Cybersecurity Law Report cslawreport.com

Feb. 21, 2024

Corporate Governance

Tracking Technologies: A 360-Degree Governance Plan

By Julie Rubash, *Sourcepoint*; Leslie Shanklin, *Proskauer*;
Michael Hahn, *IAB - Interactive Advertising Bureau*

The technologies associated with digital tracking, as well as the related laws, regulations and risks, are complex and dynamic. This complexity requires a comprehensive governance program to adequately address the significant and growing legal and business risks that tracking technologies present. As with many aspects of data protection – but particularly with digital tracking – legal teams cannot manage the risks alone.

This third installment of a four-part article series provides a roadmap for organizations starting out – or working toward – crafting a comprehensive, cross-functional program for managing digital trackers. As discussed below, such a program requires both internal policies and processes as well as external collaboration with vendors and partners to ensure alignment in approach and adequate accountability. For many organizations, achieving sound governance over digital tracking is a daunting task. Given the complexities, for many organizations the process must be undertaken in various stages centered on risk-based decisions around prioritization.

The final part of this series will focus on digital tracker compliance challenges and solutions, including those specific to the advertising industry. Part one examined legal regulation and use risks around online tracking technologies. Part two took a deep dive into the technical workings and types of digital data collection tools.

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

Understanding the Different Lenses of Risk and Responsibility

At the outset, it is important to note that tracking tech compliance is a concern that crosses many aspects of the digital world. Certainly, publishers of digital services such as websites and mobile apps often are considered to be on the front lines of regulatory scrutiny and legal challenges around digital tracking. Many other types of organizations, however, also bear compliance responsibility

and risk, including digital distribution platforms, advertisers, tech providers and those that offer other types of digital services or platforms, including a vast array of IoT devices.

The aforementioned roles are not mutually exclusive – often companies play many different roles with respect to digital tracking. Publishers are also advertisers. Platforms are advertisers and often publishers as well. Every organization must consider the various roles it plays with respect to digital tracking and evaluate the unique risks and compliance responsibilities that attach to each role.

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

Initial Audit, Evaluation and Decisioning Roadmap

There are three recommended stages for preliminary efforts to govern digital tracking: (1) auditing the current state; (2) evaluating audit results; and (3) making decisions based on the evaluation.

Auditing Current State

The first step in crafting a tracker governance plan is to gain a baseline understanding of the company's current state. It is critical to understand the following:

- what trackers – both first-party and third-party – are integrated with the company's digital properties;
- the manner in which they are integrated;
- how they are collecting data;
- what data is collected;
- where the data is going; and, ultimately,
- how that data is used.

Who leads such an audit depends upon the staffing structure of the organization. Typically, the audit and assessment work needed to begin the process of creating a sound tracker governance program is spearheaded by an organization's privacy team.

Defining the Audit Scope

To be most efficient, the audit should be conducted as a single, comprehensive process, encompassing all tracking technologies across the company's portfolio of digital properties, including its digital ads and email marketing. This will provide a full, upfront picture of the current state to allow for the most accurate and exhaustive assessment.

Before beginning the audit, to formulate its scope, two principal buckets of information should be gathered: (1) a list of internal and external stakeholders; and (2) a list of all digital properties.

Bucket one should include all teams and individuals, both internal and external, with any role in setting or managing trackers. This includes stakeholders making strategic decisions that drive the type of trackers being set, such as the teams defining what consumer insights are needed regarding engagement with a website, app, digital ad or email campaign. A good place to start is often the advertising and marketing teams, including both the strategic teams and the operational teams, but other potential stakeholders (depending on the nature and size of the company and how its operations are structured) could include digital product, engineering, data science, IT, HR or any other team that might have access to – or influence over – the development, content, operations or assessment of the company's digital properties, as well as its advertising and marketing strategy and operations.

Bucket two should at least include all websites and mobile apps, but may also include email platforms, CTV/OTT apps, IoT devices and anything else that has the potential to incorporate tracking technologies. This may be a bit of a chicken-and-egg exercise, as the stakeholders in bucket one may help to identify the properties in bucket two, but identifying the digital properties may lead to the appropriate stakeholders, so it likely will be an iterative process of gathering and refining the information between the two buckets a few times before feeling comfortable that both lists are complete.

