office of
Data Privacy

Advisory 2025-01

Website Visitor Tracking and Monitoring Tools for Utah Governmental Entities

Issued: January 6, 2025

DISCLAIMER

The Utah Office of Data Privacy makes every effort to ensure that the analysis provided in each Privacy Advisory is based on the correct interpretation of privacy laws and regulations in effect at the time the Advisory is issued. However, over time, changes in statutes, regulations, or judicial interpretations may affect the accuracy of this analysis. Readers should understand that Privacy Advisories provide general guidance and information regarding privacy protections and obligations for governmental entities, but they should not be considered legal advice. For specific legal concerns, entities are encouraged to consult legal counsel to ensure compliance with current laws.

Introduction

The Office of Data Privacy (ODP) recognizes the importance of transparency and privacy for individuals who interact with public entity websites. This document will cover the appropriate use of 1st and 3rd party tracking tools, including cookies, pixels, keyloggers, fingerprinting, audio and video recording, and other technologies. We will discuss when these tools are appropriate, provide best practices for notification and consent, and introduce a free tool to help scan and identify tracking mechanisms on your websites.

Why Governmental Entities Should Prioritize Website Tracking Transparency

Governmental entities across Utah have a duty to respect individual privacy and protect personal data, as mandated by state law. Compliance with these requirements is essential to maintaining public trust and ensuring that personal data is used responsibly. Under **Utah Code 63A-19-401 (Government Data Privacy Act)**, governmental entities are specifically required to:

- **Collect Only Necessary Data**: Under the principle of data minimization and specific requirements under GDPA[1], governmental entities must limit the personal data they collect to what is strictly necessary for a specified purpose. Tracking mechanisms that capture unnecessary data risk violating this mandate, increasing data privacy risks and potential legal exposure.
- **Avoid Undisclosed Surveillance**: GDPA prohibits government entities from establishing, maintaining or using undisclosed or covert surveillance of individuals unless permitted by law.[2] The use of tracking tools such as cookies, pixels, fingerprinting, keyloggers, and audio or video surveillance could be perceived as covert surveillance if not disclosed in an appropriate manner.
- **Restrict Sharing of Personal Data**: GDPA prohibits the sharing of personal data unless it is explicitly permitted by law[3]. Unauthorized sharing of data, particularly through third-party tracking technologies, may lead to legal liability and compromise user privacy.

[1] §63A-19-401(2)(c)
[2] §63A-19-401(2)(f)
[3] §63A-19-401(2)(h)

Furthermore, **Utah Code 63A-19-402** emphasizes that entities must provide a clear **Personal Data Request Notice** when collecting personal data, detailing the purpose, intended uses, potential consequences of refusal, data-sharing practices, and the record series the data will be included in[4]. Notice of the data collection on a website must be posted in a prominent place on the website[5] and is in addition to the website's privacy notice[6]. Failure to disclose these practices undermines the trust Utah residents place in their government, potentially compromising the effectiveness of public services and eroding public confidence.

Adherence to these laws is not only a matter of compliance but is critical for upholding public trust. Over-collection and lack of transparency can lead to heightened risks of data breaches, unintended disclosures, and harm to individuals. By prioritizing responsible data handling and website transparency, Utah's governmental entities can minimize these risks and set a standard for ethical data governance.

Types of Tracking and Monitoring Tools

1. **Cookies**: Small files placed on a user's device, often used to remember preferences or track website usage.
2. **Pixels**: small, transparent images or graphics embedded into a web page or email and used to collect data about users and their interactions with websites, emails, and ads
3. **Key Loggers**: Programs that capture keystrokes, often used for security or productivity but can be invasive if not transparently disclosed.
4. **Fingerprinting**: Technology that collects information about a user's device and browser to create a unique identifier, often used for tracking purposes.
5. **Other Tracking Technologies**: Includes tools like beacons, session replays, and analytics tools that monitor user behavior or even collect audio recordings or video recordings of the computer screen or the user and the surrounding area.

Appropriate Use of Tracking Tools

- **Purpose-Based Use**: Tracking technologies should only be used for purposes that align with public interests, such as providing the website, to improve the functionality of the website, and security, or accessibility enhancements.
- **Data Minimization**: Collect only what is necessary to fulfill the purpose for the website. Avoid technologies that gather excessive or invasive data unless authorized by law.
- **Transparency**: Entities must be clear about the reasons for tracking and provide users with accessible information on how their data is used.

When Tracking Tools are Inappropriate

- **Without Clear Purpose**: Do not use tracking tools when there is no legal authorization.
- **For Sensitive Information**: Avoid tracking technologies on pages where users may input sensitive information (e.g., financial data, health information) unless it is strictly necessary, authorized by law, and security measures are in place.
- **Without Consent**: Avoid any type of tracking, unless it is strictly necessary or authorized by law, without obtaining express consent or providing an option for users to opt out.

[4] §63A-19-402(1-2)
[5] §63A-19-402(3)(a)
[6] §63A-19-402(4)

Notification and Consent

1. **Disclosure**: Clearly disclose the types of tracking technologies in use, their purpose, what data is collected, your use and any sharing of the data, and your legal basis for the collection.
2. **Privacy Notice Update**: Ensure your website's privacy policy includes a comprehensive section on tracking tools, as required by law, including the entity's contact information, data collection practices, and users' rights.
3. **Consent Mechanisms**:
   ○ **For Cookies**: The Office recommends entities use a cookie consent banner that allows users to manage their preferences and opt out of non-essential cookies.
   ○ **For Other Tools**: Provide users with a simple way to opt out of non-essential tracking mechanisms if they choose not to be tracked.

Free Tool for Scanning and Identifying Tracking Mechanisms

To help ensure compliance and transparency, the Utah Office of Data Privacy offers a website scanning tool from ObservePoint. This tool will:

- **Scan for Tracking Technologies**: Identify cookies, pixels, keyloggers, fingerprinting, and other tracking tools on your website.
- **Provide a Report**: Generate a summary of findings.
- **Enhance Privacy Practices**: Assist in maintaining a user-friendly and privacy-compliant website for the public.

Steps for Agencies to Request a Scan

Submit your website audit (scan) using the following form. The form will collect the following details:

- Requester name and email
- Agency name.
- Website domain/subdomain URL(s) to be scanned (Only public facing websites may be scanned at this time).

For State Agencies

If the Website is Administered by DTS:

Use **Quarterly PI Planning** with your DTS IT Director to:

- Review the scan report findings.
- Collaborate with the DTS IT director and relevant teams to plan the remediation of valid issues.
- Document any remediation efforts.
- Update the agency's website privacy notices and tracking policies to reflect actual purposes and uses of website tracking technology usage.
- Submit a request to re-scan applicable websites to validate results of remediation efforts.

If the Website is Administered by a Third-Party Vendor:

Coordinate Directly with the Vendor:

- Share and review the scan report findings with the vendor.
- Work directly with the vendor to address valid issues and implement remediation efforts.
- Coordinate with the vendor to update the agency's website privacy notices and tracking policies to reflect actual purposes and uses of website tracking technology usage.

For other Governmental Entities

Coordinate with your information technology leadership and website owners to perform the following tasks:

- Review the scan report findings.
- Plan the remediation of valid issues.
- Document any remediation efforts.
- Update the entity’s website privacy notices and tracking policies to reflect actual purposes and uses of website tracking technology usage.
- Submit a request to re-scan applicable websites to validate results of remediation efforts.