detailed user profiles and facilitates targeted marketing strategies, enhancing user engagement and conversion rates.

Digital tracking technologies also underpin programmatic advertising. Through automated data analysis, trackers ease the buying and selling of ad space in real time, making advertising more efficient and cost-effective.

Moreover, trackers facilitate social retargeting. They identify users who have interacted with a brand website or app and serve those individuals with targeted ads on social platforms, increasing the chances that users will return to the brand and make a purchase.

See "Understanding Online Advertising Technology and the Pipeline Process" (Mar. 22, 2017).

What Are the Common Types of Trackers?

Three Popular Web Flavors

Just like flavors of ice cream, trackers have three predominant varieties but many alternative forms.

Pixels

Often invisible, pixel images come embedded in a website or email. When the recipient loads a website or opens an email containing a pixel, it sends a request to an external server. Pixels are particularly useful in tracking user behavior and conversions and are widely used in digital advertising to monitor campaign performance.

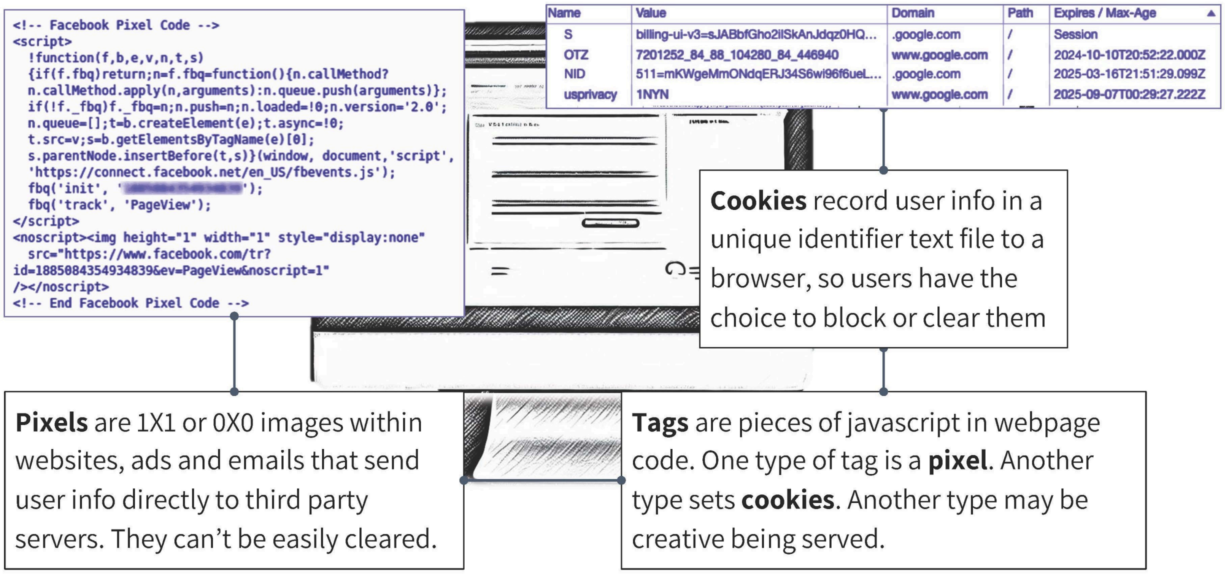
Tags

Also known as web and/or tracking beacons, tags are snippets of code inserted into a website's HTML. They collect data about visitors' interactions on the site. Tags enable website owners to optimize the user experience and track the effectiveness of various marketing initiatives. Sometimes the words "tags" and "pixels" are used interchangeably. To sort out this confusion, remember a pixel is a type of tag, but a tag is not always a pixel.

Cookies

Small data files stored on your device when you visit a website, cookies are designed to remember information about your visit. They can record login details, language preferences and other settings. Cookies play a crucial role in enhancing user experience by recalling user preferences and settings between sessions.