Conducting Stakeholder Interviews

Once the stakeholders and digital properties are defined, the audit itself can begin. Although an efficient audit is usually a single, comprehensive process, the goal of that process should be to identify and flesh out the individual details of every tracker on every digital property on the list. Therefore, the audit should be specific to the facts and circumstances of each tracker.

The best way to get a comprehensive view of all trackers on a digital property is to use a combination of stakeholder interviews and scanning technologies. The order of operations may depend on the company structure and size, but for the first "baseline" audit, it is often most effective to start with a first round of stakeholder interviews, which will provide an initial understanding of known technologies.

Depending on the stakeholder's role, the interview could be specific to certain digital properties, third-party engagements or contexts, but the goal of the interview is to uncover the following:

- a full list of first- and third-party trackers of which the stakeholder is aware;
- the purpose of the trackers;
- which digital properties they are integrated with;
- whether there is a contract (including click-to-accept terms) with the third party (for external trackers);
- whether the company (for internal trackers) or third party (for external trackers) is sharing the information downstream with other third parties or combining the information collected with other information; and, if so,
- what information and for what purpose.

Information about the context and content of the digital properties (and specific pages of the digital properties) where the trackers are placed, as well as the company's relationship with users whose information is collected, should also be gathered. For example, if there is a possibility that the trackers could be intentionally or unintentionally collecting health, financial, precise location, or other potentially sensitive data or video viewing information, or transmitting user communications, it is critical to learn that in the evaluation stage. In addition, it may be useful to know whether the user could be logged in or just a casual visitor, and whether the user could be a subscriber to video or other content.

Conducting this first set of interviews before a technical scan may seem counter-intuitive, but this approach serves multiple purposes. It will help ensure that the scope of the scan is broad enough, pinpoint any particular "high-risk" items on which the audit should focus and identify any flaws in the scan (*e.g.*, if certain "known" trackers are not showing up in the scan, there may be an issue with the scanning technology or its configuration).

Running a Tracker Scan

After the first round of stakeholder interviews is complete, the next step should be running a technical scan of the digital properties. The goal of this scan is to produce a full list of all tracking technologies, not just cookies, so a simple "cookie scanner" may not be sufficient. It is also important to ensure the scan is comprehensive enough to pick up trackers at different times of day and under various circumstances (*i.e.*, in response to assorted user interactions with the property) to produce a full, comprehensive picture of all trackers and their actions. A one-time glimpse of a digital property at a single point in time likely will not produce that full picture. In fact, adding to the significant complexity of this exercise is the reality that, in many cases, the trackers appearing on a digital property may be dynamic for some types of operations, such as programmatic advertising. Running scans over different days will provide visibility into digital operations that are resulting in a changing group of trackers, as the compliance approach for such operations will need to account for this complexity.

Filling in the Gaps

It is common for a number of trackers, or information about certain trackers, to be revealed in the scan that did not come up in stakeholder interviews. This could be due to stakeholder oversight or a gap in the stakeholder identification or interview process, but often it is due to trackers existing on the digital properties that are unknown to everyone in the company.

It is not uncommon for third-party trackers to appear as a result of a call from another third party, so it is very possible that some trackers may be several degrees removed from the first layer of vendors directly engaged by the company. This path to the original source of a tracker can often be traced through the scan, but additional stakeholder inquiry may be necessary to fully understand why third-party trackers are called, whether they are necessary, and whether a proper contractual relationship is in place.

After running a scan, therefore, stakeholders should be consulted again to verify new information and fill in any gaps about those additional trackers. This stage may also require reaching out to the third-party vendors to find additional information about their trackers or calls they are making to other third-party trackers. It may also involve looking into how specific trackers are configured.

