PUBLICATION

Digital Marketing Meets DOJ Oversight: What Businesses with Digital Campaigns Should Do to Manage AdTech Risks

Authors: Vivien F. Peaden, John S. Ghose
June 25, 2025

With the ease of apps and websites for planning activities, whether it be vacations, business trips, or shopping, we open ourselves to multiple sources of being followed across devices by collecting, analyzing, and sharing our data. While cookies enhance digital experience, they also raise concerns under the new DOJ bulk data access rules (the DOJ Rule), requiring closer collaboration between legal and marketing teams to monitor their AdTech vendors and downstream data sharing practices.

Effective on April 8, 2025, the DOJ Rule has significantly expanded the definition of "sensitive personal data" to include **mobile advertising IDs (MAIDs), IP addresses, cookie data,** and **contact information**, when used in combination with one another (as explained in this Client Alert). When digital marketing campaigns share these datasets with downstream recipients abroad, such data exchanges may face heightened scrutiny under the DOJ Rule (as described in this Client Alert). The DOJ will begin to prioritize enforcement *after* July 8, 2025. It is crucial for businesses engaged in digital campaigns to ensure that they are in compliance with the new cross-border data protection requirements. In this alert, we unpack the evolving data protection landscape under the DOJ Rule, where even targeted ads can trigger targeted DOJ enforcement.

1. Why Is Digital Advertising Suddenly a National Security Issue?

The digital marketing sector has long believed that cookies collect only anonymized data and are exempt from many data protection laws. However, this assumption is no longer valid under the DOJ Rule's broad definition of "**sensitive personal data**". Notably, the DOJ Rule's commentary sections reference the terms "**advertiser**" or "**advertising**" more than **70 times**, highlighting its potential to reshape the AdTech industry.

The DOJ Rule, often referred to as the "**Data Security Program (DSP)**," traced its foundation to **Executive Order 14117**, which was released on February 28, 2024, under the previous administration. The Executive Order highlights a growing national security concern: foreign adversaries, such as China, Iran, and Russia, have access to AI and cutting-edge technologies to potentially analyze and exploit a massive volume of sensitive U.S. personal data. **Even if such data is anonymized, advances in technology now make it easier to re-identify individuals and reveal patterns about U.S. populations and government locations. This risk increases significantly when large volumes of non-sensitive data are combined with other user information for data analytics**. Digital marketing collects and analyzes large amounts of information, creating an attractive target for downstream recipients based in any Country of Concern seeking to exploit sensitive information.

2. When Does Data Collection through Digital Marketing Trigger the DOJ Rule?

The DOJ Rule prohibits a U.S. entity from knowingly sharing Bulk U.S. Sensitive Personal Data (as defined below) with foreign entities abroad where the recipients are:

(i) In China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, Venezuela, or other foreign adversaries designed by the DOJ (**Country of Concern**);

(ii) Legal entities controlled or organized under laws of Countries of Concern (including such state-owned entities), as well as individuals primarily residing in Countries of Concern or employed by such entities under the Countries of Concern's control (**Covered Person**); or

(iii) Foreign entities (who are not Covered Persons), **unless** the U.S. entity contractually requires such foreign recipients *not* to engage in any subsequent data brokerage transactions with Countries of Concern or Covered Persons.

Under the DOJ Rule, the term "**Data Brokerage**" is broadly defined to mean:

"the sale of data, **licensing of access to data, or similar commercial transactions***, excluding an employment agreement, investment agreement, or a vendor agreement,* **involving the transfer of data from any person** *(the provider)* **to any other person** *(the recipient),* **where the recipient did not collect or process the data directly from the individuals** *linked or linkable to the collected or processed data."*

According to the DOJ, some data exchanges in the ordinary course of business may nonetheless constitute data brokerage involving Bulk U.S. Sensitive Personal Data In digital marketing, sharing cookie data or device IDs with third-party AdTech providers is under increased scrutiny if it meets or exceeds certain thresholds. When the volume of such low-risk data identifiers in combination with another exceeds **100,000 records within 12 months**, such data exchanges are now considered a covered data transaction involving "**Bulk U.S. Sensitive Personal Data**." Given their reliance on large-scale data collection and analytics, most digital and personalized ads campaigns quickly exceed this threshold. As a result, any transfer or provision of access to Bulk U.S. Sensitive Personal Data to Covered Persons, Countries of Concern, or foreign entities engaging in downstream sharing with restricted recipients may trigger DOJ scrutiny.

Another often overlooked area for due diligence under the DOJ Rule is the proliferation of "**advertising tag(s)**" or "**Ad Tag.**" An Ad Tag is a small piece of HTML or JavaScript code incorporated into a website to gather information about its visitors. Marketers rely on Ad Tags to share with third-party AdTech vendors to drive advertising, marketing, and optimization tools. While companies typically manage Ad Tags they install directly, they are often unaware that their primary Ad Tags can load additional third-party tags, known as "piggyback tags," onto the website. Because these piggyback tags can dynamically harvest sensitive personal data at scale, they pose a serious compliance risk under the DOJ Rule.