What Are Pixels, Tags and Cookies?



```
<!-- Facebook Pixel Code -->
<script>
  !function(f,b,e,v,n,t,s)
  {if(f.fbq)return;n=f.fbq=function(){n.callMethod?
  n.callMethod.apply(n,arguments):n.queue.push(arguments)};
  if(!f._fbq)f._fbq=n;n.push=n;n.loaded=!0;n.version='2.0';
  n.queue=[];t=b.createElement(e);t.async=!0;
  t.src=v;s=b.getElementsByTagName(e)[0];
  s.parentNode.insertBefore(t,s)}(window, document,'script',
  'https://connect.facebook.net/en_US/fbevents.js');
  fbq('init', '[redacted]');
  fbq('track', 'PageView');
</script>
<noscript><img height="1" width="1" style="display:none"
  src="https://www.facebook.com/tr?
id=1885084354934839&ev=PageView&noscript=1"
/></noscript>
<!-- End Facebook Pixel Code -->
```

Name	Value	Domain	Path	Expires / Max-Age ▲
S	billing-ui-v3=sJABbfGho2iISkAnJdqz0HQ...	.google.com	/	Session
OTZ	7201252_84_88_104280_84_446940	www.google.com	/	2024-10-10T20:52:22.000Z
NID	511=mKWgeMmONdqERJ34S6wi96f6ueL...	.google.com	/	2025-03-16T21:51:29.099Z
usprivacy	1NYN	www.google.com	/	2025-09-07T00:29:27.222Z

Cookies record user info in a unique identifier text file to a browser, so users have the choice to block or clear them

Pixels are 1X1 or 0X0 images within websites, ads and emails that send user info directly to third party servers. They can't be easily cleared.

Tags are pieces of javascript in webpage code. One type of tag is a **pixel**. Another type sets **cookies**. Another type may be creative being served.

© 2024 Boltive.com. All rights reserved.

Three Prevalent Categories of Pixels

Analytics: These pixels track who visits websites and gathers data such as geolocation, device used, referring URL and actions taken by the visitor. When embedded in ads, they can also count impressions.

Retargeting: These pixels are used to track website visitors who leave without completing an intended action, such as making a purchase. Retargeting pixels enable marketers to send reminder ads to these visitors, essentially re-engaging them with products or services.

Conversion: These pixels track visitors who have completed a purchase or a specific action on a website. For instance, a conversion pixel may fire when a visitor lands on an order confirmation page. They are vital in evaluating the success of ad campaigns.

Three Prevalent Categories of Cookies

Party: First-party cookies are set directly by the website the user is visiting. They are essential for user customization and storing information like language preferences and login state, and are limited to the domain of the website. Third-party cookies are often used by advertisers to track user behavior across different websites to create comprehensive user profiles for targeted advertising. Despite being anonymous, they have raised privacy concerns due to their extensive tracking capabilities.

Duration: Session cookies are first-party cookies that last only during the user's browsing session. They are vital for website navigation, remembering user actions and choices, like items in a shopping cart. Persistent cookies are stored on the user's device. They remember settings, personalizations and login credentials over a longer period, and facilitate a consistent user experience across multiple visits.

Specialization: These include HttpOnly cookies (mitigating cross-site scripting attacks), zombie cookies (regenerating after deletion), flash cookies (storing more data, harder to delete), super cookies (storing data in multiple locations) and SameSite cookies (adding security against cross-site request forgery).

Since Chrome initiated third-party cookie restrictions, the focus is expected to intensify on first-party cookies and newer, privacy-compliant cookies to provide necessary site functionalities and user experiences without compromising user privacy.

Trackers on Mobile Devices

The tracking landscape on mobile devices is distinct from traditional web tracking due to unique functionalities and technologies. The various methods underscore the expansive nature of tracking capabilities on mobile devices, each with its own set of challenges, benefits and privacy considerations.

Tracking Based on Unique IDs

Mobile Advertising IDs (MAIDs) are strings of digits assigned by operating systems like Android and Apple to mobile devices. They allow marketers to track individual devices and the behavior of their users. Unlike cookies in web browsers, MAIDs provide a more holistic view of user behavior across different apps and websites, and they remain active as long as the user uses their handset. MAIDs enable the creation of detailed user profiles for targeted advertising, linking devices to offline activities, and enhancing cross-device targeting and retargeting strategies.

SDKs in Apps

Software Development Kits (SDKs) in mobile apps play a pivotal role in facilitating tracking and adding functionalities without writing extensive code from scratch.

SDKs are widely used in app development due to their efficiency and functionality. They provide a suite of tools and APIs that help in integrating various features such as advertising, analytics and more into apps.

Despite their benefits, SDKs can be challenging to manage due to their lack of standardization. Configuration methods vary; some SDKs require configuration before coding, while others use dashboards. This variance can lead to inadvertent activation of targeted advertising features, often bypassing the visibility of compliance teams. Moreover, once implemented, some SDKs cannot be reconfigured, which poses challenges in the post-implementation stages, especially if app development is outsourced or contracted.