At the end of this process, a complete record should exist for each tracker discovered, including its business purpose, what data is collected, the complete data flow from the user through each layer of the downstream process, and whether the data may be combined with other information. If a certain category of trackers appears to be changing dynamically, it is possible that such trackers are set by third-party ad partners that are allowing some of their downstream partners to set trackers. If this if happening, identifying the original source will be critical to deciding upon a governance approach.

Evaluating Current State Audit Results

Armed with a complete record of each tracker, it will be time to move on to the evaluation stage. This involves legal, business and technical assessments, so all relevant stakeholders should remain involved.

Legal Assessment

For each tracker, all of the information gathered in the audit should be assessed to determine what laws could be implicated and how closely the facts line up with the elements of such laws. The risk tied to the tracker may be heightened based on the type of information involved, so an understanding of whether sensitive or other high-risk data is collected is an important element of this assessment.

Legal compliance is increasingly requiring more detailed information to be disclosed about individual trackers. Thus, critical to ensuring appropriate disclosures are made, the legal assessment also should contain the correct information about the tracker source, purpose, data collection and duration.

Business Assessment

An equally important part of the evaluation process for each tracker is to understand the value of the tracker to the company. Companies often discover trackers that no one in the company cares, or even knows, about, or that are no longer relevant to the original business purpose.

If the company has not had a good governance program in place to ensure trackers are disabled at the end of a particular ad campaign, for example, there may be legacy trackers still firing on services that no longer serve any useful purpose. There may be a valuable business purpose for other trackers, but that purpose may not require every element of data that is collected, placement on every page of the digital property or placement for an extended period of time. It is therefore important for this part of the assessment to understand the specific goals for use of the tracker and the

degree to which those goals can still be achieved through alternative configurations and placements that may remove legal risk. Often, the combination of the business and legal evaluations results in removal of many trackers to ensure the principle of data minimization is honored.

Technical Assessment

The third and final component of the tracker evaluation process is the technical assessment. This involves an understanding of all available technical options with respect to the tracker. In most cases, one option is removing the tracker altogether (or terminating a relationship with the third party calling the tracker). Other options that market participants frequently evaluate include de-identifying, obfuscating or preventing the sharing of certain data elements or re-configuring the tracker software or settings to prevent certain data usage. This part of the assessment may also involve an understanding of the technical requirements to obtain user consent, extend other user rights or make disclosures, depending on the particular legal risks involved.

Making Governance Decisions Based on Current State

The legal, business and technical assessments, when considered together, should lead to a final plan of action for each tracker. After completing the full assessments for each tracker, a company can decide to take different approaches on a tracker-by-tracker basis, perhaps by removing certain trackers altogether, while reconfiguring, changing the placement of, or obtaining user consent (or opt-out depending on applicable law) for other trackers.

See "Examining Security Mandates, Including California's Draft Audit Regulations, in State Privacy Laws" (Nov. 1, 2023).

Creating a Forward-Looking Governance Plan

The first tracker audit, assessment and decisioning exercise generally is the most difficult and time consuming. Once a baseline audit and evaluation is conducted, an ongoing, sustainable tracker governance plan and process should be established to: (1) discover and evaluate new trackers that business teams wish to integrate into digital products; and (2) re-evaluate existing trackers to assess updated legal, business and technical information. Creating such a plan and process generally involves the following key steps.

Assemble a Tracker Governance Team

In order to ensure appropriate oversight over digital trackers, a team should be assembled to oversee and manage the tracker governance program and facilitate continual assessment of legitimate business needs, evolving legal requirements and changing business partnerships.

The composition of the team will vary depending on the nature, size and structure of the organization, but typically the team will include representatives from:

- legal/privacy/compliance;
- digital product and engineering;
- research/consumer insights;
- marketing and advertising (representatives from strategy and operations); and
- data science/data strategy (if the organization has this team).

It is important that this tracker governance team (TGT) be composed of individuals with sufficient seniority to understand the organization's key strategic goals and make governance decisions as needed.

See "Advice From a CISO and Lawyer on Best Practices in Information and Data Governance" (Feb. 15, 2023).