Some examples where the sharing of digital advertising data could likely be in the crosshairs of national security concerns:

- A U.S. social media platform collects device ID, cookie data, and/or precise geolocation data of its users and then shares the datasets with a foreign company that is not a Covered Person. The U.S. company knows (or reasonably should know) that the foreign company is a front company staffed primarily by Covered Persons. As a result, Countries of Concern can glean valuable information about the health and financial well-being of a large number of Americans.
- A U.S. company owns and operates a mobile app for U.S. users with available advertising space. As part of selling the advertising space, the U.S. company provides IP addresses and advertising IDs of more than 100,000 U.S. users' devices in 12 months to an advertising exchange based in Europe that is not a Covered Person. Even though the EU recipient is not a Covered Person or Country of Concern, this data exchange constitutes a prohibited data brokerage transaction unless the U.S. company includes a contractual clause that prohibits the European business from reselling or otherwise engaging in a data brokerage transaction involving this set of Bulk U.S. Sensitive Personal Data with a Country of Concern or Covered Person.

- A U.S. company knowingly deploys tracking pixels or software development kits (SDK) to its mobile platform. For targeted advertising purposes, the platform provides Covered Persons (including social media platforms that develop these pixels and SDKs) access to device IDs, precise geolocation data, IP addresses, and/or MAC addresses. This data transfer constitutes a prohibited data brokerage transaction.
- A U.S. mobile platform sells advertising space to an advertising exchange based in a Country of Concern during a 12-month period. As a result of this transaction, the ad exchange, which is a Covered Person, will access precise geolocation data, IP address, and/or advertising IDs of U.S. users. This sale of advertising space is a prohibited transaction involving data brokerage. Importantly, the DOJ does not exempt cases where low-risk data, such as IP addresses or contact details, is combined only with advertising or device IDs, without further data in combination with other higher-risk data.

3. What Should U.S. Businesses Do to Reduce DOJ Enforcement Risk while Running Digital Marketing Campaign?

Obtain written commitments: When a U.S. company uses cookies or operates digital marketing campaigns from its website or mobile apps, it may be engaging in a data brokerage transaction, especially if the dataset is shared with or accessible by foreign entities. Even if the recipients are not Covered Persons or Countries of Concern, companies must still obtain written commitments to ensure downstream data sharing does not involve these restricted parties.

Maintain systems and controls: U.S. companies subject to the DOJ Rule are still responsible for maintaining appropriate systems and controls, such as reasonable and proportionate due diligence**,** to reduce the risk of non-compliance. Businesses involved in data brokerage transactions with non-covered foreign entities cannot simply shift responsibility or rely entirely on their foreign partners to follow these contract terms. In other words, if a U.S. business fails to conduct proper due diligence and ignores the foreign person's violations, it could still face enforcement action. Additionally, a U.S. business must also report any known or suspected violation involving the prohibited onward transfer or resale of Bulk U.S. Sensitive Personal Data within 14 days after any discovery.

Conduct regular tag audits and exercise strict oversight: The widespread use of Ad Tags is introducing new compliance challenges. Without the website owner's knowledge or explicit consent, a primary Ad Tag can introduce additional tags loaded by downstream AdTech providers, i.e., the "piggyback tags." This lack of visibility and control over piggyback tags increases the risk of unauthorized data access by the Covered Person and non-compliance with regulatory requirements. To keep these hidden trackers in check, companies involved in digital marketing should conduct regular tag audits and exercise strict oversight over the use of AdTech providers.

4. How Should U.S. Businesses Respond to a DOJ Rule Enforcement Investigation?

If a U.S. business is served with legal process related to a DOJ Rule investigation, such as a subpoena, civil investigative demand, or national security letter, it should respond quickly and strategically. First, legal counsel (internal or external) should verify the document's validity and lead a privileged internal investigation, using consistent documentation and a secure, access-restricted team. Litigation holds must be issued immediately to preserve all relevant data, including structured/unstructured data, chat logs, cloud buckets, and ad-tech sources. Subject matter experts in privacy and national security should be consulted under privilege, including through common interest arrangements with business partners. At the same time, businesses should map any cross-border data flows to assess what personal data left the U.S., how, when, and through whom, evaluating any potential violations or applicable exemptions.

Once data has been gathered, analyzed, and risks assessed, the business should engage with DOJ on a rolling basis – producing information, raising objections when warranted, and, if necessary, meeting with investigators to explain technical systems and data architecture. Concurrently, companies should also brief audit committees and investors on potential future risks, including potential enforcement actions. These coordinated legal and operational steps are critical for companies to effectively navigate a DOJ Rule enforcement inquiry.

5. Summary

As digital marketing continues to drive business growth, the DOJ Rule has significantly elevated the stakes for cross-border data collection, use, and transfers. With common data types like device IDs, and IP addresses now deemed sensitive, even routine marketing practices can trigger compliance obligations. To manage risks, U.S. businesses must embed compliance into every layer of their digital marketing strategy, from regularly auditing website cookies, identifying hidden piggyback tags, and conducting enhanced vendor assessments, to enforcing strict contractual controls. To successfully navigate the complex landscape under the DOJ Rule, proactive compliance is no longer a choice but a branding advantage that protects consumer data and builds trust.

For more information or assistance regarding a compliance program, please contact Vivien Peaden, AIGP, CIPP/US, CIPP/E, CIPM, PLS, John Ghose, or a member of Baker Donelson's Data Protection, Privacy and Cybersecurity Team.