SDKs in apps also present auditing challenges. This becomes particularly problematic when SDKs update and default to targeted advertising settings. Such updates can occur without explicit knowledge or consent from the app development team, raising serious privacy concerns.

Despite those challenges, regulators expect companies to have full knowledge of their app data flows. The seriousness of this expectation is underscored by class action lawsuits, such as the case with Tim Hortons' use of the Radar SDK in Canada. This incident involved inadvertent transmission of geolocation data, highlighting the risks associated with third-party SDKs. Radar's stance was that customers were fully responsible for any misuse of location data, highlighting the need for vigilant management of SDKs in apps. A thorough list of SDK risks and claims has been published by Daniel Goldberg and Rick Borden of Frankfurt Kurnit.

Tracking by Webview Traffic to Third Parties

In mobile apps, webview is used to display web content within the app. Tracking in webview can occur when third-party websites or content is loaded, allowing these third parties to gather data about user interactions within the app. This type of tracking is less transparent to users, as it occurs within the app's environment, blending with native content.

GPS Tracking

GPS tracking in mobile devices is another significant area of data collection. It provides precise geolocation data, which can be used for various purposes, from location-based advertising to analytics. However, GPS tracking raises substantial privacy concerns, as it involves the collection of sensitive location data, necessitating stringent data protection measures and user consent.

Other Tracking Methods

Mobile devices also can be tracked using other methods such as Wi-Fi triangulation, Bluetooth beacons, and even device fingerprinting, which combines various device attributes to uniquely identify a user.

See "Benchmarking the Impact of State Privacy Laws on Digital Advertising" (Oct. 11, 2023).

How Do Trackers Get Added to Websites?

Trackers can be added to web pages manually. Tags are often integrated directly into a web page's source code. This method involves inserting small snippets of code, typically JavaScript, into the HTML. When a user visits the site, these scripts activate and start collecting data, such as user interactions, behaviors and preferences. This direct integration allows for precise tracking but requires technical know-how and access to the site's backend.

A more streamlined and increasingly popular approach is the use of tag management systems (TMSs) like Google Tag Manager and those from Tealium or Adobe. These systems simplify the process by allowing marketers to manage tags without needing to alter the site's core code. The process involves placing a single container tag in the website's header. From there, marketers can add, edit or remove various tracking tags through the TMS interface. This approach makes tag management more accessible and enhances site performance by reducing the impact on page load times.

How Are Trackers Triggered?

Upon a user's visit to a website, a browser loads specific code, including scripts and tags. These elements activate third-party services such as chatbots, anti-fraud protection or targeted advertising.

This kicks off a data exchange with third parties. When these third-party services are activated, they send information back to their respective servers. This data transfer enables these services to function correctly on the website. The types of information sent back can include user browsing behavior, preferences and interaction data, which are essential for third-party vendors to tailor their services for the site.

Information flows continuously. The passing of information is not one-time. Depending on the service provider, there's an ongoing back-and-forth of data between the website and the vendor's servers. This continual exchange allows for responsive services on the website, such as live-chat support or real-time fraud detection.

But it does not stop with the initial website. Cross-site consumer tracking is common. As users continue browsing the web, the same third-party vendors may offer services on other sites they visit. This interconnectivity allows these businesses to track activities across multiple websites.

For instance, an advertising service can track interests across different sites to build comprehensive user profiles, which are then used for targeted advertising.

See "France's Cookie Enforcement Against TikTok and Microsoft Highlights Common Compliance Missteps" (Jan. 25, 2023).