Establish Legal Requirements

In order for the TGT and other governance process stakeholders to have a clear understanding of the baseline legal requirements for the implementation and management of tracking technologies, it is recommended that the legal/privacy team create a set of defined and documented legal requirements for trackers that address variances in law across different territories.

The legal team's documentation also should address the various roles an organization may be playing with respect to trackers. As noted above, a single organization could be acting as a platform, digital publisher, advertiser and/or tech provider, and each role will require a different approach to compliance.

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

Create a Centralized Process for Setting and Managing Trackers

With an understanding of the baseline legal requirements that apply in each territory of operations and across different business divisions, and taking into account other overarching principles the organization applies to data governance, the TGT should work together to create a defined process for setting and managing trackers. Most critically, this process should be based upon a centralized structure, with the foundational principle being that no trackers are integrated into a digital property without going through a defined review and approval process. Depending on the size of the organization and scope of its digital operations, this review and approval process can be organized around a single organization-wide process owner, or there can be pods of centralized processes that apply to particular properties or operational divisions. The established process should include the following.

Review, Approval and Management

There should be a clear intake point for submission of new trackers that business teams wish to integrate so that each tracker can be reviewed with appropriate consideration of business need and legal requirements. The assigned process owners should also be assigned responsibility for ensuring that trackers are appropriately configured and deprecated when the business justification for them has ended. This process should have clearly defined lines of oversight and responsibility.

Technology Strategy

Management of trackers will require technology solutions. The TGT will need to consider legal requirements, business goals and existing tech infrastructure to determine what technology tools are needed to implement the governance strategy. The relevant tech may include tag managers, consent management platform tools and industry group technology solutions (such as the IAB Tech Lab's solutions discussed in part four), as well as technical configuration of trackers and tech integration with third-party platforms and tools.

Third-Party Governance

Critically, external partners such a marketing agencies and ad partners should not have authority to implement trackers directly into an organization's digital properties – all trackers should run through an internal review, approval and implementation process to ensure the trackers comply with the organization's policies and are implemented and managed correctly from a tech perspective.

Internal Policies

Once a tracker governance process has been established, written policies and guidance documents should be created that document the organization's guiding principles around tracking technologies, the rules and guidelines to be followed, and the agreed processes. These policies should align with other internal data governance policies as well as external-facing privacy notices. Fundamental privacy principles, such as data minimization, purpose limitation and transparency should be foundational to the governance strategy and woven into both the policies and the defined operational processes.

Ensure Vendor and Partner Contracts Align With Governance Approach

Once an internal governance plan is in place, work will need to be done to ensure that vendor and partner contracts align with the company's policies and processes as well as evolving prescriptive legal requirements. These contracts should clearly define the following:

- what trackers are being set;
- the data to be collected from the trackers (and relevant specific prohibitions);
- how collected data is allowed to be used and shared; and
- how long the trackers will be live.

In the case of trackers the company seeks to exclude from do-not-sell-or-share opt outs in the U.S., the relevant contracts with those third-party tracking providers will need to reflect the required legal provisions and prohibitions on the partner's use of data. Many vendor contracts are now integrating a "tracker appendix" that sets out relevant details about any trackers at issue in the engagement or partnership with specificity.

These third-party efforts bring tracker governance full circle.

See "Expedia and Lululemon Privacy Pros Discuss Scaling Vendor Contracting for New Privacy Laws" (Apr. 19, 2023).

Julie Rubash is GC and chief privacy officer for data privacy software company Sourcepoint, where she coordinates legal efforts and ensures that the product suite innovates and expands to meet the demands created by the changing regulatory landscape. Rubash brings over 15 years of legal experience both at law firms and as internal counsel in the media, technology and advertising sectors. Prior to joining Sourcepoint, she served as vice president of legal at advertising platform Nativo.

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.

Michael Hahn is executive vice president and GC at IAB and IAB Tech Lab. He has responsibility for all legal matters, including the direction of legal strategy, privacy compliance, antitrust compliance, intellectual property rights issues and general corporate matters. Hahn also serves as an advocate for the digital advertising industry on common legal issues affecting member companies.

© 2024 Mergermarket Limited. All rights reserved.