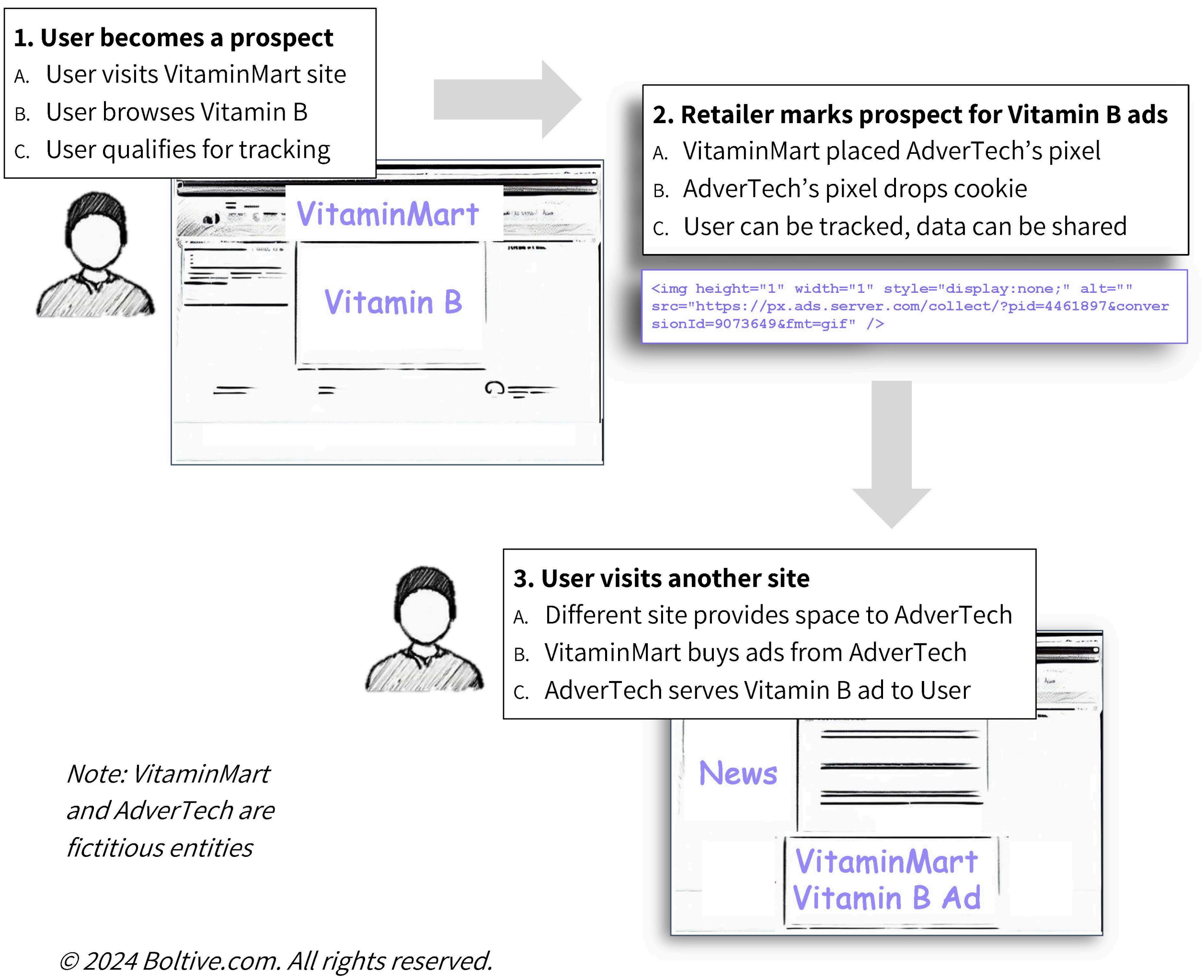
How Do Trackers Work Across Sites?

Conventional ad retargeting begins with the initial user interaction. A user visits an e-commerce website, let's say "Vitamin Mart." Next the user browses and interacts with the e-commerce functions. The user may shop various products, focusing on Vitamin B. They may even add the product to their cart without completing the purchase. Since the user has not made a purchase yet, the individual becomes a mark for retargeting.

Now the retailer can respond, often through partners that empower retargeting. Prior to the user's visit, "VitaminMart" has placed a pixel from an advertising technology company, say AdverTech. When the user visits the website, AdverTech's pixel drops a cookie in the user's browser. This cookie allows the user's behavior to be tracked across websites, enabling the collection and sharing of data for retargeting purposes.

Then the voodoo happens as the advertiser engages the user on different platforms. As the user browses other websites, the indivdual encounters spaces allocated to AdverTech for advertising. "VitaminMart" buys ad space from AdverTech. AdverTech then serves specific ads, like those for Vitamin B, to the user, based on the tracking data obtained from the pixel and cookie.

Putting It All Together: Trackers, Webpages, and Ads



1. User becomes a prospect

A. User visits VitaminMart site

B. User browses Vitamin B

C. User qualifies for tracking

2. Retailer marks prospect for Vitamin B ads

A. VitaminMart placed AdverTech's pixel

B. AdverTech's pixel drops cookie

C. User can be tracked, data can be shared

```
<img height="1" width="1" style="display:none;" alt=""
src="https://px.ads.server.com/collect/?pid=4461897&conver
sionId=9073649&fmt=gif" />
```

3. User visits another site

A. Different site provides space to AdverTech

B. VitaminMart buys ads from AdverTech

C. AdverTech serves Vitamin B ad to User

Note: VitaminMart and AdverTech are fictitious entities

© 2024 Boltive.com. All rights reserved.

Why Are There So Many Trackers and Related Vendors?

Piggybacking

The practice of "piggybacking" introduces a more complex layer to data sharing. Tag piggybacking binds additional parties. It occurs when one tag on a webpage loads another through server redirect. This process can lead to a chain of redirected requests and linked tags, each with access to the data collected by the original container tag. This chain can grow, introducing potential risks.

While tag piggybacking can streamline data distribution, it poses significant challenges. Data leakage is one risk. As more tags are added, more parties gain access to data, increasing the risk of unauthorized data access. In the era of strict data protection laws like the GDPR and CCPA, piggybacking tags can lead to non-compliant data collection, posing legal risks.

Tags also can harm performance. More tags mean more server requests, potentially slowing down the website. Excessive tags can also lead to data loss due to slow loading times or blocking of tags.

Monitoring and managing tag piggybacking is essential. Traditional TMSs might not detect these tags, especially if they are nested deeply. Advanced auditing platforms continuously analyze code changes, distinguishing potential threats and providing a comprehensive view of the tag ecosystem.

Network Requests

Network requests are another form of piggybacking. The process begins when a website or app, ready to display ads, initiates a request to its partner. This is the start of an auction, where coalitions of parties compete to determine who has the most comprehensive data about a consumer currently viewing a page. Often, the most complete profiles of consumers win the auction.

Many times, a single network request will trigger additional requests from other parties. This process can continue in a chain-like fashion, with each request leading to more requests from other entities.

In this interconnected system, it is common to see a dozen vendors actively involved in a single request, with the potential of hundreds of adtech vendors participating in the process overall.

The resultant data-rich, auction-enabled environment is what drives the effectiveness of modern digital advertising, but it also raises concerns about privacy and data management.

See "Why Companies Unintentionally Fail to Honor Opt-Outs" (Aug. 16, 2023).

What Are Probabilistic Methods?

Probabilistic identity resolution uses fuzzy matching to estimate the likelihood that two pieces of data belong to the same person.

Fingerprinting

A common probabilistic method is called device fingerprinting. It analyzes features such as the user agent string, time zone, language, HTTP request headers, OS, screen size, fonts and browser elements to create a unique identifier. Unlike cookies that are stored on the user's device, this information is maintained server-side in a database. Two fingerprinting practices are popular.

Browser-Based: These include using the device model, screen resolution, operating system, language and browsing history to create a browser fingerprint that identifies users each time they open their browser. Browser plug-ins may supplement information such as fonts and hardware elements.

Canvas: Using HTML5 coding for websites, this technique examines how a user's browser responds to graphical instructions, using the HTML5 Canvas element to draw an image and then analyzing responses from hardware and software configurations based on how the image is rendered.

Identity Graphs

Another typical probabilistic approach is identity graphs. These are collections of data points used to track users across multiple devices and platforms, creating a unified view of a user's online activity. The data for these graphs is sourced from login information, device IDs, geolocation and online behavior, among others. Many graphs are hybrids that layer probabilistic methods to create broader connections on top of a foundation of deterministic matches.

What Are Deterministic Methods?

Deterministic identity resolution is generally viewed as more accurate than probabilistic methods because it is provided by individuals. But is it truthful? That depends on the user and circumstance.

First-party data is the most common form of deterministic data. This method is effective when there is robust data, such as email addresses, browsing patterns or purchase history, directly provided by customers through service use or by subscriptions. It involves merging new data with existing customer records to identify matches.

The strength of this approach is its high confidence level, allowing businesses to be certain that an online action is associated with a specific identity, even if some users disguise the information requested.

Authenticated Traffic Solutions are another practice. Based on websites with user accounts, these leverage logged-in user data for targeting. They link authenticated user data to persistent identifiers that can be used in programmatic ad buying. Examples include LiveRamp's RampID, LiveIntent's LiveID, and Unified ID 2.0. Other mechanisms such as Epsilon's CORE ID and Neustar's Fabrick ID rely on both authenticated and unauthenticated traffic.

What Are Marketers Doing to Manage Private and Public Sector Changes?

Navigating Google's Third-Party Cookie Deprecation

The biggest shock to trackers in 2024 is the deprecation of third-party cookies in Google Chrome. Following similar changes in Safari, Firefox, Edge and other browsers, Chrome's blocking of third-party cookies is driving the development of new tracking technologies that are more privacy-focused and reliant on first-party data. Google Chrome began restricting third-party cookies in early January 2024. Deprecation will culminate in Q3 2024 if the schedule holds.

In addition, expanding regulatory pressures – from E.U. interpretations to U.S. state laws and federal rulemaking – increase the role of user consent and data privacy in trackers. This leads to a more transparent and ethical approach to data collection and usage.

Businesses are adapting to changes in privacy expectations. They leverage new tools and methods that respect user privacy while providing valuable marketing insights. This balance maintains trust and loyalty with customers and complies with evolving regulations.

The deprecation of third-party cookies does not mean the end of pixels and tags, however. Although their ability to track user behavior across sites will be diminished, they will still function effectively within the boundaries of the sites on which they are placed. Sites will no longer set third-party cookies to track users across the web, but they remain valuable tools for gathering first-party data, such as user interactions on a single site.

Pixels and tags will still be able to track conversions, measure ad effectiveness and gather site-specific analytics, which is crucial for website performance optimization and understanding user behavior on a single site.

With these changes, marketers will explore probabilistic and deterministic elements to deliver relevant ads while respecting user privacy.

See "After Death of the Cookie, New Advertising Strategies Raise Compliance Questions" (Sep. 2, 2020); and "Recommended Data Strategies As Google Swears Off Web Tracking" (Mar. 24, 2021).

Building New Capabilities and Collaborating With Partners

In efforts to find complementary strategies for the new regulatory and post-cookie world, many businesses are testing the Google Privacy Sandbox. Google solutions are an amalgam. Deterministic elements are the Topics API, which assigns users to groups based on specific "topics" they browse, and Federated Learning of Cohorts, which creates "cohorts" based on many browsing habits. Probabilistic elements foster privacy-preserving ad exchanges and attribution solutions.

Some share data in clean rooms. Advertisers upload first-party data, which is then matched against anonymized data such as purchase data from a retailer or browsing data from a publisher. Advertisers can evaluate campaign results by aggregated segments without revealing personally identifiable information.

Others are building data management capabilities. Businesses are experimenting with combinations of first-party data, data management approaches, investments in technology and data partnerships. They use statistical models to match users across platforms, offering lower match rates but potentially higher privacy.

The majority are expanding data partnerships and addressable media channels. Businesses are forming more partnerships with walled gardens like social networks and exploring new addressable media channels such as CTV and digital audio. These channels use first-party data.

Publishers are enhancing contextual targeting. It begins with ads served based on the surrounding content users are consuming. Then other signals such as browsing history and search queries are blended. Now AI, namely natural language processing for sentiment analysis, and computer vision for image analysis, super-charge contextual targeting.

See "Ad Industry's Third-Party Data Use Grew Despite Impending Cookie Shutdown" (Feb. 23, 2022).

Dan Frechtling is CEO of Boltive, inventor of simulated user technology that automates privacy and security compliance. Enabled by eight patents, Boltive software interacts with websites, apps and ads, detecting code errors, vendor risks and malicious behavior. Prior to joining Boltive, Frechtling was president of G2 Web Services, a cybersecurity company acquired by Verisk.

Matt Pollard is the global head of data responsibility, privacy and AI ethics for Slalom, a next-generation professional services company creating value at the intersection of business, technology and humanity. Founded in 2001, Slalom is an employee-owned, high-growth company known for bringing together deep local expertise with global insights across 39 offices in eight countries. Before joining Slalom, Pollard held executive-level positions at global technology companies.

Leslie Shanklin is the head of Proskauer's global privacy & cybersecurity group, a partner in its corporate department and a member of its technology, media & telecommunications group. Prior to joining the firm, she led global privacy teams for media and entertainment companies for over a decade and most recently served on the privacy leadership team for Warner Bros. Discovery. Her practice focuses on privacy and data security, delivering comprehensive expertise around data-related risk and compliance.